Surveillance, Privacy and Security

This volume examines the relationship between privacy, surveillance and security, and the alleged privacy–security trade-off, focusing on the citizen's perspective.

Recent revelations of mass surveillance programmes clearly demonstrate the ever-increasing capabilities of surveillance technologies. The lack of serious reactions to these activities shows that the political will to implement them appears to be an unbroken trend. The resulting move into a surveillance society is, however, contested for many reasons. Are the resulting infringements of privacy and other human rights compatible with democratic societies? Is security necessarily depending on surveillance? Are there alternative ways to frame security? Is it possible to gain in security by giving up civil liberties, or is it even necessary to do so, and do citizens adopt this trade-off? This volume contributes to a better and deeper understanding of the relation between privacy, surveillance and security, comprising in-depth investigations and studies of the common narrative that more security can only come at the expense of sacrifice of privacy. The book combines theoretical research with a wide range of empirical studies focusing on the citizen's perspective. It presents empirical research exploring factors and criteria relevant for the assessment of surveillance technologies. The book also deals with the governance of surveillance technologies. New approaches and instruments for the regulation of security technologies and measures are presented, and recommendations for security policies in line with ethics and fundamental rights are discussed.

This book will be of much interest to students of surveillance studies, critical security studies, intelligence studies, EU politics and IR in general.

Michael Friedewald is Senior Research Fellow at the Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe, Germany.

J. Peter Burgess is Professor and Chair in Geopolitics of Risk at the École Normale Supérieure, Paris, and Adjunct Professor at the Centre for Advanced Security Theory (CAST), University of Copenhagen, Denmark.

Johann Čas is Senior Researcher at the Institute of Technology Assessment, Austrian Academy of Sciences, Vienna, Austria.

Rocco Bellanova is Senior Researcher at the Peace Research Institute Oslo (PRIO) and Visiting Lecturer at the Université Saint-Louis – Brussels (USL-B).

Walter Peissl is Deputy Director of the Institute of Technology Assessment, Austrian Academy of Sciences, Vienna, Austria.

PRIO New Security Studies

Series Editor: J. Peter Burgess, École Normale Supérieure (ENS), Paris

The aim of this book series is to gather state-of-the-art theoretical reflexion and empirical research into a core set of volumes that respond vigorously and dynamically to the new challenges to security scholarship.

Surveillance, Privacy and Security

Citizens' Perspectives

**Edited by Michael Friedewald,
J. Peter Burgess, Johann Čas,
Rocco Bellanova and Walter Peissl**

Contents

Contributors

Rocco Bellanova is Senior Researcher at the Peace Research Institute Oslo (PRIO) and postdoctoral researcher at the Université Saint-Louis – Brussels (USL-B). His research focuses on data-driven security practice, surveillance and data protection.

Peter Bescherer is a Researcher at the International Centre for Ethics in the Sciences and Humanities (IZEW), University of Tübingen. His research examines the role of civic engagement and issues of justice in the context of urban (in)security. His interests lie in the fields of critical theory of society, urban sociology and social movements. A case study on conflicts resulting from different security perceptions in Wuppertal/Germany has been published in *Kritische Justiz* 1/2016.

Tijs van den Broek is a Researcher and Lecturer at the University of Twente in the fields of social media, corporate social responsibility, and social movements. Tijs also coordinates inter-disciplinary research on online campaigns at the University of Twente, for which his team won a Twitter datagrant in 2014. He has worked as a consultant and contract researcher at the non-profit research institute TNO, focusing on the societal implications of ICTs. He obtained a master's degree in both Industrial Engineering and Management and Psychology (with distinction) from the University of Twente, and defended his dissertation 'When Slacktivism Matters' with distinction at the same university.

Jelena Budak is a Senior Research Fellow with the Institute of Economics, Zagreb. She had participated in research projects on various aspects of Croatia's accession to the EU, such as institutional convergence, public sector policies and regional development issues. Her research interests are institutions and applied institutional analysis, and most recent publications are in economics of corruption and privacy issues. She is a lead researcher of the PRICON project.

J. Peter Burgess is a philosopher and political scientist. He is Professor and Chair in Geopolitics of Risk at the École Normale Supérieure, Paris, and Adjunct Professor at the Centre for Advanced Security Theory (CAST), University of Copenhagen, Denmark.

Johann Čas is a Senior Researcher at the Institute of Technology Assessment at the Austrian Academy of Sciences. His current research focus is on data protection and privacy in the information society, privacy-enhancing technologies and their deployment within ambient intelligence, security technologies and health related applications. He co-ordinated the PASR Supporting Activity PRISE and the FP7 project SurPRISE. He is also acting as scientific and ethics evaluator of Horizon 2020 proposals and as ethics advisor of research projects.

Sara Degli Esposti is the Executive Director of the Spanish Information Security Advancement Society (ismsforum.es). Her research focuses on people's privacy expectations and organizational cybersecurity, dataveillance, and data protection practices. Sara has a PhD in Information Management from the Open University (UK), a MSc in Business Administration and Quantitative Methods from Carlos III University (Spain), and a BA in Sociology (Hons) from the University of Trento (Italy).

Jim Dratwa's research and publications address the interconnections between knowledge, values and action. He heads the team tasked with Ethics in Science and New Technologies at the European Commission, he is the Secretary-General of the EC International Dialogue on Bioethics and the EC representative in the international organizations dealing with the ethical implications of science and new technologies. Jim Dratwa holds degrees in physics, philosophy, politics and the life sciences. He received the Fulbright Scholar Award, was Harvard Boas Fellow, Ramón y Cajal Scholar, and was pre- and post-doctoral Fellow at Harvard Law School and Harvard Kennedy School of Government, in the Belfer Center for Science and International Affairs and with the program on Science, Technology, and Society. He has taught at the École des Mines de Paris, Harvard University, and the universities of Brussels, where he is currently based. He is Invited Professor and Global Fellow at the Woodrow Wilson Center, Washington, DC.

Evelien De Pauw is an assistant and a member of the research group Governing and Policing Security (www.gaps-ugent.be), located at the Department of Public Governance, Management and Finance in the Faculty of Economics at Ghent University. Her research examines the influence of the use of information technology on the governance of security. Furthermore she is guest lecturer at the University College Vives in Kortrijk. She has been affiliated to this institution for the past ten years. The focus of her research at the Research Group Society and Security' at Vives University College was the use of technology within police forces and the acceptation of the use of security oriented surveillance technology by citizens.

Prokopios Drogkaris is an NIS Officer at the European Union Agency for Network and Information Security (ENISA) and his interests focus on privacy enhancing technologies, personal data protection and trust. Previously he was involved in several EU-funded research projects and held teaching assistant positions in higher education institutions in Greece.

Michael Friedewald is a Senior Research fellow at the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe Germany and leads the ICT research group. His recent work focuses on privacy and data protection challenges of future and emerging information and communication technologies. He is also working in the field of foresight and technology assessment. He has co-ordinated several FP7 projects including PRESCIENT, SAPIENT and PRISMS. He is co-editor (together with R.J. Pohoryles) of *Privacy and Security in the Digital Age* (Routledge, 2014).

Gloria González Fuster is a Research Professor at the Vrije Universiteit Brussel (VUB). As a member of the Law, Science, Technology and Society (LSTS) Research Group, she investigates legal issues related to fundamental rights, privacy, personal data protection and security, and lectures at VUB's Institute for European Studies (IES). She also lectures on the master's degree course inn Technology and Privacy at the University of Girona and Eticas Research & Consulting.

Serge Gutwirth is currently Vice-Dean and Professor in the Faculty of Law and Criminology of the Vrije Universiteit Brussels (VUB), where he studied law, criminology and also obtained a postgraduate degree in technology and science studies. He directs The Centre for Law, Science, Technology and Society-Research (LSTS) at the VUB. His interests currently include legal issues related to privacy and data protection, and more generically, the role of law amongst other practices such as science, technology, politics, religion and ethics.

Georgios Kolliarakis works at the Institute for Political Science and is a member of the Cluster of Excellence "Normative Orders" at the University of Frankfurt. He conducts research on organizational and strategic aspects of security policies, with a particular focus on non-intended impacts. Georgios is an expert with several International Organisations, and has chaired more than 30 panels at academic and policy conferences. After his Master's studies in Engineering at the Technical University of Athens, and in Political Geography at the University of Bonn, Georgios earned a PhD in International Politics from the University of Munich. His publications include *Politics and Insecurity. Strategies in a changing Security Culture* (in German, Campus, 2014), *Recognition in International Relations* (Palgrave, 2015), and *Anticipation and Wicked Problems in Public Policy. The creation of 'unknown knowns'* (Springer, 2017).

Matthias Leese is a Senior Researcher at the Center for Security Studies (CSS), ETH Zurich. His research interests are broadly located in the fields of critical security studies, surveillance studies, and science and technology studies. He has published in the fields of international political sociology, security dialogue, critical studies on security, criminology and criminal justice, and global society. With Stef Wittendorp, he is the editor of *Security/Mobility: Politics of Movement* (forthcoming 2016, Manchester University Press).

George Leventakis has 22 years of professional experience in the public sector, of which 16 years were spent in in Security Management. He has participated in several national, European and international projects and initiatives regarding physical security of critical infrastructures, border management (land and sea border surveillance), civil protection/homeland security technology and operations.

Marc van Lieshout is Senior Researcher at TNO, the largest Dutch research and technology organization. He is part of the team Digital Society. His work focuses on digital privacy and electronic identities. He is business director of the Privacy & Identity Lab, a collaboration between TNO, Radboud Unversity (Digital Security) and Tilburg University (Tilburg Institute for Law, Technology and Society). He has contributed to several European projects, most recently PRISMS.

Luisa Marin is Assistant Professor of European Union Law at the Centre for European Studies, University of Twente, the Netherlands. Luisa graduated cum laude in Law at the University of Bologna and received her PhD from the University of Verona. Her research interests cover the Area of Freedom, Security and Justice (AFSJ) broadly speaking and her publications focus on the principle of mutual recognition in the AFSJ; on border surveillance, including the deployment of drone technology in border surveillance and its implications; on data protection, Internet and surveillance. Luisa is a member of the Meijers Committee, the Netherlands, and of the European Data Protection Experts Network (EDEN) at Europol.

Francesca Menichelli is a British Academy Postdoctoral Fellow at the Centre for Criminology at the University of Oxford. Her current research looks at the local governance of crime prevention. She has published on CCTV, urban security and public space and, most recently, is one of the editors of *Order and Conflict in Public Space*, published by Routledge in May 2016.

Lilian Mitrou is an Associate Professor at the University of the Aegean/Greece and Visiting Professor at the Athens University of Economics and Business. She has served as a member of the Greek Data Protection Authority (1998–2003) and as Chair of the DAPIX/EU Council (2014). Her experience includes senior consulting and researcher positions in private and public institutions and projects.

Merel Ooms MSc, is a research scientist at TNO with a background in Sociology and policy research. She has contributed to several European and Dutch national projects on topics related to the relationship between technology and human behaviour. Her research activities focus on privacy, sustainable energy and social innovation. On these topics she collaborated in the European FP7 projects PRISMS and SI-DRIVE.

Maria Grazia Porcedda is a PhD candidate in law at the European University Institute (EUI), where she is investigating the relationship between

cybersecurity and privacy rights in EU law. She is also a Research associate within the Centre for Judicial Cooperation at the Robert Schuman Centre for Advanced Studies, where she is contributing to the CharterClick! Project. From 2012 until 2015, Maria Grazia worked as a research associate within the Department of Law of the EUI for the EU-funded FP7 projects SurPRISE and SURVEILLE. Maria Grazia's research interests and publications span the fields of IT law – particularly protection of personal data, cybersecurity and cyber-crime – fundamental rights, the EU AFSJ, empirical legal studies and well-being in the workplace. She is a member of Europol's EDEN. Maria Grazia holds an LLM from the EUI and an MA in International Relations from the University of Bologna.

Vincenzo Pavone is Permanent Research Fellow at the Institute of Public Policies (IPP) of the *Spanish National Research Council* (CSIC). He has a PhD in *Political Science* from the European University Institute (EUI). Vincenzo currently works on the complex relationship between science, technology and politics, with a special focus on neoliberalism and global bio-economies. In his publications he has explored the social and political implications of technologies such as: surveillance-oriented security technologies, transgenics and cis-genics, and assisted reproductive technologies.

Walter Peissl holds a PhD in social sciences. He is Deputy Director of the Institute of Technology Assessment, Austrian Academy of Sciences (ITA/OeAW). He has also lectured at various Austrian universities since 1992. His major research fields include social and economic effects of new ICT and methodological issues of technology assessment. His current focus is on privacy, ICT in health care and participatory methods in technology assessment. He has been involved in or directed projects in virtually all subject areas of the ITA. He has published several books and numerous articles on a wide range of subjects.

Sven Rung is a Junior Researcher at the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe Germany in the ICT research group and a PhD student at the University of Hohenheim. His recent work focuses on the economic impact of future and emerging information and communication technologies.

Edo Rajh is a Senior Research Fellow at the Institute of Economics Zagreb, Croatia and a team member researcher in the PRICON project. His primary research areas are consumer behaviour, market research methodology and measurement scales development. Recent publications are related to his work on survey-based research projects.

Vedran Recher is a Doctoral Researcher at the Institute of Economics, Zagreb, Croatia, Department for Innovation, Business Economics and Business Sectors, and a team member researcher in the PRICON project. His main research interests are applied economics and econometrics, and his recent publications deal principally with privacy issues and economics of crime.

Elvira Santiago–Gómez is an Assistant Lecturer at Complutense University of Madrid. Her current area of expertise is science and technology studies (STS), and her research specifically addresses public engagement with, and public assessment of, science and technology and new approaches for collaborative risk management. With a BA and a PhD in Sociology, her research experience has focused on European security policies and involved extensive social research around risk controversies and risk management related to safety and security in the EU.

Bernadette Somody is a constitutional lawyer, and a Senior Lecturer at the Constitutional Law Department of the Faculty of Law, Eotvos Lorand University (Budapest), and a Researcher at the Eotvos Karoly Policy Institute. Her research interests centre on the mechanisms and methods of fundamental rights protection. Her PhD thesis was on ombudsman institutions. She formerly worked for the Hungarian Parliamentary Commissioner for Fundamental Rights, and at the Office of the Commissioner for Educational Rights.

Stefan Strauß is a Researcher at the Institute of Technology Assessment (ITA) at the Austrian Academy of Sciences in Vienna. In his research he explores the interplay between information technology and society with particular focus on the related impacts on political processes, identity construction, security, surveillance and privacy. Further research interests include information and computer ethics and the philosophy of information. He has been involved in different European research projects including those on privacy, security and surveillance, cloud computing, e–democracy and identity, critical infrastructures. He has authored a number of publications on ICT-supported participation, digital identity, security and privacy. His most recent papers deal with the implications of big data.

Máté Dániel Szabó is a lawyer specializing in the protection of fundamental rights. His PhD thesis focused on the constitutional borders of the informational power of the state. Currently he is the director of programs at the Hungarian Civil Liberties Union, a leading Hungarian human rights NGO. Previously he was the director of Eotvos Karoly Policy Institute, and a Lecturer at the University of Miskolc. He formerly served in the staff of the Hungarian Commissioner for Data Protection and Freedom of Information, and in the Office of the Commissioner for Educational Rights.

Iván Székely is a social informatist and an internationally known expert in the multidisciplinary fields of data protection and freedom of information. He was formally Chief Counsellor of the Hungarian Data Protection Ombudsman, he is currently Senior Research Fellow at the Vera and Donald Blinken Open Society Archives at Central European University, an Associate Professor at the Budapest University of Technology and Economics, and an Advisory Board Member at the Eotvos Karoly Policy Institute. His research interests and publications are focused on information autonomy, openness and secrecy, privacy, identity, surveillance and resilience, memory and forgetting, and archivistics.

Dimitris Tsapogas is a Postdoctoral Researcher at the Department of Computer Science of the University of Oxford and the executive director of the non-profit association Critical Citizens. He has previously worked as a PhD researcher at the University of Vienna where he completed his thesis, which explored the relationship between electronic surveillance and political participation. Dimitris' research has been presented at numerous international conferences and he has published on surveillance and citizenship, privacy and surveillance attitudes, privacy and data protection policies, and digital citizenship. He has also taught related topics at the University of Vienna and elsewhere. His personal website is www.tsapogas.info

Hans Vermeersch has a PhD in Sociology and is associated with the research groups Security and Society and Youth and Society at the Centre for Social Innovation at Vives University College (Kortrijk, Belgium). His research focuses on youth, gender, risk-taking behaviour and security-related attitudes.

Foreword

Ethical experimentations of security and surveillance as an inquiry into the Open Beta Society

Jim Dratwa

Once upon a time this philosopher, this adviser in the castle, sent a message to a wise man asking him to come to his country, far far away. The philosopher was convening a grand gathering on the ethics of security and surveillance technologies and he was hoping the wise man would talk to all of those gathered.

   But this was how the man responded:

> Let me first thank you for your kind invitation. As you know, I am very sensitive to the problem of Security Technologies to which your Group is devoting its attention.
>
> But precisely for that reason I am a little embarrassed by your invitation. I am firmly convinced that, as far as these technologies are concerned, the only possible ethical attitude is to refuse them completely, as they are inhuman and barbarous, and, moreover, are not intended to attain the goal they pretend to aim to. And – and this should particularly concern your commission – they are acting on western democracies as a power that, establishing a kind of perpetual state of exception, is progressively evacuating any real democracy.
>
> This is why I am hesitating and cannot accept your invitation. Ethics should never be conceived as something that accepts *de facto* an inhuman situation and tries to establish juridical limits to it.
>
> Yours sincerely,

And so the philosopher gave a similarly heartfelt answer:

> Thank you very much for your response. To tell you quite frankly, that is precisely why I feel it is vital that you come. I have conveyed some of those pivotal concepts such as that of state of exception in the work of the Group, and indeed several of its members are starting to experience the embarrassment and hesitation which you justifiably point out.
>
> There is no 'participation trap' in this setting and I do believe that your presence and contribution to the reflection could do more good than a decision to abstain.
>
> In any case I am deeply grateful that you gave me the chance of this generative hiatus of critique and reflexivity.

I hope that you will be able to come to Brussels to give this chance to all the others too.

With all best wishes,

The wise man came.

On that day, in that faraway land, that wisdom was shared – with one and all.

A story within a story. Caution and care. Critique and ambivalence.

That story starts with the letter that was sent by the President of the European Commission to the European Group on Ethics in Science and New Technologies, asking it to prepare an Opinion on the ethical implications of security and surveillance technologies.

Now as the group was developing the report, the revelations of Edward Snowden intervened and emphasized how important a reorganization and reinterpretation of our approach to security and surveillance is. Indeed the predicament of data flows and surveillance activities thrown into sharp relief by these revelations and their aftermath forms part of the evolving backdrop against which that Opinion is set.

It is in this context that I joined the invaluable research dynamics, practices and practitioners at the origin of the present book.

In the context of this collective thought experiment, of this sharing and crafting of perplexities, arguments and analyses, several subversive insights and transformative questions shone out to me: the unpacking of security, in particular in relation to notions of risk, commodification, social contract and the state; the scrutinizing and surpassing of trade-off framings; the reflection on the role – indeed on the embedding and instrumentalization – of ethical, political, social scientific engagement; the exploration of all the above as an experimentation of the polity (of the European project) putting identity and citizenship at stake. I have addressed these elsewhere.[1] To my delight, but not to my surprise, the book, as a coherent research endeavour, further develops, takes up and compellingly analyses many important facets of these issues.

And then there is perhaps the most perplexing question or shining beacon: citizens. That is to say, the inquiry into the evolving assemblages entangling the citizen, the state and the making of the world. Such is the perspective that I will trace and probe in this short exploratory piece: first, by considering the bigger picture of what I term here the Open Beta Society; second, with crisp stories of interplay between empowerment and exploitation; third, by developing these tensions through a closer scrutiny of surveillance and citizen veillance, and fourth, by examining the ethical issues at the nexus between citizens and surveillance and developments in new health technologies. All the while and as initiated from the outset, this short piece pursues an exploration of the role of ethical questioning and of the role of stories therein. True to form, the conclusion sheds summative and formative light on these.

We are witnessing profound shifts in the ways knowledge and innovation are produced, processed and legitimated. The wider public is increasingly involved in

research and innovation across a multitude of roles and functions, a change accompanied and reinforced by parallel shifts in conceptualizations and institutionalizations of the scientific endeavour. Indeed these transformations are notably striking in the area of health, which affords peculiar configurations of our surveillance societies.

These new forms of life and socio-technical arrangements, these new ways to exercise – individually and collectively – citizenship and creativity and rights, hold tremendous transformative potential, and indeed tremendous entanglements of empowerment and exploitation. That is what this preface takes on, nurturing resources of recalcitrance and reconstruction.

The Open Beta Society: work in progress

What would happen if computer programs (consider gaming software for example) were released while still containing bugs, shortcomings and faults, issues which may still cause crashes or losses, so that users would deal with them in the field and report those faults so that in turn they could be addressed? In the software development and release life cycle, this is called the 'Beta' stage.

Perhaps we should pay to get this at this stage or rather wait for the 'real thing'. There will be patches and updates anyway. Or perhaps the beta-users themselves should be recompensed for their development work.

Now what about public policies? Should they trade in certainty, premised on scientific certitude (and its particular articulation of definite knowledge with definite action) to provide legal certainty or should they be tentative and unsettled, amenable to learning and change, to wising up.

What about genetically modified organisms (GMOs)? How and when should they be deliberated and released? How to cultivate learning and change with them. And then what about medicinal drugs, security technologies, and so many other entities?

In interesting ways, such is our world and age, evolving in a state of variously open (and variously perpetual) Beta.

Key features of our 'Open Beta Society' are the ambivalence of participation (strained between empowerment and instrumentalization or subjection), the ambivalence of sharing (strained between the ideals of the commons and new forms of appropriation, commodification and exploitation), the ambivalence of learning (confronted with lip service; with new cultures of obsolescence and oblivion; with the ratcheting up of the new) and the ambivalence of reflexivity (strained between the opening up of alternative imaginaries and the ultimate 'we saw it coming, we thought of it' validation/normalization of dystopian transformations; strained between externalization and internalization, with the outsourcing and embedding – or swallowing whole – of reflexivity).

The developments which we are confronted with also call upon the notion of 'narratives society' or 'story-telling society' as the melding and spinning of words and worlds plays such a decisive part in the ontology – the ontological diplomacy – of individuals as well as institutions.[2]

At the close of this section, the notion of 'Society society' is a useful marker with regard to the demiurgic act of naming at the heart of (social) scientific creativeness.

Who will get to tell the story? Who invites participation? Who divides the labour in the collective experiment and distributes the roles (experimenter, experimentee; vigil or vigilante; watcher, watched, watcher watched), or indeed what stories get told and how? In other words, referring to the developments above, through which agendas, processes and practices do certain softwares and policies and GMOs and drones and medicines come to make up the world in which we live together?

Figments and ferments: exploitation and empowerment

It is a peculiar feature of the set of socio-technical transformations which we address here that they challenge at one and the same time our understandings of democracy and of knowledge production (of political representation and of scientific representation).

This key dimension is recounted in a different way in the short evocative sparks that follow, which also draw attention to interplays between public and private, individual and collective, free and shared and owned.

In the crispest terms this means: on the one hand, dynamics of commodification and exploitation, on the other, dynamics of sharing and empowerment hand in hand.

Imagine that you go to a pastry shop (oh, the sweet smell of freshly baked loaves) and, just when you are about to buy your daily bread, you are asked to give your phone number. And your geolocation, current and future, and, while we are at it, the names and contact details of all the other people you know. Well, you want the bread, right? There is no other way to get it. But the good news is that there is no need to open your purse. You can even have it for 'free'.

All the while there is an underpinning question to be mindful of: What world? Such is the nagging question. Why and how this world or others? Or in a more operational and ambitious form: in what world do we want to live together? How do we compose *that* together?

This nagging question also opens two other paths of questioning, blazed in the story with which this preface started.

First, how can we possibly accept this, the world as it is? How can we simply click on the 'I agree' button, every morning, every instant. What is dignity without indignation? As a case in point, how can we resist and ju-jitsu the security and surveillance economy into alternative futures to invent together?

Second, is engaging in critique already inevitably a form of embracing, of condoning? And further, can we not only deconstruct and critique, but imagine and construct alternative futures?

Think back to the citizens of the city-state of Athens assembled for the Dionysia, the Gutenberg Bible (as well as Shen Kuo and Bi Sheng), the advent of the movie theatre, then of the home television, of the personal computer, of the internet. Now imagine a website or app (idiotis-box, goggle, you-are-the-tube, self-image, show-business, broad-cast, do-unto-others, pan-opticon, multi-plex) allowing users to

upload, view, search and share videos and other content. Revolutionary empowerment (revolution here in the sense of a Kantian Copernican revolution in view of the trajectories traced above, i.e. placing the subject centre-stage) organically intertwined with dynamics of capitalistic exploitation (network externalities, tragicomedy of the commons, Matthew effects) and subjection, as well as with the rise of a culture of the self and the selfie, personal development, sharing and crowdsourcing, cultures of trust and distrust, pursuit of attention, ubiquitous connectedness and surveillance, mobile and semidetached – indeed 'cephalophoric' (Serres 2001, 2012) i.e. head on the sleeve or in the cloud – smartness.

Before we delve deeper, these story stems – while not developed here – also call attention to the fact that the story we weave has many more strands (and indeed to the fact that not all strands will be weaved). We will now more closely scrutinize surveillance and citizen veillance; citizen veillance, as a reference to forms of citizen participation or citizen science in the broad area of – even as a counterpoint to – surveillance, stands in the in-between. On the fence. Here: the feats and stories of liberation and empowerment, which we want to witness, to construct, to spread. There: the systems of exploitation to critique or deconstruct and the traps of instrumentalization to avert or defuse.

Unpacking surveillance and citizens' veillance

The notion of surveillance comes to us with a rich and textured layering of meaning. Its common definition is that of close observation, especially the act of carefully watching a suspected spy or criminal or a place where an incident may occur.

It comes from the French verb *surveiller* 'oversee, watch' (sixteenth century), from *sur-* 'over' and *veiller* 'to watch', from Latin *vigilare*, from *vigil* 'watchful'. Interestingly, 'surveiller' carried with it from the start a tension between the meanings of watching over, of taking care of, and of suspicion and control. It also comprised from the start the complementary notion of watching over oneself and one's own behaviour.

'Surveillance' is first attested in 1768, in an article (in the economic journal *Éphémérides du citoyen*) pertaining to the role of the police in marketplaces, drawing together individuals and the state, public and private interests, law and law enforcement. It is also worthy of note that the word surveillance came to English from the Reign of Terror in France: during the French Revolution 'surveillance committees' were formed in every French municipality by order of the Convention – pursuant to a law of 21 March 1793 – to monitor the actions and movements of all foreigners, dissidents and suspect persons, and to deliver certificates of citizenship.

What do we want to secure and surveil? Why and how, and at what price? What do we want to make or keep safe? And who is in the 'we'?

This also traces the early connection between surveillance and citizenship, indeed between empowerment, participation and subjection.

Having given heed above to the tensions crisscrossing our age (indeed our beta/story/learning/experimental/surveillance society), it is important to reflect on the concept of *citizen veillance* as such.

What is at stake in our defining it as referring to 'activities performed by citizens broadly and primarily to produce socially useful, empowering knowledge – rather than as a means of control. Therefore, the working definition proposed for veillance is a condition of citizens' cognitive alertness and knowledge production being proactively oriented towards the protection of common goods'? (Tallacchini *et al.* 2014).[3] Could this move be a bracketing out of the unwanted, of the unintended, of that which we do not wish to think of (*Ungedachte* or *Nichtwissen*), nipping these possibles in the bud at a definitional conceptual level?

This bracketing out echoes Max Weber's own presentation of his ethics of responsibility, with its treatment of desired and foreseeable consequences (Weber 1995: 172), proxies for the unending strands of ins and outs, of actions and risks and consequences. And here lies a seminal ambiguity in the thought of Weber on his *Verantwortungsethik*, characterized by the responsibility for the consequences of one's actions. Translations published in English and French cover it up, but it is a crucial moment of explicit hesitation, of bracketing out. For in fact he writes 'die (voraussehbaren) Folgen' (answer for the (foreseeable) consequences of one's actions), perhaps dampening but certainly not addressing the volatile foreseeability upon which this hinges.

We should be mindful of two shortcomings inherent in this definition of citizen veillance.

The first one, as Weber discretely alerts us to, with his own bracketing out, consists in neglecting or obfuscating the unintended and unforeseen (or more crucially still, the question of how futures are made).

The second one consists in the mereological fallacy of presenting or considering a part (of a set of activities, putative goals, or consequences) as the whole (as in the image of cultivating the wheat without the chaff – the double sense of the term 'wheat' here underscoring this synecdoche).

This is not merely a theoretical consideration but a particularly thorny practical one, as a key feature of our surveillance societies, however named, is precisely the ambiguity/undecidability – double entendre or doublethink – between (social) control and empowerment.

Three further considerations enrich the aforementioned conceptual contours of citizen veillance.

First, the dialectics of means and ends (cf. 'rather than as a means of control' above; 'guns don't kill people, people do'), extending from notions of axiological neutrality of technologies to studies into how the research agenda is shaped and into how users reconfigure technological innovations, through to our above discussion of intended and unintended consequences.

Second, the opening as to what is 'socially useful' and 'empowering', attached to the individual and collective characterization of the good life and the common good, which cannot simply be posited (or left out) a priori. This further opens to questions about the means to determine – in diverse groups, institutions or societies – the socially binding delineation of what is true and of what is good (Jasanoff 2005, Dratwa 2004 and 2014, Latour 2004 and 2012).

Third and overarchingly, the narrative of citizen veillance calls upon all of us to reflect on the choice of what stories we wish to tell as we probe into the societal

and ethical implications of science and new technologies. Among all shades and strands, will we favour cautionary tales, foreboding stories of subjection and alienation, irenic songs, and/or stories of resistance and possibilities?

Stories can also be technologies of resistance and emancipation, the commons and the transitions, technologies of choice, of capability, of justice and solidarity. Stories are also technologies to hack and make.

Healthy scepticism

The nexus between citizens and surveillance (including the involvement of the wider public in the research endeavour) and developments in health, including new health technologies, gives rise to several areas of tensions.

Aided by the proliferation of digital technologies, citizen involvement initiatives in health are thriving. Indeed, health appears to offer fertile ground for fruitful citizen engagement, being a subject high on the public's list of concerns, and an area in which each and every individual has a particularly personal stake. Indeed, the contention that the knowledge and perspectives of non-experts (e.g. patients) can enrich the global understanding of scientific problems (e.g. illness, wellbeing) may be less contentious in the domain of health than in other areas. That notwithstanding, the consequences and future implications of growing citizen involvement in healthcare are complex and potentially transformational. Reconfigurations in the doctor/patient relationship, evolving patient autonomy, and resulting tensions between expert medical knowledge and patient's experiential knowledge trace a blurring of established health categories and a by-passing of twentieth-century institutional arrangements around health and medical care.

Beyond challenges to medical practices and institutions, citizen involvement challenges – and thus can enrich – the notion of 'scientific method' itself, and its mechanisms and standards (including 'research integrity'). Furthermore, in societies premised on the exercise of citizenship and celebrating ideals of democracy, these forms of engagement – notably in the context of citizen veillance – can come as a challenge or enrichment to existing political forms and power relations.

Yet as a counterpoint, calls for democratization, participation and public debate cannot ignore the study (and history) of the involvement and disqualification of the public – be it framed as 'citizen', 'witness', 'lay', 'ignorant' or otherwise – in matters of science as well as of politics, including its disqualification under the head of democratization (Shapin and Schaffer 1985, Irwin and Wynne 1996, Latour 1999, Jasanoff 2005, Dratwa 2011b).

Another important dimension to be attentive to is that these evolutions may also change our understandings of the normal and abnormal, of health and illness (beyond a narrow medicalized understanding), of wellbeing and the good life. Furthermore, these new forms of engagement with health and health technologies may challenge the notion that the body is a given, a bounded and fixed entity.

Diverse methods of enhancement, gene editing, personalized/precision/stratified medicine, electronic and mobile health, and the strands of the 'quantified self' and 'body hacking' movements are significant in that regard.

These evolving practices and technologies also trace evolving notions of the self, identity and the relationship with the body, life and the question of our common humanity. These are illustrative of – and integral to – the biopolitical shifts (i.e. in the crispest possible form: enhanced empowerment, enhanced subjection, enhanced ambivalence) of our Open Beta Society as examined above.

Conclusion

The above issues open to a cognate set of ethical tensions, but considered from the perspective of justice and of solidarity (including matters of access, inequality and fairness).

The key dialectics in this regard are between individual and collective, between national and transnational (e.g. European or wider afield), between public and private, while the core questions are attached to this: where do we place the boundaries of our 'imagined community' in which solidarity is located?

Yet taking a step back with regard to solidarity, is there a tension here between the respect for privacy and calls for solidarity? Is there a shift or twisting of autonomy away from considerations of privacy and consent (explicit informed consent with a possibility not to consent) towards an imperative of solidarity ('for the greater good' of the many or of the few)? Is ethical normativity itself at the risk of accompanying or facilitating that form of twisting?

The hegemonic framing to contend with in this set of policy areas is that of the 'trade-off narratives', characterizing certain issues or policy dossiers as matters of a trade-off between competitiveness and human rights, between security and freedom (see EGE 2014 for the unpacking of these trade-off narratives).

Against the backdrop of data-intensive innovations (here the possibility to capitalize on growing health data availability to generate medical innovation) being held up as the source of the next medical 'great leap forward', controversies surrounding the confidentiality of electronic patient records, legal challenges in the context of the Apple watch launch, and evidence of the systematic breach of data protection rules through smart phone apps underscore the privacy, security and confidentiality concerns regarding citizen involvement.

Undercutting the trade-off frames are questions of risks, costs, benefits, and the unequal distribution thereof. If personal data is the 'new oil' and 'new infrastructure' heralding a 'new industrial revolution' and a 'new scientific revolution', then who owns the data? And who owns – or shares in – what comes out of it?

With data conceived of as a 'tradeable good', are citizens entitled to gain (financially or otherwise) from providing their data? At one end of this logic are initiatives such as MyHealthBook, a company offering financial incentives in exchange for citizens' health data. Others do not even offer such acknowledgement and compensation. Yet, given the considerable wealth generated by companies from repositories of data derived from individuals (sometimes without their knowledge or consent), should greater reflection not be paid to allowing people to share in the impacts of their contributions?

More widely, is a re-conceptualization of ownership-sharing and benefit-

sharing required when these pertain to knowledge and innovation? As a telling example, when a pharmaceutical company discovers a new drug, should the data surrounding the production of that medication be considered the sole property of the company concerned or a wider public good (given the shared investment in that innovation: patients who participated in research trials, researchers, education and training systems, etc.)?

As examined above, these 'openings' undergird the promise of open innovation and open science, of citizen science as well as citizen veillance.

As one of the core tensions they comprise, citizen veillance and other involvement initiatives can either subsume or aim to counterbalance the notion of lay people as research 'subjects' – a resource from which data and samples can be extracted but often with no access to the ins and outs of the endeavour. This raises the question: to what extent can participants be genuine public policy and research 'partners'? Or indeed do some such initiatives normalize a situation in which everyone is a potential research subject (but without the corresponding traditional checks and safeguards, such as the framework of consent as a subset of socio-technical arrangements giving shape to values of justice, solidarity, dignity and autonomy).

Beyond the above references to solidarity and other ethical principles, the role played by institutionalized ethics in these matters is a delicate one.

The same way that given technologies can ('by design', 'by default') obfuscate or confiscate ethical reflexivity and justification of choices, algorithmically and materially black-boxing them away, removing them from most people's intervention and understanding, ethics councils and cognate bodies must themselves remain vigilant, indeed fully aware of the risk of ethical confiscation that they represent, as well as of the risk they run of their own instrumentalization in these processes of normalization pertaining to new technologies.[4]

If our collective experimentations are changing – in the digital and genetic age, in the era of big data, in the Open Beta Society – then we need to invest the necessary efforts to develop and revise the protocols and rules of methods that will allow for reframing, reconsideration, deliberation, experience-drawing and cumulative learning to make the most of our collective experimentations.

In closing, the ethical implications which surveillance, privacy and security assemblages call upon us to pay heed to are those of our own – individual and collective – choices, of our own research agenda, of what we share and how, including the conceptual frames we resort to. What stories will get told and how?

Notes

1   Regarding these questions and reframing moves, see in turn Dratwa (2007), EGE (2014), Dratwa (2011a), BEPA (2014), Jasanoff (2011) and Dratwa and Pauwels (2015).
2   It should also be noted that this 'Open Beta Society', alongside pervasive characterizations of the information society and the knowledge society, shares features with the developments of the risk society (Beck 1992 and 2009, Giddens 1990 and 2005); the test society (Callon *et al.* 2007); the experimental society (Haworth 1960,

Dratwa 2002); and indeed the surveillance society (Marx 1985, Lyon 1988, Ball *et al.* 2012) and control society (Razac 2008 alongside the work of Deleuze and Foucault).

3   This was part of the excellent framing of the conference convened by the European Commission's Joint Research Centre on 'Emerging ICT for Citizens' Veillance' at which my keynote address was given on 20 March 2014.

4   I gratefully acknowledge the galvanizing collaboration and exchanges with Giorgio Agamben on these difficult issues (personal communications, 15 July 2013, 18–19 September 2013, 24 June 2014; see also Agamben 2000), also referred to at the inception of this preface. With regard to the normalizing role of technologies and to the normalizing role of ethics committees as technologies of governance, see EGE (2014: 87–88). Complementary forms of capture and entrapment of ethical reflexivity are discussed in Dratwa (2011b, 2014).

References

Agamben, G. (1993) *The Coming Community*, Minneapolis, MN: University of Minnesota Press.

Agamben, G. (2000) *Means without Ends: Notes on Politics*, Minneapolis, MN: University of Minnesota Press.

Ball, K., Haggerty, K.D. and Lyon, D. (eds) (2012) *Routledge Handbook of Surveillance Studies*, London: Routledge.

Barry, A. (2001) *Political Machines: Governing a Technological Society*, London: The Athlone Press.

Beck, U. (1992) *Risk Society: Towards a New Modernity*, London: Sage

Beck, U. (2009) *World at Risk*, Cambridge: Polity Press.

BEPA (Bureau of European Policy Advisers, Directorate-General for Justice of the European Commission) (2014) 'Fundamental Rights and Ethics in the Context of 'Open, Data-driven and People-focused way of doing Research and Innovation' (Science 2.0)', Brussels.

Callon, M., Millo, Y. and Muniesa, F. (eds) (2007) *Market Devices*, Oxford: Blackwell.

Dewey, J. (1927) *The Public and its Problems*, Athens, OH: Swallow Press.

Dewey, J. (1938) *Logic: The Theory of Inquiry*, New York: Henry Holt and Company.

Dratwa, J. (2002) 'Taking Risks with the Precautionary Principle: Food (and the Environment) for Thought at the European Commission', *Journal of Environmental Policy and Planning*, 4: 197–213.

Dratwa, J. (2004) 'Social learning at the European Commission and the Codex Alimentarius', in Reinalda B. and Verbeek B. (eds) *Decision Making within International Organizations*, London and New York: Routledge.

Dratwa, J. (2007) 'Risque, Rixe, Rhizome: Guerre et Paix avec l'Analyse des Risques et les Organisations Internationales', in Kermisch C. and Hottois G. (eds) *Techniques et Philosophies des Risques*, Paris: Vrin.

Dratwa, J. (2011a) 'Representing Europe with the Precautionary Principle', in: Jasanoff, S. (ed.) *Reframing Rights: Bioconstitutionalism in the Genetic Age*, Cambridge, MA and London: MIT Press.

Dratwa, J. (2011b) 'Europe's Collective experiment with Nanotechnologies as a Construction of Possible Futures: Political and Ethical Stakes', in Kermisch C. and Pinsart M.-G. (eds), *Nanotechnologies: towards a transformation of ethics?*, Brussels: EME Editions.

Dratwa, J. (2014) 'How Values Come to Matter at the European Commission: Ethical Experimentations of Europe', *Politique Européenne*, 45: 86–121.

Dratwa, J. and Pauwels, E. (2015) 'How Identity Evolves in the Age of Genetic Imperialism', *Scientific American*, 13 March 2015.

EGE (European Group on Ethics in Science and New Technologies) (2014) *Ethics of Security and Surveillance Technologies*, Opinion no. 28. http://ec.europa.eu/archives/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf (last accessed 7 November 2016).

Giddens, A. (1990) *The Consequences of Modernity*, Cambridge: Polity.

Giddens, A. (ed.) (2005) *The New Egalitarianism*, Cambridge: Polity.

Haworth, L. L. (1960) 'The Experimental Society: Dewey and Jordan', *Ethics* 71: 27–40.

Irwin, A. and Wynne, B. (eds) (1996) *Misunderstanding Science? The Public Reconstruction of Science and Technology*, Cambridge: Cambridge University Press.

Jasanoff, S. (2005) *Designs on Nature. Science and Democracy in Europe and the United States*, Princeton, NJ: Princeton University Press.

Jasanoff, S. (2011) 'Rewriting Life, Reframing Rights' in Jasanoff S. (ed.), *Reframing Rights: Bioconstitutionalism in the Genetic Age*, Cambridge, MA and London: MIT Press.

Latour, B. (1999) *Politiques de la Nature*, Paris: La Découverte.

Latour, B. (2004) 'From "Matters of Facts" to "States of Affairs"': Which Protocol for the New Collective Experiments?', in Schmindgen H., Geimer P. and Dierig S. (eds) *Kultur im Experiment – Experimental Cultures*, Berlin: Kulturverlag Kadmos.

Latour, B. (2012) *Enquête sur les modes d'existence: une anthropologie des Modernes*, Paris: La Découverte.

Lyon, D. (1988) *The Information Society: Issues and Illusions*. Cambridge: Polity Press.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*, Cambridge: Polity Press.

Marx, G. T. (1985) 'The Surveillance Society: The Threat of 1984-style Techniques', *The Futurist*, June: 21–26.

Muldur, U., Corvers, F., Delanghe, H., Dratwa, J., Heimberger, D., Sloan, B. and Vanslembrouck, S. (2007) *A New Deal: The Design and Impacts of the 7th Framework Programme*, The Hague and New York: Springer.

Razac, O. (2008) *Avec Foucault, après Foucault. Disséquer la société de contrôle*, Paris: L'Harmattan.

Serres, M. (2001) *Hominescence*, Paris: Éditions Le Pommier.

Serres, M. (2012) *Petite Poucette*, Paris: Éditions Le Pommier.

Shapin, S. and Schaffer, S. (1985) *Leviathan and the Air-Pump*, Princeton, NJ: Princeton University Press.

Stengers, I. (1997) *Cosmopolitiques*, Paris: La Découverte.

Strauss, L. (1953) *Natural Right and History*, Chicago, IL: University of Chicago Press.

Tallacchini, M., P. Boucher and S. Nascimento (2014) *Emerging ICT for Citizens' Veillance: Theoretical and Practical Insights* (JRC Science and Policy Reports EUR 26809 EN). Luxembourg: Publications Office of the European Union.

Weber, M. (1995) [1919] *Le savant et le politique*, Paris: Plon.

Wynne, B. (2001) 'Creating Public Alienation: Expert Cultures of Risk and Ethics on GMOs', *Science as Culture*, 10: 445–481.

Wynne, B., Felt, U., Callon, M., Eduarda Gonçalves, M., Jasanoff, S., Jepsen, M., Joly, P.-B., Konopasek, Z., May, S., Neubauer, C., Rip, A., Siune, K., Stirling, A. and Tallacchini, M. (2007) *Taking European Knowledge Society Seriously*, Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, Luxembourg: Office for Official Publications of the European Communities.

Introduction

Surveillance, privacy and security

Johann Čas, Rocco Bellanova, J. Peter Burgess,
Michael Friedewald and Walter Peissl

Everyday surveillance is endemic to modern societies.

(David Lyon[1])

I am disturbed by how states abuse laws on internet access. I am concerned that surveillance programmes are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly-tailored use of surveillance. But that is all the more reason to safeguard human rights and fundamental freedoms.

(Ban Ki-moon[2])

Is mass–surveillance the new normal?

In modern societies, surveillance is progressively emerging as a key governing technique of state authorities, corporations and individuals: 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction' (Lyon, 2007, p. 14). The 'Snowden revelations' of mass-surveillance programmes brought into the light of day the ever-increasing and far-reaching capabilities of digital surveillance technologies (Greenwald, 2014). The lack of serious reactions to these activities shows that the political will to implement digital surveillance technologies appears to be an unbroken trend. Moreover, the massive accumulation and processing of digital data is not limited to secret programs. For some time, and especially in the framework of the 'War on Terror', public authorities, governments and supranational institutions have openly advocated the need to deploy surveillance technologies for the sake of security (Amoore and De Goede, 2005).

The underlying rationale supporting data-driven security practice is that the harvesting of personal and meta-data would permit authorities to intervene in a targeted and intelligence-led fashion: focusing their attention and their resources on emerging threats and possibly disrupting them before their very occurrence. This "dream of targeted governance" (Valverde and Mopas, 2004, p. 233) fosters the ambition of security actors to increase their capacity to collect and process large data-sets; the capability to exploit *big data* (Andrejevic and Gates, 2014) would permit them to garner information about the whereabouts, behaviours and

relations of people, and ultimately sort out risky individuals (Lyon, 2014). For example, in 2016 the European Union (EU) institutions have adopted the 'EU PNR scheme': a pan-European programme to collect, store, exchange and process passenger information (Directive (EU) 2016/681). This measure is highly representative of the progressive shift of security practice towards data-driven governance: massive amounts of information generated in commercial settings are syphoned and processed for security purposes (Bellanova and Duez, 2012). Inspired by a similar system run by United States (U.S.) authorities since the late 1990s, it allows national authorities to profile travellers (Leese, 2014) and has been the object of nearly a decade of political debates (Huijboom and Bodea, 2015).

This drive towards a security governance based on digital mass-surveillance raises, however, several issues: Are the resulting infringements of privacy and other human rights compatible with the Charter of Fundamental Rights of the European Union or the EU data protection framework and the values of democratic societies? Does security necessarily depend upon mass-surveillance? Are there alternative ways to frame security? Do surveillance technologies address the most pressing security needs, and if so, are they the most efficient means to do so? In other words, the promotion and adoption by state authorities of mass-surveillance technologies invites us to ask again if the argument of increasing security at the cost of civil liberties is acceptable, and thus to call into question the very idea that this would be necessary to preserve democratic societies.

Bringing citizens' perspectives to the forefront of debates

These questions about surveillance, privacy and security are not new and have already often brought into debate. For example, in the aftermath of the Snowden revelations, experts, policy makers, security professionals and advocates have discussed and argued again and again about the effects of surveillance technologies on those who are governed and on democracy altogether. Yet, citizens' perspectives are rarely integrated into policy-making and academic debates – and often only through reference to Eurobarometer inquiries or rhetorical moves of security professionals or activists to legitimate their speaking position (Monahan, 2006, Goold, 2010, Pavone and Degli Esposti, 2012).

Three FP7 Security Research projects (PRISMS, PACT and SurPRISE) have addressed these and related questions by putting the perspective of European citizens at the very centre of the research focus. The main aims of the projects were to better understand the relation between surveillance, security and privacy, to inform policy-making and to support decision making with the gained insights. The revelation of practically unlimited surveillance activities of the NSA (Greenwald, 2014), the rejection of the Data Retention Directive by the Court of Justice of the European Union (Lynskey, 2014) or the recently adopted Opinion on Ethics of Security and Surveillance Technologies by the European Group on Ethics in Science and New Technologies to the European Commission (2014) were unambiguous signals that a more thorough understanding of the tensions triggered by the introduction of mass-surveillance is urgently needed.

In November 2014 the projects convened a scientific event[3] to discuss these and other questions related to 'Citizens' Perspectives on Surveillance, Security and Privacy', which collected contributions from the research projects, high level keynote lectures, and presentations from researchers working on similar and related topics. This volume is based on selected contributions to this conference, aiming to present a comprehensive picture of the state of research. Additional authors have been invited in order to round off the content of the book.

Focusing on the citizens' perspective on surveillance, privacy and security, this volume contributes new insights from empirical research and theoretical analysis to a debate, characterized by evident tendencies to provide simplified answers to apparently multidimensional and correspondingly complex societal issues like security. These tendencies are not specifically pertinent to security; on the contrary, it appears that the more complaints about increasing complexity dominate mainstream thinking, the more there is an inclination to seek salvation in predominately simple policy responses. Security represents a prototypical showcase in this context, characterized by an unjustified focusing on particular aspects of complex problems, superseding analyses by one-dimensional perceptions, and proposing simple, politically oriented solutions, presented in an either-or, extortionist fashion, refusing the consideration or even existence of other options (Berling and Bueger, 2015). This post-fact, counter-rationality intensifies the danger of limiting the role of open debate and pluralistic analysis. Without an open methodological debate, scientific discourses fall prey to narratives of exclusion and repression.

Challenging too linear views on the relations between security and privacy

The ever-increasing role of security in political debates is paralleled by the narrowing of the meaning of security. The many dimensions entailed in concepts of *human* or *societal* security (Kaufmann, 1973), embracing components like economic and social conditions, health, nutrition, political and natural environment or fundamental freedoms, seem largely side-lined in policy and media debates about security. It is rather discourses of organized crime, terrorism and border security which largely dominate current security policies and media coverage of security problems. The uptake by state authorities of mass-surveillance technologies goes hand-in-hand with a more or less explicit reformulation of the classic notion of *national* security, now less centred on the defence of a given territory and more concentrated on profiling as the ultimate protection of the state and its citizenship (Bigo, 2006). The everyday practice of digital mass-surveillance is very far from traditional descriptions of state security, and its securitizing action heavily relies on transnational cooperation among security professionals (Bauman *et al.*, 2014) and diverse private-public surveillance nexuses (Hayes and Vermeulen, 2012). Moreover, the predominant perspective on security is largely reduced to debates on how to find the right balance between privacy and security (Neocleous, 2007), which inherently assumes and fosters the idea that data-driven surveillance is the sole solution to any threats.

This book tries to further nurture a debate that challenges the assumption that more security requires less privacy, and that more surveillance necessarily implies more security (Bigo *et al.*, 2008). A key motivation is the wish to incorporate into new analyses the perspectives, attitudes and preferences of citizens, understood as being the main beneficiaries of security measures, while at the same time potential and actual targets of mass-surveillance programmes conducted in the name of responding to imminent security threats. In the dominant political discourse, citizens are expected to accept the concentration on this specific framing of security and to support the implementation of new surveillance measures and technologies, even though such measures result in intrusions into privacy or infringements of other fundamental rights.

The protection of privacy will remain a challenging task in the face of the technical progress in information and communication technologies already made and expected in the near future. In particular, digital technologies not only make surveillance in a strict sense more capable and intrusive, but they also blur the boundaries between traditional surveillance devices and digital apparatuses that we use in everyday life and that are increasingly embedded in the environments we inhabit. For example, sophisticated 'smart TVs' equipped with cameras and microphones could be converted into spying devices that provide companies with behavioural data and recordings of their users. CCTV surveillance is augmented by algorithms providing face recognition or detecting unusual behaviour, and it becomes mobile when attached to drones or other moving objects. However, far more challenging to the state of fundamental rights and values are those data generated by mobile devices or by services provided through the Internet. Even if the contents of communications were excluded, accumulated information on the whereabouts, communication partners or visited websites – so-called meta-data – provides sufficiently deep insights to be highly attractive for exploitation for commercial or security purposes.

The temptation to embrace mass-surveillance technologies seems hard to resist for institutional actors, as demonstrated by recent revelations of clandestine mass-surveillance activities and by the intense policy-making surrounding a measure like the EU Data Retention Directive (Ripoll Servent, 2013). This measure has been initially introduced in 2006 (Bignami, 2007), with the goal of making compulsory the storage by telecommunication providers of traffic and location data of all communications, so to make them available to law enforcement and security authorities for a period between 6 months to 2 years. The directive has been later on declared as invalid by the Court of Justice of the European Union (Lynskey, 2014), and by several constitutional courts of member states, often intervening in cases lodged by civil-society organizations or ad hoc citizenship committees (de Vries *et al.*, 2011). The disputes on data retention, full of conflicts and of sharp turns in policies, show clear evidence for the interplay between technology development and surveillance capabilities, on the one hand, and regulation and security politics on the other hand. Only the digitization of telecommunication networks created the possibility to access traffic data on a large-scale, data being generated automatically by the new technology. The regulatory response, in line with data-

protection principles, was to mandate the deletion of these data once not needed anymore for billing purposes. These regulations were then turned upside down by the Data Retention Directive, requesting the mandatory retention of this data for law enforcement purposes. Then, several of these legal instruments were challenged in court and annulled. In other words, the case of the Data Retention Directive highlights that the relation between surveillance and data protection is not as linear as conveyed by the image of the balance. Privacy can become a vector of surveillance – the directive was formally devised as a data protection instrument – but it can also be reclaimed by citizens and used as a legal grip to contest mass-surveillance (Hornung *et al.*, 2010).

And yet, concerns that such conflicts will proliferate in the near future are more than justified. There are constant demands to expand the use of meta-data even further for profiling activities in the context of crime and terror prevention. Not only technology will progress further, the Internet of Things will generate data of unprecedented comprehensiveness and explicitness of persons inhabiting future environments, and create corresponding demands and desires to access and analyse this data (Čas, 2011). Also from a societal and political perspective, little prospects for relaxations exist. Economic policies are deepening and extending the crisis, which began in 2008, rather than bringing the EU back to a path of economic prosperity and decreasing income disparities. Consequently, social cohesion and political stability within the EU and its member states is becoming increasingly endangered. Political instability and violent conflicts are persisting in neighbouring regions of Europe. Moreover, human mobility within and into the EU is still framed by several political actors as a security challenge, invoking an intensification of travellers' surveillance. Both, these internal and external developments are fuelling citizens' worries about their security and fear of terrorism.

Taking privacy seriously

Different perceptions of privacy, and of the importance of protecting it, are principal factors complicating the balancing or trading of privacy and security against each other. From a simplified point of view, privacy is certainly not ranked highest in the hierarchy of needs; privacy would be positioned after basic needs like food, shelter or bodily security (Maslow, 1943). From such a perspective sacrificing some privacy for more security appears to be a logical consequence, at least as long as gains in security are evaluated as more important than the resulting losses in privacy. From a formal human rights perspective, there are no predetermined hierarchies present in respective charters and declarations, apart from absolute prohibitions like slavery or torture. In the case of the respect for private life or the privacy of communications, categories of possible limitations to this right are usually included in the respective provisions, national security belonging to the explicitly mentioned reasons for exceptions. For example, Article 8 of the European Convention of Human Rights provides for the "right to respect for private and family life" and states that:

1   Everyone has the right to respect for his private and family life, his home and his correspondence.

2   There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Decisions about the legitimacy of legal provisions based on this exception or about security measures infringing privacy require, however, an individual judgment about the adequacy, necessity and proportionality of specific acts or measures (Bagger Tranberg, 2011).

Privacy is not only one of the core fundamental rights, but it also plays a central role for exertion of other fundamental rights and freedoms, for balancing powers between the state and citizens, for democratic development, societal and economic innovativeness or individual autonomy (Solove, 2008b). Privacy is a precondition for thinking and expressing oneself freely, in general and in particular when new media or social networks come into play. Respect for or disregard of privacy is pivotal for the function and functioning of the Internet as the information and communication backbone of liberal societies. Whether the Internet can continue to be an infrastructure for unrestricted communication and access to information, supporting the freedom of expression and political participation or whether it is converted into an instrument of control and surveillance depends predominantly on the respect for privacy.

The secret exertion of mass-surveillance is in itself a clear symptom of disesteem of democratic principles. Such tendencies might be inherent to intelligence services, always working in a secret mode and thus with some discretion from legislation; new are the possibilities offered by new technologies to cover essentially all forms of communication and thus also the whole population. Whereas the secretiveness of individual acts of surveillance or observation may constitute an essential precondition for the effectiveness of such measures, it makes assertions to implement mass surveillance as an outcome of a process balancing privacy and security essentially meaningless. Doing actually what is possible potentially, actively excludes any consideration of effectiveness, intrusiveness or proportionality. In the case of mass surveillance the claim of balancing turns into a general justification (EGE 2014), free from any obligation to substantiate such measures. In this way, paradox situations are created: for individual acts of surveillance or interception of communications, directed against specific suspect(s) for a limited time, a high burden of proof is necessary. In contrast, for essentially unlimited measures of surveillance, in terms of people affected, means used, data collected and duration, the burden of proof is reduced to the existence of abstract, and as such always prevalent, security threats, without any need to provide evidence for the effectiveness of measures of bulk surveillance.

Security incidents tend to get more attention and to be attributed with more weight than privacy when trading one for another is at stake. Strong differences in

visibility and immediateness of the consequences of privacy violations, on the one hand, and of security incidents, on the other, are additional factors contributing to this phenomenon. The latter are usually directly impacting the concerned persons; privacy violations, on the other hand, can happen in an unnoticeable manner. The consequences of such violations may only become visible with long delays. Owing to these delays, it might be difficult to associate specific forms of discrimination to infringements of privacy and even more difficult to provide proof for causal relationships. In many cases it might be even impossible to recognize such links at all. Security incidents, in particular if they are related to terrorism, immediately get highest attention from media and policy-making. In contrast, only very large-scale privacy infringements make it to the headlines and are hardly followed up by policy debates or concrete actions.

The limits of trade-off and balancing approaches

A generalized application of the trade-off approach or the justification of infringements of privacy or other fundamental rights in the name of security requires that a reverse relationship between the issues at stake exists. Whereas in one direction a reverse proportionality can be observed generally – it is at least very difficult to construct examples where more surveillance increases privacy – it is by no means obvious that such mechanisms are also working in the other direction. On the contrary, privacy in itself constitutes an element of security; infringements of privacy may not result in any direct security gains, but influence security negatively in indirect ways. Apart from the essential role which privacy plays for the protection of citizens against (the abuse of) state powers, the protection of personal data and privacy is a key component of online security. The prevalence of the trade-off thinking in matters of internal security seduces to request ever more surveillance without asking for effectiveness and efficiency. Ineffective surveillance measures cause inefficiencies anyway as they consume scarce human and financial resources for their operation. Mass-surveillance systems generate necessarily high numbers of suspects if they are set sensitively enough to detect dependably potential threats; too high numbers of (false and correct) positives to be handled by law enforcement in a meaningful way (Saetnan, 2007). The inherent promise of the privacy–security trading-off metaphor that surveillance is automatically increasing security does not only cause misallocations of resources between security measures in a short-term perspective, it also causes long-term misallocations by prioritizing end-of-pipe solutions in comparison to targeting root causes of insecurity. In a more general way, this technological bias further reinforces already strong tendencies to focus on specific aspects of security. Security threats for which remedies involving surveillance technologies are promoted gain in attention at the expense of social and societal security issues, which would require policy measures to maintain economic or social wellbeing.

Ironically, privacy–security debates, allegedly based on a trade-off approach, are in reality often rejecting trading rather than trying to find a balance. They are frequently characterized by unbalanced confrontations between extreme positions,

represented by statements that security improvements inevitably require unrestricted access to any kind of data imaginable, on the one hand, and an essentially complete denial of any security gains resulting from extending surveillance possibilities, on the other. The contributions of this book provide many insights to allow for more meaningful debates and decisions on surveillance, security and privacy. They bring back complexity, meaning and responsibility to a discourse in which particular interest and prejudgements seem to be triumphing over evidence, rationality and historical wisdom. They help to disclose the hostile symbiosis between security and liberty (Wittes, 2011) and hence to identify areas where it might be appropriate and legitimate to balance security and privacy, but also to see clearly the dangers and limits of balancing (Solove, 2008a). Measures of mass surveillance which eliminate the core of the fundamental right of privacy and thus also the foundation of individual freedoms, democratic liberties, economic prosperity and societal development should never become a serious matter of trade-off thinking.

The structure of the book

The material in this book is divided into three main parts. The first part of the book, 'Citizens' perceptions on security and privacy – empirical findings' presents and analyses at the heart of the volume the results of the participatory activities and social surveys undertaken by the three European projects and related studies.

In Chapter 1, 'Privacy and security – citizens' desires for an equal footing', Tijs van den Broek, Merel Ooms, Michael Friedewald, Marc van Lieshout and Sven Rung, take up the now traditional debate on the opposition between the privacy and security as the equation to be solved in order to provide adequate societal security. Based on empirical results from the social survey carried out in the PRISMS project, the article presents new findings about the role of 'invasiveness' in the determination of public acceptance of surveillance measures.

In Chapter 2, 'Citizens' privacy concerns: does national culture matter?', Jelena Budak, Edo Rajh and Vedran Recher take a closer look at the relationship between concerns for privacy and national culture. Culture, they suggest, is an important determinate of the outcome of the security–privacy equation.

In Chapter 3, 'The acceptance of new security oriented technologies, a "framing' experiment"', Hans Vermeersch and Evelien De Pauw take a critical approach to the security–privacy opposition by analysing closely surveillance technologies as a way of better focusing the angle of analysis of security technologies in social settings.

In the book's fourth chapter, 'Aligning security and privacy: the case of Deep Packet Inspection', Sara Degli Esposti, Vincenzo Pavone, and Elvira Santiago-Gómez take up the question of the premises and impact of DPI, drawing attention to nuances in the notion of the public acceptance of 'surveillance oriented security technologies' (SOSTs). Based on empirical data gathered at the SurPRISE citizen summits, the chapter investigates the multiple layers and levels of public acceptance and their relation to both the acceptability and effectiveness of mass-surveillance measures.

In the final chapter of Part I, 'Beyond the trade-off between privacy and security? Organizational routines and individual strategies at the security check', Francesca Menichelli takes up the Foucauldian concept of governmentality in order to re-interpret the PRISMS data, using it to cast light on the concepts of mobility and its role in airport security settings.

The second part of the book, 'Emergent security and surveillance systems', identifies and analyses more fundamental changes taking place at the heart of Europeans' social reality as a consequence of the increasing imposition of surveillance measures.

In Chapter 6, 'The deployment of drone technology in border surveillance, between techno-securitization and challenges to privacy and data protection', Luisa Marin analyses the impact on the security–privacy and data protection equation of drone technologies in border surveillance operations.

In Chapter 7, 'Perceptions of videosurveillance in Greece: a 'Greek paradox' beyond the trade-off of security and privacy?', Lilian Mitrou, Prokopios Drogkaris and Georgios Leventakis provide an overview of the recent use of the CCTV technologies in Greece, analysing this new surveillance reality in relation to the existing Greek regulatory frameworks and social norms.

In the final chapter of this section, 'Urban security production between the citizen and the state', Matthias Leese and Peter Bescherer turn their attention to the way in which urban politics mediates social friction creating a special case of the privacy–security trade-off.

The third and final part of the book, 'Governance of security and surveillance systems', gathers chapters that examine and interpret in detail the empirical results of both, the three research projects at the heart of the book and of further relevant research, interrogating the limits of the security–privacy trade-off, and taking up new solutions of accommodating to the practical and political challenges of legal regulation in the age of digital surveillance.

In Chapter 9, 'Moving away from the security–privacy trade-off: The use of the test of proportionality in decision support', Bernadette Somody, Máté Dániel Szabó and Iván Székely focus on the question of the legitimacy of security measures and the limits of the trade-off model of security–privacy analyses by introducing distinctions stemming from traditional legal proportionality tests.

In Chapter 10, 'The legal significance of individual choices about privacy and personal data protection', Gloria González Fuster and Serge Gutwirth take up the inherent tension between rights-based legal approaches to governing surveillance measures and the actual experiences and perceptions they might be expected to reflect.

In Chapter 11, 'The manifold significance of citizens' legal recommendations on privacy, security and surveillance', Maria Grazia Porcedda extends this citizen-oriented approach by examining the recommendations made by citizen-participants in SurPRISE participatory events. The chapter demonstrates, among other detailed results, that it is possible to submit complex policy issues, not least legal ones, to the general public.

In the following Chapter 12, 'The importance of social and political context in explaining citizens' attitudes towards electronic surveillance and political

participation', Dimitris Tsapogas examines the relation between the expansion of electronic surveillance practices and political behaviour, while at the same time formulating a number of important methodological insights about the need for integrating contextual aspects in explaining attitudes about surveillance measures.

In the next chapter, 'In quest of reflexivity: towards an anticipatory governance regime for security', Georgios Kolliarakis turns his attention to the 'epistemic modalities' of security research. He argues that current research-based security policy has built upon on a too-narrow understanding of the relationship between knowledge-building and security governance, suggesting that a second-order or consultative integration of civil-society knowledge is a condition for coherent security policy.

In the final chapter of the section, 'A game of hide and seek? – unscrambling the trade-off between privacy and security', Stefan Strauß reasons that the security–privacy trade-off is a fallacy that has negative impacts on privacy protection, arguing that there is a need for alternatives that put greater emphasis upon the factual intersections and differences between privacy and security.

Notes

1   Lyon (2007, p. 14).
2   Video message to the fourth Annual Freedom Online Coalition Conference: Free and Secure Internet for All, 28–29 April 2014. www.un.org/sg/statements/index.asp?nid=7634 (accessed 18 December 2016).
3   http://surprise-project.eu/events/international-conference/ (accessed 18 December 2016).

References

Amoore, L. and De Goede, M. (2005) 'Governance, Risk and Dataveillance in the War on Terror', *Crime, Law and Social Change,* 43: 149–173.

Andrejevic, M. and Gates, K. (2014) 'Big Data Surveillance: Introduction', *Surveillance & Society,* 12: 185–196.

Bagger Tranberg, C. (2011) 'Proportionality and Data Protection in the Case Law of the European Court of Justice', *International Data Privacy Law,* 1: 239–248.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R.B. (2014) 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology,* 8: 121–144.

Bellanova, R. and Duez, D. (2012) 'A Different View on the "Making" of European Security: The EU Passenger Name Record System as a Socio-technical Assemblage', *European Foreign Affairs Review,* 17: 109–124.

Berling, T.V. and Bueger, C. (eds) (2015) *Security Expertise. Practice, Power, Responsibility*, London: Routledge.

Bignami, F. (2007) 'Privacy and Law Enforcement in the European Union: The Data Retention Directive', *Chicago Journal of International Law,* 48: 233–255.

Bigo, D. (2006) 'Protection. Security, Territory and Population', in J. Huysmans, A. Dobson and R. Prokhovnik (eds) *The Politics of Protection. Sites of Insecurity and Political Agency,* London: Routledge, 84–100.

Bigo, D., Walker, R.B.J., Carrera, S. and Guild, E. (2008) 'The Changing Landscape of European Liberty and Security: Mid-Term Report of the Challenge Project', *International Social Science Journal,* 59: 283–308.

Čas, J. (2011) 'Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions', in S. Gutwirth, Y. Poullet, P. De Hert and R. Leenes (eds) *Computers, Privacy and Data Protection: An Element of Choice,* Dordrecht: Springer, 139–169.

'Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', *Official Journal of the European Union*, L 119, 4.5.2016, 132–149.

European Group on Ethics in Science and New Technologies to the European Commission (EGE) (2014) *Ethics of Security and Surveillance Technologies,* Luxembourg: Publications Office of the European Union.

Goold, B.J. (2010) 'How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy', in D.W. Schartum (ed.) *Overvåking i en rettsstat*. Bergen: Fagbokforlaget, 38–48.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York: Metropolitan Books.

Hayes, B. and Vermeulen, M. (2012) *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the 'Smart Borders' Proposals,* Berlin and Brussels: Heinrich Böll Stiftung. Available at: www.statewatch.org/news/2012/jun/borderline.pdf (accessed 3 August 2016).

Hornung, G., Bendrath, R. and Pfitzmann, A. (2010) 'Surveillance in Germany: Strategies and Counterstrategies', in S. Gutwirth, Y. Poullet and P. De Hert (eds) *Data Protection in a Profiled World,* Dordrecht: Springer, 139–156.

Huijboom, N. and Bodea, G. (2015) 'Understanding the Political PNR-debate in Europe: A Discourse Analytical Perspective', *Perspectives on European Politics and Society,* 16: 241–255.

Kaufmann, F.-X. (1973) *Sicherheit als soziologisches und sozialpolitisches Problem: Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften,* 2nd ed., Stuttgart: Ferdinand Enke.

Leese, M. (2014) 'The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union', *Security Dialogue,* 45: 494–511.

Lynskey, O. (2014) 'The Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and is Invalid in its Entirety: Digital Rights Ireland', *Common Market Law Review,* 51: 1789–1812.

Lyon, D. (2007) *Surveillance Studies: An Overview,* Cambridge: Polity Press.

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data & Society,* 1: 1–13.

Maslow, A.H. (1943) 'A Theory of Human Motivation', *Psychological Review,* 50: 370–396.

Monahan, T (2006) *Surveillance and Security: Technological Politics and Power in Everyday Life,* New York: Routledge.

Neocleous, M. (2007) 'Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics', *Contemporary Political Theory,* 6: 131–149.

Pavone, V. and Degli Esposti, S. (2012) 'Public Assessment of New Surveillance-oriented Security Technologies: Beyond the Trade-off between Privacy and Security', *Public Understanding of Science,* 21: 556–572.

Ripoll Servent, A. (2013) 'Holding the European Parliament Responsible: Policy Shift in the Data Retention Directive from Consultation to Codecision', *Journal of European Public Policy,* 20, 972–987.

Saetnan, A.R. (2007) 'Nothing to Hide, Nothing to Fear? Assessing Technologies for Diagnosis of Security Risks', *International Criminal Justice Review,* 17: 193–206.

Solove, D.J. (2008a) 'Data Mining and the Security-Liberty Debate', *The University of Chicago Law Review,* 75: 343–362.

Solove, D.J. (2008b) *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Valverde, M. and Mopas, M.S. (2004) 'Insecurity and the Dream of Targeted Governance', in W. Larner and W. Walters (eds) *Global Governmentality,* New York: Routledge, 233–250.

Vries, K. de, Bellanova, R., De Hert, P. and Gutwirth, S. (2011) 'The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)', in S. Gutwirth, Y. Poullet, P.D. Hert and R. Leenes (eds) *Privacy and Data Protection: An Element of Choice,* Berlin: Springer, 3–23.

Wittes, B. (2011) *Against a Crude Balance: Platform Security and the Hostile Symbiosis Between Liberty and Security.* Washington. Available at: www.brookings.edu/wp-content/uploads/2016/06/0921_platform_security_wittes.pdf (accessed 4 August 2016).

Part I

Citizens' perceptions on security and privacy – empirical findings

1 Privacy and security

Citizens' desires for an equal footing

Tijs van den Broek, Merel Ooms, Michael Friedewald, Marc van Lieshout and Sven Rung

Introduction

PRISMS (PRIvacy and Security MirrorS) is a FP7 project that focuses on the so-called trade-off relationship between privacy and security. The most prominent vision is that security comes with a price, namely at the expense of privacy. One cannot have both, and being secure means that control needs to be exercised over one's situation, often by third parties who thus need access to the private sphere of citizens. This trade-off thinking is however criticized from a number of perspectives (Solove 2008; Pavone *et al.* 2012). The criticism points at faulty assumptions that take stated preferences of respondents on face value while these conflict with actual behaviour (Ajzen 1991). It also criticizes the fundamental presupposition that seems to deny that it is factual impossible to have both. Trade-off thinking is *a priori* framed in a discourse that apparently rejects the possibility that security can be achieved without infringement on privacy (Hundt 2014). This framing endangers democratic society, putting the conditions for security above the conditions for living in a free and democratic society. The PRISMS Project has questioned this trade-off relationship by organizing a series of reflexive studies and by organizing a pan-European survey in which EU citizens have been asked how they perceive situations in which both privacy and security are addressed on equal footing. The reflexive studies showed how the political discourse on privacy and security inevitably – at least so it seems – considers privacy infringements to be legitimized by referring to the security threats that present-day society faces. The framing is solid, and is hardly questioned (Huijboom and Bodea 2015). An analysis of technological practices shows, on the basis of various cases, how technological practices are framed in security jargon while privacy is minimized as a potential technological asset (Braun *et al.* 2015).

The survey focused on general attitudes of European citizens vis-à-vis the trade-off model. The use of the terms 'privacy' and 'security' was avoided in the survey to prevent the *a priori* framing of these concepts as this often occurs in surveys.[1] The results of the generic part of the survey have been reported earlier (Friedewald *et al.* 2015a). The results demonstrate that citizens do not consider security and privacy to be intrinsically linked. The results rather show that citizens simply want both: if no direct link is presupposed between privacy and security, citizens

consider both values relevant for their well-being. They also consider the concepts that give rise to security different from the concepts that give rise to privacy, thereby questioning the existence of the trade-off.

In this chapter we will explore another element of the trade-off in greater detail. The survey used the so-called vignette methodology to concisely describe a number of situations in which both security and privacy issues play a role (again, without using the terms privacy and security in the description of the vignettes; see Appendix A for the vignette descriptions) (Hopkins and King 2010: 201–222). Respondents were subsequently asked in what sense they agreed with the situation, and whether they considered the situation to impact on fundamental rights. For some of the vignettes a number of alternative approaches were presented. These approaches either offered an alternative for the measure, which was described or alleviated parts of the measure.

In this chapter we will start with a concise presentation of the vignettes. We will then outline the research method for studying the vignettes, followed by a presentation of the overall results. Finally, two vignettes that reflect extreme responses will be presented in greater detail. The chapter will end with some conclusions from the interpretation of the results.

The vignettes – situations presented to European citizens

Having asked the respondents about their attitudes and concerns regarding more generic security and privacy features,[2] the survey continued by presenting eight vignettes. A vignette represents a concise storyline that may help positioning the respondents in a specific situation. If done properly, a vignette refrains from explicating specific values (though the storyline itself can be used to discover how respondents value the represented situations). The PRISMS project team spent considerable time in drafting vignettes that covered different types of privacy, different sets of actors (public, public/private and private) and both online and physical contexts. A large set of hypotheses has been constructed that helped in mapping out the different contexts that should be covered by the vignettes. Many of these hypotheses deal with the orientation of independent variables (such as gender and age). In this chapter we will not start from the hypotheses as such, but we will present the results from these hypotheses whenever appropriate (see next sections).

The vignettes were clustered around two axes. The first axis represented the variety of dominant actors in a vignette. This can be considered a relevant variable: we expected that public actors would receive more legitimacy for their actions than actors from the private sector in specific situations and for specific parts of the European population. Just to give an example: even though left-wing respondents generally will exhibit a higher resistance against the presence of the police in safeguarding specific events than right-wing respondents, one would still expect that left-wing respondents in general would accept the legitimacy of this actor. Similarly, one may expect that right-wing or more conservative respondents will accept a larger degree of influence by private actors than left-

wing or more socialist/liberal oriented respondents. Trust in institutions is one of the variables we introduced to be able to make these distinctions as well as directly asking how respondents would position themselves on a political scale (see next section).[3]

The second axis differentiates between vignettes that are primarily situated in the online or virtual world and vignettes that are situated in the physical or real world. In many situations today one can observe an integration of online and offline activities.[4] Still, the physical reality poses constraints different from the virtual reality. An almost trivial distinction is that within the physical reality actions do have a physical component. Monitoring speeding with cameras, for instance, means that physical objects – the cameras – are involved, which can be noticed. Of course, one can attempt to conceal the physical objects (such as hiding cameras behind trees or hiding them in boxes) but the physical dimensions of these cameras cannot be denied, nor can the physical dimensions of the objects they monitor (speeding cars) be denied.[5] Legislation usually obliges the involved actor to indicate to the public that these cameras are in place and that people should know they are being observed.[6] In virtual life, on the other hand, activities may go fully unnoticed. This can be so, because the actors involved use their skills to conceal their activities. It also can be the consequence of the limited ability of the observed to understand what is happening in the virtual world.[7] This is a distinction between the virtual and the real world: in the real world, the first layer of observation is direct and requires no specific abilities on the side of the observed. Only when actors use specific strategies to conceal their activities, do additional skills and competences come into play.

Using these two axes enabled us to plot the eight vignettes in one figure (see Figure 1.1). The vignettes range from being set only in the virtual world to being set only in the real world and from having public actors engaged to having private actors engaged. They relate to:

1   Foreign government (NSA type) surveillance – a charity organization shown to be under surveillance.
2   Biometric access management system – using biometrics for access to a school.
3   Smart meters – using data from smart meters to offer additional services.
4   Monitoring visits on terrorist websites – a young person using the Internet looking at terrorist sites, potentially monitored by government.
5   ANPR speed control – using cameras in a neighbourhood to track speeding.
6   ISP data selling – Internet service providers selling data they collect on the Internet usage of their clients.
7   Police use of DNA databases – DNA data that has been provided for medical research but is used for other purposes as well.
8   Crowd surveillance – the police monitoring a crowd at a demonstration/ monitoring supporters and hooligans at a football match.
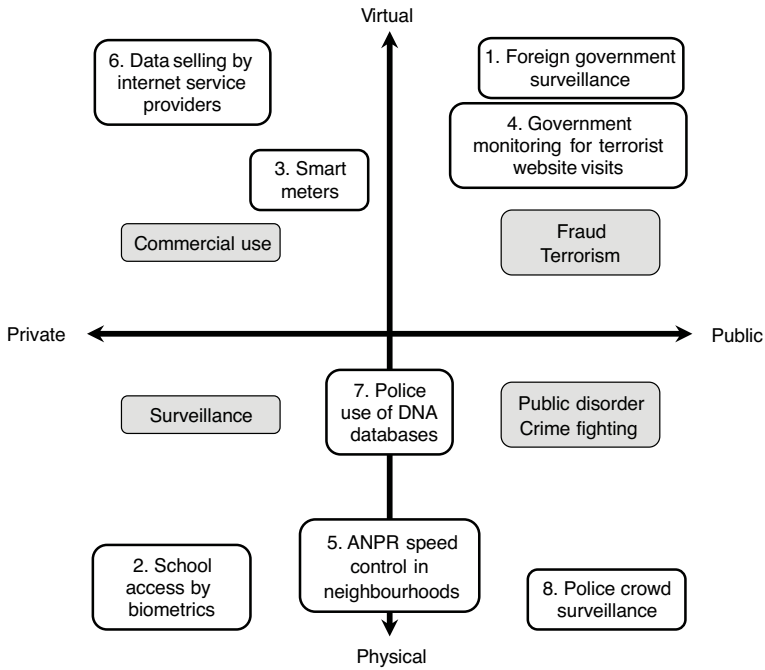
Figure 1.1 Matrix depicting the various vignettes along the axes virtual–physical and private–public

Source: Friedewald *et al.* (2016).

The survey – some methodological considerations

The composition of the sample

To study how European citizens perceive issues in which privacy and security play a role, we conducted a large-scale survey in all 27 EU countries. The data collection took place between February and June 2014. The survey company Ipsos MORI conducted around 1,000 telephone interviews in each EU Member State except Croatia (27,195 in total) using a representative sample (based on age, gender, work status and region) from each country (see Table 1.1).

The vignettes that were constructed were refined through sixteen focus groups in eight representative EU countries. In this way, it was ensured that the vignettes would be understood uniformly in different languages and that they would not cause extreme reactions that would bias results. Each interviewee was presented with four randomly selected vignettes, resulting in approximately 13,500 responses for each vignette (500 per country). Appendix A provides descriptions of the vignettes.

Table 1.1 Descriptive statistics of the sample

Vignette	n	% of total population	% male	% Age 16–34	% Age 35–59	% Age > 60	N/A
1. Foreign government surveillance	13200	12.4%	49.2%	29.5%	41.7%	28.6%	0.2%
2. School access by biometrics	13462	12.6%	48.0%	29.3%	41.6%	28.9%	0.2%
3. Smart meters	13231	12.4%	48.4%	29.3%	42.1%	28.5%	0.1%
4. Monitoring visits on terrorist websites	13190	12.3%	48.8%	29.0%	42.0%	28.8%	0.2%
5. ANPR speed control	13462	12.6%	47.7%	28.7%	41.6%	29.5%	0.2%
6a. Selling your data by ISP	6816	6.4%	50.0%	35.6%	45.8%	18.4%	0.2%
6b. Selling customer data by ISP	6768	6.3%	49.7%	34.6%	46.4%	18.9%	0.1%
7. Police use of DNA databases	13305	12.5%	48.3%	29.2%	42.1%	28.5%	0.2%
8a. Crowd surveillance (demonstration)	6668	6.2%	48.8%	28.5%	41.8%	29.4%	0.3%
8b. Crowd surveillance (football)	6729	6.3%	47.6%	29.3%	42.3%	28.2%	0.2%
Average			**48.7%**	**30.3%**	**42.8%**	**26.8%**	**0.2%**

Table 1.1 provides an overview of the sample for each vignette. On average, 48.7 percent of the population was male. Forty-three percent was in the 35–59 age. The population is evenly distributed across the vignettes, with the data selling and crowd surveillance vignettes equally split. The data selling vignette (6a/b) was received by a slightly younger population than the other vignettes.

Construction of variables

Dependent variable

For each vignette we constructed the same dependent variable, being the variable that indicates the relationship the respondents demonstrate in their responses to a specific vignette. This dependent variable is what we called the level of societal resistance (or acceptance, depending on the perspective one chooses) of the scenario presented in each vignette. For each vignette, respondents were asked to what extent, if at all, they thought the main actor in the vignette should or should not collect and process data in that specific scenario. Respondents were able to answer this question on a Likert-scale ranging from 'definitely should' (1) to 'definitely should not' (5). Consequently, a higher score means higher resistance and thus a lower societal acceptance of the vignette. The exact wording of the question is included in Appendix B.

Independent variables

Security concern was measured on a summated scale of perceived general security concern and perceived personal security concern. Respondents were asked how often they worried about a list of general and personal security indicators, with answer options ranging from 'most days' to 'never' (Friedewald *et al.* 2015b). The exact wording and indicators are included in Appendix B. To reduce the number of items and keep the information of all items, we conducted a factor analysis to see whether items could be combined in one construct. The factor loadings in the analysis showed that this was indeed possible on the European level, and thus a 'high security concern' scale was created by recoding the responses into low (0) and high (1) concern for security.

Attitudes towards privacy were measured by asking respondents to rate the importance of a list of indicators that measures the importance of keeping things private or privacy related actions. A factor analysis showed that items could be combined and the scale 'high privacy concern' was created accordingly, ranging from low (0) to high (1) concern for privacy.

To measure the perception of trust in institutions, the survey asked respondents to indicate for a number of institutions whether they do not trust this institution at all (0) or have complete trust in it (10). This question was recoded in a dummy variable with 0 = no trust at all and 1 = complete trust.[8]

Two alternative variables were taken into account in the analysis that measure attitudes to privacy and data protection practices in another way. The first is 'experience with privacy invasion'. Respondents were asked whether they ever had the feeling that their privacy was invaded in seven different situations such as online, at a supermarket or at an airport. This was recoded into respondents who said they never had this feeling (0) and respondents who did experience this feeling (1). The second variable was privacy activism, which is how active respondents are when it comes to protecting their privacy, measured in whether they have undertaken one or more of seven named activities to protect their privacy. The exact wording of these two questions can be found in the annex. To construct the variable, the number of activities a respondent claims to have undertaken are added up.

The survey included the following demographic questions as control variables: age (coded into three categories: 16–34 years, 35–59 years and 60+ years), gender, education level (coded into three categories: lower education, medium education and higher education) and political preference. The last control variable measured the political attitude of respondents on a spectrum from 'left' to 'right'. This variable was recoded into three categories (left-wing, neutral and right-wing preference).

Analysis of dependent and independent variables

As the dependent variable's measurement scale is ordinal, we conducted an ordered logistic regression analysis for each vignette, in which the societal acceptance question is regressed on security concern, privacy importance, specific attitudes to

privacy and data protection practices, social values and demographics as control variables. The independent variables were added as dummy variables in the analysis. We weighted the analysis to correct for population differences between the countries and the respondents in the dataset regarding age, gender and work status.

How do European citizens value privacy and security?

Main results of the vignettes

Tables 1.2–1.4 present the results of the ordered logistic regression analysis. Each table represents a different category of actors that are described in the vignettes: private sector actors (e.g. companies), semi-public sector actors (e.g. energy companies) and public sector actors (e.g. government agencies). The results show the average societal resistance, privacy type (virtual or physical), and the odds, standard error and statistical significance of the regression analysis. Odds, in contrast to regular coefficients of linear regression, represent how strongly, in terms of probability, the presence or absence of the independent variables are associated with the presence or absence of the dependent variable.

The vignettes in which private actors collect and process personal data elicit a high level of resistance from the respondents, with selling personal data as being the most contentious vignette (see Table 1.2). Attitudes towards privacy concern significantly increase the resistance, while a concern for security decreases the resistance. Trust in institutions significantly decreases resistance, especially for the data-selling vignettes. Practices regarding privacy and security (experience of privacy infringements and security concerns) hardly have any effect on the resistance of vignettes, except that no experience of privacy invasions decreases the resistance for the use of biometrics for school access. Surprisingly, we find the reverse effects of demographics between the vignettes with private actors. While men experience more resistance in the biometric school access vignette, they experience less resistance when their data is sold by their ISP. Young people show lower levels of resistance to the data-selling vignettes than older respondents. Last, respondents with left-wing orientation show higher levels of resistance to the use of biometrics for access to schools.

The vignettes in which semi-public sector actors collect and process personal data elicit lower levels of resistance from the population, with ANPR use against speeding in neighbourhoods as the most acceptable vignette (see Table 1.3). Similar to the previous three vignettes, attitudes towards privacy significantly increase resistance, while a concern for security measures decreases resistance. The effect of security concern is less significant for the smart meters vignette. On the contrary, trust in institutions showed itself to be most important in relation to the acceptance of the smart meters vignette: the higher the trust, the higher the acceptance of collecting personal data for smart meters. Young people and men have higher acceptance levels for smart meters collecting personal data and the DNA databases vignette than for ANPR use against speeding in neighbourhoods. Finally, political attitude showed to have an effect across all public/private vignettes: the higher the

Table 1.2 Results of ordered logistic regression analysis of vignettes involving private sector operators

	← Agreeable							Contentious →		
Average societal resistance	3.26			4.22			4.27			
Vignette	2. School access by biometrics			6b. Selling customer data by ISP			6a. Selling your data by ISP			
Privacy type	Physical			Virtual			Virtual			
	Odds		s.e.	Odds		s.e.	Odds		s.e.
High privacy concern	1.268	***	.101	1.024	***	.129	.642	***	.130
High security concern	−1.218	***	.123	−.610	***	.149	−.822	***	.151
High trust in institutions	−.347	***	.136	−1.335	***	.177	−1.361	***	.170
No experience in privacy invasion	−.104	***	.046	−.181	*	.058	−.002		.058
Low degree of privacy activism (0 or 1 times)	−.143		.105	.161	*	.119	−.175		.121
Medium degree of privacy activism (2 or 3 times)	−.026		.102	.475		.117	−.013		.119
Being male	.119	***	.043	−.066	***	.054	−.301	***	.054
Age 16–34	−.173	***	.089	−.814	*	.084	−.812	***	.080
Age 35–59	−.017	**	.082	−.450		.078	−.278	***	.078
Low educational level	−.249		.062	−.017	**	.081	−.010		.079
Medium educational level	−.176	***	.051	−.062		.060	.057		.060
Political left	.404	***	.067	.128		.082	.097		.081
Political neutral	.121		.055	.173		.068	.160	*	.067

Notes: n per vignette is listed in Table 1.1 with descriptive statistics.
* p < .05; ** p < .01; *** p < .001
Reference group: Old age (60+) / Female / Higher education / Political right–wing preference / High privacy activism (people who have actively protected their privacy more than three times)

Table 1.3 Results of ordered logistic regression analysis of vignettes involving semi-public sector operators

	← Agreeable						Contentious →		
Average societal resistance	2.17			2.92			2.97		
Vignette	5. ANPR speed control			3. Smart meters			7. Police use of DNA databases		
Privacy type	Physical			Virtual			Physical		
	Odds		s.e.	Odds		s.e.	Odds		s.e.
High privacy concern	1.429	***	.105	.887	***	.102	1.105	***	.065
High security concern	−.881	***	.126	−.415	**	.121	−.703	***	.080
High trust in institutions	−.738	***	.139	−1.437	***	.135	−.335	***	.085
No experience in privacy invasion	−.102	*	.047	−.183	***	.047	−.086	**	.029
Low degree of privacy activism (max. 1 times)	−.269		.115	−.137		.106	.051		.067
Medium degree of privacy activism (2 or 3 times)	−.092		.113	.038		.104	.118		.065
Being male	232	*	044	−.160	***	.043	−.058	*	.027
Age 16–34	−.217	***	.093	−.798	***	.064	−.245	***	.058
Age 35–59	−.080		.083	−.333	***	.054	−.197	***	.054
Low educational level	−.163	***	.062	.005		.062	−.271	***	.039
Medium educational level	−.063	***	.052	.005		.050	−.167	***	.031
Political left	.114	***	.067	.248	***	.067	.279	***	.041
Political neutral	.105	***	.056	.203	***	.055	.168	***	.035

Notes: n per vignette is listed in Table 1.1 with descriptive statistics.
★ p < .05; ★★ p < .01; ★★★ p < .001
Reference group: Old age (60+) / Female / Higher education / Political right-wing preference / High privacy activism (people who have actively protected their privacy more than three times)

preference for left-wing parties, the higher the resistance. This effect, however, is weaker in relation to ANPR use against the speeding in neighbourhoods vignette.

The vignettes in which public sector actors collect and process personal data elicit lower levels of resistance from the population than vignettes with private sector actors (see Table 1.4). The foreign government monitoring vignette triggered the highest level of resistance, while monitoring terrorists' online behaviour was most accepted by respondents – though the practices are similar. Similar to the previous three vignettes, higher concerns towards privacy significantly increase resistance, while a concern for security decreases the resistance. These effects of security concern and privacy attitudes are the strongest in the crowd surveillance of demonstrations vignette. Respondents' trust in institutions is an important factor in the context of monitoring of political demonstrations, while it is less important for monitoring terrorists' online behaviour or football matches. Interestingly, a younger age positively influences the acceptance of government monitoring, while it negatively influences the acceptance of monitoring crowds at football matches.[9] Respondents with a low and medium level of education have significantly lower resistance levels than higher educated respondents, specifically in relation to monitoring terrorists' online behaviour and both crowd surveillance vignettes. Finally, political attitude is a relevant factor when the purpose of data collection is politically oriented: respondents that prefer left-wing political parties show more resistance when political demonstrations are monitored than terrorist behaviour or football matches.

Detailed presentation of the findings of two vignettes

In this section we will show that context is a relevant determinant for attitudes towards privacy. To demonstrate this relevance of the context we will use the two most extreme vignettes in terms of responses to the question whether citizens agree or disagree with the situation presented in the vignette.

The two vignettes that are the most extreme in this respect are the vignette 'Selling data by ISP', relating to companies who want to sell information about people's use of the Internet, and the vignette 'crowd surveillance', relating to police monitoring of a crowd. The two vignettes differ in the context they represent. The 'Selling data by ISP' vignette describes a situation in the online world. An Internet Service Provider provides end-users the connection to the Internet and may offer additional services (for instance an e-mailbox, or security services).[10] An ISP offers its clients a usually lengthy and hard-to-read policy document that encompasses the way the ISP handles the personal data of the client. Many ISPs sell client data to third parties (advertorials or other commercial parties). The 'The police survey football match/demonstration' vignette describes a situation in the physical world, in which security measures cover a variety of approaches (camera surveillance, police officers clearly visible). Though this was not explicitly included in the description of the vignette in the questions we posed, these various measures were presented.

Both vignettes were presented in two variations. The vignette on 'Selling data by ISP' was varied in one approach that says that 'your' information is being sold

Table 1.4 Results of ordered logistic regression analysis of vignettes involving public sector operators

	← Agreeable 2.28			2.28			2.72			Contentious → 3.6		
Average societal resistance												
Vignette	4. Monitoring visits on terrorist websites			8b. Police surveys football match			8a. Police surveys demonstration			1. Foreign government surveillance		
Privacy type	Virtual			Physical			Physical			Virtual		
	Odds		s.e.	Odds		s.e.	Odds		s.e.	Odds		s.e.
High privacy concern	.600	***	.070	1.188	***	.105	2.069	***	.147	.855	***	.068
High security concern	−.750	***	.090	−.738	***	.127	−1.650	***	.174	−.504	***	.083
High trust in institutions	−.523	*	.093	−.288	*	.137	−1.309	***	.190	−.699	***	.092
No experience in privacy invasion	−.066	*	.032	.021		.046	−.173	**	.066	−.184	**	.032
Low degree of privacy activism (max. 1 times)	.025		.076	−.206		.106	.374	*	.165	−.035		.073
Medium degree of privacy activism (2 or 3 times)	.002		.074	−.078		.103	.525	**	.161	.046	***	.072
Being male	.068	**	.030	−.031		.043	−.129	*	.060	.138		.029
Age 16–34	.251		.043	.404	***	.091	.014		.133	−.361	***	.043
Age 35–59	.006		.039	.170	*	.084	.046		.122	−.113	***	.038
Low educational level	−.285	***	.042	−.359	***	.061	−.566	***	.087	−.075		.043
Medium educational level	−.206	**	.034	−.273	***	.050	−.418	***	.071	−.143		.035
Political left	.446	***	.047	.446	***	.067	.889	***	.097	.216		.046
Political neutral	.168	*	.040	.145	*	.058	.421	***	.079	.015	*	.037

Notes: n per vignette is listed in Table 1.1 with descriptive statistics.
　★ p < .05; ★★ p < .01; ★★★ p < .001
　Reference group: Old age (60+) / Female / Higher education / Political right–wing preference / High privacy activism (people who have actively protected their privacy more than three times)

and one that says that 'their customers' information' is being sold. It was expected that respondents might react more strongly when the word 'you' is used and they are thus addressed more directly. In the vignette 'The police survey football match/demonstration', we introduced a variation in which one group of respondents was informed 'a demonstration' is monitored and the other group of respondents was informed that a 'crowd of football fans' is monitored. It was expected that respondents might be more approving of monitoring when it concerns football fans as opposed to a demonstration, since a demonstration might appeal to exercising fundamental rights while hooliganism can be expected to raise security concerns among a large part of the population.

Figure 1.2 presents the response to the question 'To what extent, if at all, do you think that companies offering services on the Internet should or should not be able to sell information about (people/you) in this way?' in the case of the 'Selling data by ISP' vignette and 'To what extent, if at all, do you think that the police should or should not monitor the (demonstration/fans) in this way?' in case of the 'The police survey …' vignette.

The responses to the vignette about 'Selling data by ISP' show that citizens are rather averse towards practices in which Internet service providers sell customer data (respectively 80.8 percent of answers probably or definitely should not for 'your data' and 79.5 percent answers probably or definitely should not for 'their customers data'). Differences between the two variations ('your data' versus 'their customers data') are relatively small. For the vignette 'The police surveys …' almost the opposite applies, especially when football fans are said to be monitored. For this vignette a large majority (68.2 percent in the case of football fans and 54.4 percent in the case of a demonstration) think the police should probably or definitely
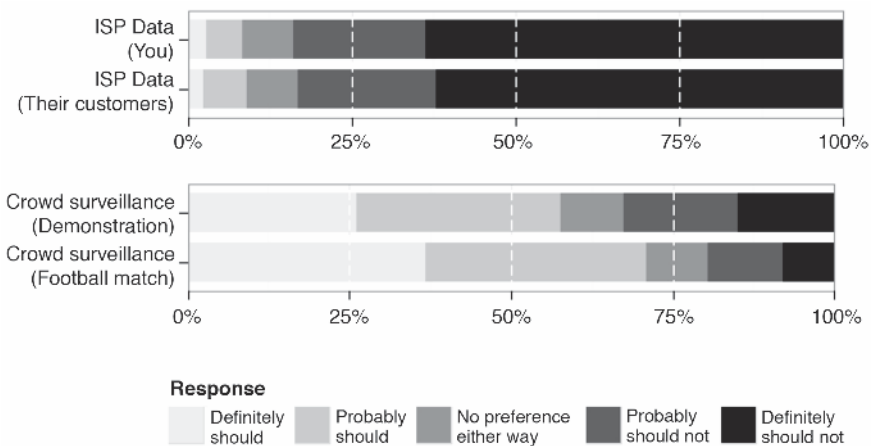

Figure 1.2 Responses to vignettes 'ISP data' and 'crowd surveillance'

monitor the crowd. Differences between the two variations presented in surveying a demonstration or a football match are clear. Only 22.1 percent of respondents think that the police probably or definitely should not monitor the crowd at a football match, while 34.3 percent have this opinion for a demonstration. Regression analysis shows that political attitude moderates the effect. The practice in which a demonstration is surveyed thus meets more resistance than the surveillance of a football match.

In contrast to the findings of Budak *et al.* (2016, in this volume) on the cultural context of privacy concerns, the EU countries hardly differ in the average score on the Likert scale in terms of the acceptance of these vignettes. The average score on the 'Selling data by ISP' vignette is 4.27 with the lowest average being 4.258 (Germany) and the highest 4.299 (Cyprus). The average score on the 'The police survey…' vignette is much lower meaning more acceptance, being 2.72 with the lowest average being 2.699 (Greece) and the highest being 2.749 (Romania). We might conclude that there seems to be much agreement among EU countries that companies should not be able to sell information, and that European citizens accept practices in which the police monitor a crowd of demonstrators or football fans.

The regression analysis presented in Tables 1.2 and 1.4 reveals differences in factors which affect resistance to the crowd monitoring and data-selling vignettes. Firstly, a high trust in institutions strongly increases the acceptance of the vignettes, except for the monitoring of football matches. Although this latter correlation (or absence of a correlation) seems a bit strange at first sight, it essentially means that respondents with lower trust in institutions have a similar level of acceptance of the police monitoring hooligans as respondents with higher trust in institutions. Secondly, privacy activism only plays a role in the selling customer data vignette. Thirdly, a younger age decreases the resistance to selling personal data, while increasing the resistance to surveying crowds during football matches. Lastly, political attitude only matters when the context of the vignette is political itself. Hence, political attitude does not affect the acceptance of selling personal data to an ISP, but it does affect the acceptance of surveilling political demonstrations.

While the statistical analysis yields interesting perspectives on which factors are relevant in the various vignettes, it does not reveal directly why European citizens assess the various situations differently. Looking at the complete set of vignettes we tentatively conclude that two dimensions seem to be relevant. Firstly, it seems that people make a distinction between those contexts which have a predominantly online dimension and those which have a predominantly physical dimension. We did not ask respondents to indicate how they perceive these dimensions so we only can make tentative observations. However, it looks as if respondents evaluate the online situation in terms of being less in control and the overall situation as being less transparent to them than the physical situation. This could be attributed to the competence one needs to act in the online world versus the competence one needs to act in the physical world. Secondly, many of the actions we described in the various vignettes are less observable in the online context than in the physical contexts.

A CCTV device is more easily recognized and a biometric access management system at a school is more visible than the government monitoring websites, which may be done completely invisibly. This makes these actions more 'creepy' and, again, outside the boundaries of control by the respondents.

An additional observation that helps explaining the different responses to the two vignettes is the different approach both vignettes represent in addressing privacy and security concerns. While in the case of the monitoring vignettes there is a clear combination of both privacy and security concerns (physical security), this is less clearly visible in the ISP selling data vignette. The security dimension in this latter vignette is somewhat related to cyber security (preventing the unexpected intrusion in one's data) but could be perceived as being less prone to security concerns than the monitoring vignette. The ISP vignette could thus be evaluated by respondents as being primarily relevant for its privacy dimension while the monitoring vignette could be considered relevant in both its privacy and security dimension.

We present these observations as tentative conclusions, meriting further attention and research. With the rise of surveillance tools, which predominantly rely on online technologies (the emergence of big data and data analytics), trust in these technologies needs to be safeguarded in order to achieve legitimacy for actions both by private and public actors. Although respondents indicate a higher level of trust in activities exercised by public actors, this higher trust is only minimal.

Conclusions

We analysed the results of the responses of EU citizens in a number of situations. The situations were phrased as short vignettes, or storylines, that presented a specific security practice in which privacy aspects were embedded. We refrained from an explicit reference to either security or privacy as constituting components of the vignettes, in order to avoid a framing of the vignettes as a built in trade-off approach. We wanted to study how respondents would value a situation in which no explicit reference to either security or privacy is made but that depicts situations similar to those pertaining in real life.

The first conclusion is that attitudes towards privacy depend on the security issue, as the degrees of acceptance highly differ for varying privacy intrusive situations. The results of the two opposing vignettes showed that the practice in which a demonstration is surveilled meets more resistance than the surveillance of a football match. This difference in response was equally shared among the EU countries. We conclude that respondents make a distinction between actions that may counter a legitimate interest of EU citizens (gathering for demonstrations as a fundamental right) and actions that are meant to safeguard the majority of EU citizens (and protect them against potential violent behaviour with no direct legitimate basis). This conclusion is tentative; we did not check the motives of respondents.

A second conclusion is that trust in institutions plays a relevant role, and that trust in public institutions correlates positively with acceptance of privacy intrusive measures. Other variables point in a direction one would expect: left-wing

oriented respondents are more critical of public actors' activities than right-wing respondents; respondents who are more critical with respect to their privacy are more critical of public intervention while respondents who expressed a higher security concern show a higher level of acceptance of these practices. A higher level of education was shown to be correlated with higher resistance to interventions that impacted on privacy.

A third conclusion is that the type of actor (whether from the public or private sector) that collects and processes personal data is relevant: vignettes with public sector actors receive higher levels of acceptance than vignettes with private sector actors. This was especially visible in the case of selling data by Internet service providers. We conclude tentatively that this could partly be related to the fact that, in this case, the link between the activity of the actor and the interest of the individual data subject is hardly present: the profits of selling data are for the private actor with no clear profit for the data subject.

The fourth conclusion, finally, is that a high level of privacy awareness negatively affects acceptance levels while a high level of security concern corresponds positively with acceptance levels. The findings of Pavone *et al.* (2012) support this and add trust and concern as mitigators by showing that more trusting citizens consider security as more important and less trusting citizens find privacy more important. Privacy activism significantly affects how respondents value the vignettes concerned with government monitoring. This vignette, in which the government monitors visits to suspect sites, may have been triggered by the Snowden revelations, as this scandal started before the survey was held. However, future research could further study the link between news coverage of privacy scandals and acceptance levels of personal data collection in varying contexts. Likewise, Degli Esposti *et al.* (Chapter 4, this volume) show that users need to be aware of the intrusiveness and risks of surveillance technology to reject the use of it.

The vignettes helped us to create a large data set that reveals the relationship between a large set of independent variables covering attitudes and demographics. In this contribution we only scratched the surface of these relationships. We interpret the results presented in this contribution as an indication that EU citizens assess security and privacy aspects as rather independent values that both need to be secured.

Acknowledgments

Notes

1   The experiment described by Vermeersch and de Pauw (Chapter 3, this volume) demonstrates that framing surveillance technology affects citizens' perception. Similarly,

Mitrou *et al.* (2016, this volume) highlights the importance of framing with a case study of CCTV video in Greece.

2   See (Friedewald *et al.* 2015b) for an extensive overview and discussion on these results.

3   Trust has been part of empirical research since the earlier surveys by Alan Westin. See for instance (Fox *et al.* 2001; Margulis *et al.*2010; Lusoli *et al.* 2012).

4   For a philosophical reflection on the merging or blurring of the boundaries between the online and offline world see (Floridi 2015).

5   We admit that due to the shrinking size of cameras it will become increasingly difficult to really see cameras. The examples we provide however, deal with the requirement to indicate the presence of cameras.

6   We do not deny that the psychology of observation may play tricks with the observed. See Foucault (1995).

7   The World Economic Forum introduces a distinction between voluntary provided information, for instance information people post on social media and of which they are thus aware, and observed data, for instance cookies that are inserted in web pages or GPS-coordinates that are broadcast to third parties. These observed data go mostly unnoticed for people and may conceal the associated activities. See World Economic Forum *et al.* (2012: 19).

8   The institutes mentioned were the (country's) government, the legal system, the police, the press and broadcasting media, businesses.

9   Though we only observe that this influence of age is present, some tentative remarks can be made on this age-related effect. Younger persons may be over-represented as supporters attending football matches, thus rejecting being monitored at a football match. A second argument could be the differences in socio-political profiles between young persons and older persons. This is tentative, and requires further research.

10   Today, most ISPs offer triple play services, i.e. a connection to the Internet, TV-channels and telephony.

References

Ajzen, I. (1991) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes,* 50: 179–211.

Braun, S., Friedewald, M. and Valkenburg, G. (2015) 'Civilizing drones: military discourses going civil', *Science & Technology Studies,* 28: 73–87. Available at: http://ojs.tsv.fi/index.php/sts/article/view/55351 (accessed 6 May 2016).

Budak, J., Rajh, E. and Recher, V. (2016) 'Citizens' privacy concerns: does national culture matter?', in M. Friedewald, P.J. Burgess, J. Čas, R. Bellanova and W. Peissl (eds) *Surveillance, Privacy and Security: Citizens Perspectives*, London: Routledge, 36–51.

Finn, R.L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy', in S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (eds) *European Data Protection: Coming of Age,* Dordrecht: Springer, 3–32.

Floridi, L. (ed.) (2015) *The Onlife Manifesto – Being Human in a Hyperconnected Era,* Heidelberg, New York, Dordrecht, London: Springer.

Foucault, M. (1995) *Discipline and Punishment: The Birth of the Prison,* New York: Vintage Books.

Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T. and Carter, C. (2001) *Trust and Privacy Online: Why Americans Want to Rewrite the Rules,* Washington, DC: Pew Research Center. Available at: www.pewinternet.org/files/old-media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf (accessed 4 May 2016).

Friedewald, M., van Lieshout, M., Rung, S., Ooms, M. and Ypma, J. (2015a) 'Privacy and security perceptions of European citizens: a test of the trade-off model', in J. Camenisch,

S. Fischer-Hübner and M. Hansen (eds) *Privacy and Identity 2014, IFIP AICT, vol. 457,* Heidelberg, Berlin: Springer, 39–53.

Friedewald, M., van Lieshout, M., Rung, S., Ooms, M. and Ypma, J. (2015b) *Report on the Analysis of the PRISMS Survey*. PRISMS Project, Deliverable 10.1. Available at: http://prismsproject.eu (accessed 4 May 2016).

Friedewald, M., van Lieshout, M., Rung, S. and Ooms, M. (2016) 'The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security', in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Dordrecht: Springer, 51–74.

Gellert, R. and Gutwirth, S. (2013) 'The legal construction of privacy and data protection', *Computer Law & Security Review,* 29: 522–530.

General Secretariat of the Council (2010) *Internal Security Strategy for the European Union: Towards a European Security Model,* Luxembourg: Publications Office of the European Union.

Hallinan, D., Friedewald, M. and McCarthy, P. (2012) 'Citizens' perceptions of data protection and privacy', *Computer Law & Security Review,* 28: 263–272.

Hopkins, D.J. and King, G. (2010) 'Improving anchoring vignettes: designing surveys to correct interpersonal incomparability', *Public Opinion Quarterly,* 74: 201–222.

Huijboom, N. and Bodea, G. (2015) 'Understanding the political PNR-debate in Europe: a discourse analytical perspective', *Perspectives on European Politics and Society,* 16: 241–255.

Hundt, R. (2014) 'Saving privacy', *Boston Review – A Political and Literary Forum*. Available at: http://bostonreview.net/forum/reed-hundt-saving-privacy (accessed 7 June 2015).

Kreissl, R., Norris, C., Krlic, M., Groves, L. and Amicelle, A. (2015) 'Surveillance: preventing and detecting crime and terrorism', in D. Wright and R. Kreissl (eds) *Surveillance in Europe,* London, New York: Routledge, 150–210.

Lagazio, M. (2012) 'The evolution of the concept of security', *The Thinker*, 43(9): 36–43.

Lusoli, W., Bacigalupo, M., Lupiañez, F., Andrade, N., Monteleone, S. and Maghiros, I. (2012) *Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management,* Luxembourg: Publication Office of the European Union.

Margulis, S.T., Pope, J.A. and Lowen, A. (2010) 'The Harris-Westin index of general concern about privacy: an exploratory conceptual replication', in E. Zureik, L.L.H. Stalker, E. Smith, D. Lyon and Y.E. Chan (eds) *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons,* Montreal, Kingston: McGill-Queen's University Press, 91–109.

Mitrou, L., Drogkaris, P. and Leventakis, G. (2016) 'Legal and social aspects of surveillance technologies: CCTV in Greece or an attempt to explain some divergent findings of PACT's survey', in M. Friedewald, P.J. Burgess, J. Čas, R. Bellanova and W. Peissl (eds) *Surveillance, Privacy and Security: Citizens Perspectives*, London: Routledge, 123–138.

Pavone, V. and Degli Esposti, S. (2012) 'Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security', *Public Understanding of Science*, 21: 556–572.

Solove, D.J. (2008) '"I've got nothing to hide" and other misunderstandings of privacy', *San Diego Law Review,* 44: 745–772.

World Economic Forum and Boston Consulting (2012) *Rethinking Personal Data: Strengthening Trust,* Cologny, Geneva. Available at: www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (accessed 7 February 2016).

Zedner, L. (2009) *Security,* London, New York: Routledge.

Appendix A – description of the vignettes

1   NSA surveillance

An international disaster relief charity has been sending a monthly newsletter by email to its supporters. The people who run the charity find out through the media that a foreign government has been regularly capturing large amounts of data on citizens of other countries by monitoring their emails. The foreign government says it needs to monitor some communications to help keep its citizens safe and that the main purpose is to focus on terrorism. The charity's officials are unsure whether this means their supporters' personal information is no longer confidential.

2   Biometric logical access control systems

At a local primary school a new system for getting into the school has been installed. All pupils, teachers, parents, other family members and other visitors have to provide their fingerprints on an electronic pad to identify themselves in order to enter or leave the school.

3   SMART grids / meters

A power company has decided to offer smart meters to all its consumers. Smart meters enable consumers to use energy more efficiently by allowing them to see how much they are using through a display unit. The data recorded by smart meters allows power companies to improve energy efficiency and charge lower costs. They also enable power companies to build up a more detailed picture of how their customers use energy. It also enables the companies to find out other things, like whether people are living at the address, or how many people are in the household.

4   Internet monitoring

A student is doing some research on extremism and as part of his work he visits websites and online forums that contain terrorist propaganda. When his parents find out they immediately ask him to stop this type of online research because they are afraid security agencies such as the police or anti-terrorism bodies will find out what he has been doing and start to watch him.

5   ANPR cameras

Michael lives in a suburban neighbourhood, where his children like to play outside with their friends. However, his street is a short cut for commuters who drive faster than the speed limit. In response to complaints from residents, the local authority decides to install automatic number plate recognition (ANPR) systems, which identify and track all vehicles and calculate their average speed. This allows those who drive too fast to be prosecuted.

6   ISP data

VERSION A: companies offering services on the Internet want to sell information about your Internet use to advertisers and other service providers so the information can be used to create more personal offers and deals. This would include the searches you conduct and the websites you visit. Your provider says the information they sell will be anonymous.

VERSION B: companies offering services on the Internet want to sell infor-

mation about their customers' Internet use to advertisers and other service providers so the information can be used to create more personal offers and deals. This would include the searches they conduct and the websites they visit. Their provider says the information they sell will be anonymous.

7   DNA databases
James voluntarily provided a sample of his DNA to a company that carries out medical research. DNA contains the genetic pattern that is uniquely characteristic to each person. He then learns that the research company has been asked to disclose all their DNA samples to police for use in criminal investigations. Samples of DNA can be used to understand potential health problems but also to identify people and to make inferences about who they are related to.

8   Crowd surveillance
VERSION A: Claire is an active member of an environmental group, and is taking part in a demonstration against the building of a new nuclear plant. The police monitor the crowd in various ways to track and identify individuals who cause trouble: they use uniformed and plain-clothes police, CCTV, helicopters and drones, phone-tapping, and try to find people on social media.
VERSION B: David is a football fan who regularly attends home matches. The police monitor the crowd in various ways to track and identify individuals who cause trouble: through uniformed police and plain-clothes police, CCTV, by using helicopters and drones, tapping phones, and by trying to find people on social media.

Appendix B – overview of survey questions

The following question was asked for each of the four vignettes in the survey:

Societal resistance: 'To what extent, if at all, do you think that (actors) should or should not (do this)' with answer options on a 5-point Likert-scale ranging from 'definitely should' to 'definitely should not'.

The following questions were asked only once in the survey:

General security: 'How often, if at all, have you worried about each of the following in your country in the last year?', with answer options on a 5-point Likert-scale ranging from 'most days' to 'never' for the following indicators:

a) Poor people not being able to access healthcare services
b) Youth unemployment
c) Corporate tax evasion
d) Women not being treated as equal to men
e) Terrorist attacks anywhere in your country
f) Young people using alcohol and drugs excessively
g) Extreme weather conditions
h) Viruses damaging the national Internet infrastructure

Personal security: 'And how often, if at all, have you worried about each of the following in the last year?', with answer options on a 5-point Likert-scale ranging from 'most days' to 'never' for the following indicators:

a)   Getting a serious sickness
b)   Losing your job
c)   Being a victim of a theft in your neighbourhood
d)   Being discriminated against
e)   Being a victim of a bomb attack (in your country/in your city)
f)   Immigrant families moving to your neighbourhood
g)   Being a victim of a natural disaster
h)   Someone hacking into your computer

Attitude towards privacy: 'How important, if at all, is it for you to be able to...', with answer options on a 5-point Likert-scale ranging from 'essential' to 'not at all important' for the following indicators:

a)   Know who has information about you?
b)   Control who has access to your medical files?
c)   Use the Internet anonymously?
d)   Make telephone calls without being monitored?
e)   Keep who you vote for in elections private?
f)   Keep your religious beliefs private?
g)   Attend a demonstration without being monitored?
h)   Meet people without being monitored?

Trust in institutions: 'Please tell me on a score of 0–10 how much you trust each of the institutions...', with answer options on a 10-point scale ranging from 'complete trust' to 'no trust at all' for the following institutions:

a)   (Country's) government
b)   The legal system
c)   The police
d)   The press and broadcasting media
e)   Businesses

Privacy activism: 'Have you ever done the following for the purpose of protecting your personal information?', with answer options ranging from 'yes' to 'no' on the following indicators:

a)   Refused to give information because you thought it was not needed
b)   Asked a company to remove you from any lists they use for marketing purposes
c)   Asked a company not to disclose data about you to other companies
d)   Asked a company to see what personal information they had about you in their records

e) Deliberately given incorrect information about yourself
f) Read the online privacy policies on websites

Privacy invasion: 'Have you, to the best of your knowledge, ever felt uncomfortable because you felt your privacy was invaded, in the following situations?', with answer options ranging from 'yes' to 'no' on the following indicators:

a) When you were online
b) When a picture of you was posted online without your knowledge
c) When you were stopped for a security check at an airport
d) When you visited a bank for personal business
e) When you were shopping at a supermarket

2 Citizens' privacy concerns

Does national culture matter?

Jelena Budak, Edo Rajh and Vedran Recher

Culture, privacy and beyond

There is abundant literature on cross-cultural research, and a growing body of scholarly and practitioners' work on privacy issues. However, more in-depth research on cultural variations is still needed to explain views and behaviour related to privacy concerns. This chapter is an attempt to fill a gap in knowledge by linking empirical cultural and privacy studies. It is is an integral part of an extensive research project focused on developing a comprehensive model of online privacy concerns and empirically tests it to provide deeper understanding of various antecedents and consequences of online privacy concerns and their interactions. Past research has identified a number of different antecedents to online privacy concerns, including user-level antecedents that are the focus of our research (see for example Graeff and Harmon, 2002; Dommeyer and Gross, 2003; Yao, Rice and Wallis, 2007). In general, there are three broad categories of user-level antecedents: demographic factors (e.g. gender, education), experience factors (e.g. internet use, web expertise) and socio-psychological factors (e.g. the psychological need for privacy, generalized self-efficacy, belief in privacy rights). Bearing in mind that privacy in an online context refers to 'the rights and interests of an individual that apply to the processing of the information obtained from or about that individual' (Gellman and Dickson, 2011:268), and that advances in IT pose multifaceted challenges to data usage and security (Nemati, 2011), we are led to think of the cultural heritage that shapes our understanding of privacy rights and interests. If cultural attributes change more slowly than rapid technology-induced habits, how does people's online privacy behaviour change in terms of speed and direction? How do individuals manage the balance between privacy, security and acting online? The trade-off between privacy and security (Henderson, 2015) could depend on the cultural characteristics of the given society as well. These are just some of the questions intriguing researchers nowadays.

Within the wider research framework (Figure 2.1), our intuition is that the cultural characteristics of a society determine the level of privacy concerns. Such soft indicators are often used in studies explaining individual sets of values, working habits, and other behaviour patterns of individuals. Almost three decades ago, Triandis (1989) stated that three aspects of the self – private, public, and collective
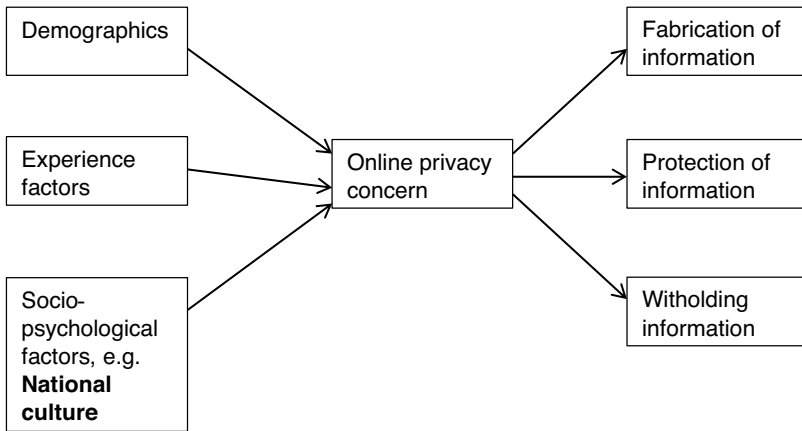
Figure 2.1 Conceptual model of research

– are formed depending on different aspects of the environment, including cultural patterns. Privacy is a much discussed term with different definitions that depend on the legal, social and cultural contexts of privacy. Different cultures have different approaches to privacy, as stated in Gellman and Dixon (2011), and what about culture and privacy concerns when online? As regards privacy, Reed (2014) argues that the internet, in conjunction with other digital technologies, has dealt privacy a severe blow. Although the particular notions of privacy vary from culture to culture, the key issue is whether or not people have control over the disclosure of their personal information. By this definition, privacy has been deeply eroded through the use of digital technologies. However, it has not been fully explored if the cultural attributes of a nation shape citizens' perceptions on privacy, and, if so, in which way. This research sheds some light on this issue.

The chapter is organized as follows. After first presenting a brief research background, we elaborate national cultural dimensions as developed by Hofstede, and their intuitive interactions with online privacy concerns. The survey methodology and method used to construct indices is described in section 4, which is followed by a discussion of the results in section 5. The last section concludes on selected cultural characteristics to be included in the model and suggests a line of future research.

Research background

Alan Westin provided one of the most cited definitions of privacy: 'Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (Westin, 1968:10). Altman (1975) defined privacy as an individual's ability and effort to

control social contacts. Following the theories of general privacy (a review provided by Smith *et al.*, 2011) academic literature recognizes privacy concerns as a growing issue in the digital age, especially for the new EU member states and post-transition countries. The impact of a rather traumatic transformation, marked by considerable distrust in institutions, recalls a number of Hofstede's national cultural dimensions, notably regarding the distribution of power and resources, the balance between individualist and collectivist values, and the threat felt when facing uncertain or unknown situations.

Hofstede's cultural indices have been popular among researchers examining information system security and privacy issues, and studies in this field show that information security concerns in the global financial services sector vary across nations (see Ifinedo, 2011). The study of Bellman *et al.* (2004) claims that differences in internet privacy concerns can be explained by cultural values and internet usage experience, and that these cultural differences are mediated by regulatory differences. These authors posit that regulation can mediate the relationship between cultural values and privacy concerns. As privacy legislation is set at the national level in Croatia, the regulatory framework is the same for all Croatian counties, and this might suppress regional variations in the nexus of privacy concerns and cultural dimensions. Lowry, Cao and Everard (2011) investigate and confirm the relationship between the use of self-disclosure technologies and culture. They find that cross-cultural dimensions are good predictors of information privacy concerns and of the desire for online awareness. Furthermore, Dinev *et al.* (2005) Chiou, Chen and Bisset (2009) and Ur and Wang (2013) all find support for cross-cultural differences with regards to privacy concerns.

As this research examines cultural characteristics at the regional level, there are two streams to consider, both dealing with criticism of Hofstede's national culture dimensions. One stream explores culture that crosses borders, which results in grouping countries into culturally homogenous regions, and the other stream explores cultural differences at the sub-national level, i.e. regional differences within a country. Hofstede and his collaborators, in response to the objection that within countries there might be cultural diversity, found that in a large sample of in-country regions in the world (except Europe), nations do not intermix across the borders (Minkov and Hofstede, 2012). This finding proved to be valid for European regions, as empirically supported in a later study (Minkov and Hofstede, 2014). Regional cultures refer to the diversity of cultures within the same country or to the similarities that may exist between geographical areas belonging, in legal terms, to several countries (Meier, 2004).

Kaasa, Vadi and Varblane (2014) found in the sample of European states that some countries are quite homogeneous while others are not, and that there was no general rule applicable for all of Hofstede's cultural dimensions. The authors conclude that country-level cultural indicators may not be sufficient to represent cultural differences. Hofstede's survey that we applied should also be suitable for a comparison of geographical regions other than countries, i.e. within one nation or across nations, as stated in Hofstede *et al.* (2010). The results of empirical testing of

the meaningful application of Hofstede's national cultural dimensions to compare regions within a country using the sample of Brazil (Hofstede *et al.* 2010) are on the same track: more refined 'cultural' characteristics should be captured to measure and compare sub-national regional differences.

Although the described research provides interesting insights into the cross-cultural topic, and our study offers only a lateral contribution, our main aim is to connect cultural characteristics with online privacy concerns. Within this preliminary research, we empirically test the dimensions of national culture as potential antecedents of online privacy concerns. This study has enabled us to decide whether to include some of the cultural indicators into future research. For this purpose, here we construct an index of privacy concern and national cultural dimension indicators and examine their interrelations. Both sets of indicators were created using data collected in two public surveys in Croatia. Testing the model on the Croatian population is seen as an appropriate way to empirically test the concept and interrelations, especially as it concerns a medium-developed EU country that constitutes part of the digital society.

The privacy concern index is obtained from survey data exploring public attitudes to privacy and behaviour patterns when taking different roles and actions related to online privacy infringements and data protection in Croatia. Budak *et al.* (2013) describe in detail the legal framework of personal data protection and supervision of the collecting, processing and use of personal data in the Republic of Croatia. This is regulated in the Act on Personal Data Protection, which establishes the Croatian Personal Data Protection Agency as an independent and autonomous body for the purpose of supervising the work of personal data processing in the Republic of Croatia. The Croatian Constitution guarantees personal data protection for every person in order to protect the privacy of individuals and other human rights and fundamental freedoms in the process of collecting, processing and use of personal data. Personal data protection guaranteed by the law comprises information on an individual's health, personal identification numbers, data on earnings, school grades, bank accounts, tax refunds, biometrical data, passport or ID card numbers, and so on. Despite this legal framework, privacy protection is often seen as insufficient due to the poor implementation of the law and weak control mechanisms (Budak *et al.*, 2013).

Hofstede's (1980) seminal work points to the way in which certain national cultures determine how businesses in different countries and parts of the world are organized and operate. Our empirical research employs survey data collected in accordance with the Hofstede methodology on national cultural dimensions (http://geert-hofstede.com/) using a large sample of 1,500 citizens. Indicators for five dimensions of national cultures (Power Distance, Individualism vs. Collectivism, Masculinity vs. Femininity, Uncertainty Avoidance, and Long-Term Orientation) are constructed. In the next step, national culture indicators are compared to the privacy concern index at a regional level comprising 21 Croatian counties, as shown in Figure 2.2.

Figure 2.2 Political map of Croatia

National culture

Cultural differences are important to understand human behaviour (Kruger and Roodt, 2003). However, it is difficult to measure and compare the cultural characteristics of various nations. One of the most used methods was developed by Hofstede (1980) who identified the dimensions of national culture and their measures. His assumption was that culture is a 'collective programming of the mind that distinguishes the members of one group or category of people from others' (Hofstede, 2010:5) where the core of culture is formed by common values shared in the society. The five Hofstede dimensions of national culture are shown in Table 2.1.

Power distance is defined as the extent to which the less powerful members of institutions (family, school, etc.) and organizations (workplace) within a country expect and accept that power is distributed unequally. There is inequality in most

Table 2.1 Major characteristics of five cultural dimensions

Dimensions (indicators)	Major characteristics
Power distance (PDI)	• It is defined as the extent to which less powerful members of institutions and organizations within a society expect and accept that power is distributed unequally. • In cultures with small power distance, bosses are not autocratic, subordinates and superiors consider themselves equal and subordinates easily approach and contradict their bosses. There is a preference for consultation. Organizations may be decentralized, while the gap in salaries might be low. • In large power distance cultures, there is considerable dependence of subordinates on bosses. Subordinates are unlikely to approach and contradict their bosses. Organizations centralize power, and subordinates expect to be told what to do. There is a wide gap in salaries, while the superiors have privileges.
Individualism vs. collectivism (IDV)	• It stands for a society in which the interests of the individual prevail over the interests of the group. • In more individualistic cultures, their job leaves employees with sufficient personal time; they are free to adopt their own approach at work, and get from their job a personal sense of accomplishment. Incentives and bonuses should be linked to an individual's performance, while the poor performance of an employee might be the cause of firing. Rich countries score high on individualism, while poor countries usually score high on collectivism. • In less individualistic cultures, people are integrated into strong united groups, and economic life is organized by collectivistic interests. In collectivist societies, training, physical conditions and the use of skills are important. Employers might hire a person who belongs to a group. Incentives and bonuses should be given to the group, not to individuals.
Masculinity vs. Femininity (MAS)	• It refers to the degree to which values are associated with stereotypes of masculinity (such as aggressiveness and dominance) and femininity (such as compassion, empathy, and emotional openness). • High masculinity cultures tend to have stronger emphasis on achievement, earnings, recognition, advancement and challenge in jobs. People are more assertive and show less concern for individual needs and feelings. There are rich and poor masculine and rich and poor feminine countries. • In feminine cultures, managers have a good relationship with employees, and cooperation and employment security are highly valued. Conflicts are resolved by negotiations. Women are also managers. Employees like to live in an area which is desirable for them and their families. Feminine cultures have an advantage in services, consulting, and transportation.
Uncertainty avoidance (UAI)	• Uncertainty avoidance is defined as the extent to which members of institutions and organizations in a society feel threatened by uncertain and unknown situations.

Table 2.1 continued

Dimensions (indicators)	Major characteristics
	• In highly uncertainty avoidance societies, people often feel nervous at work; company rules should not be broken, and they prefer stable jobs and a long-term career with a company. People stick to the rules, prefer a formal life structure and operate in seemingly predictable situations. Uncertainty-avoiding societies have more formal laws, more internal regulations and informal rules controlling work, rights and duties. Consumers in these societies are hesitant about new products and information, and are slower in introducing communication tools. • In weak uncertainty avoidance cultures, only strictly necessary rules are acceptable. People tend to be more innovative and entrepreneurial.
Long-term orientation (LTO)	• It stands for a society that fosters an orientation toward future rewards, persistence, thrift and savings. Wide economic differences are considered undesirable. • In countries with a long-term orientation, planning has a longer time horizon; companies are willing to make substantial investments in employee training and development. • The short-term orientation, a typical western cultural characteristic, reflects values oriented toward present, immediate, short-term results.

Source: Authors based on Hofstede, Hofstede and Minkov (2010)

societies and the Power Distance Index (PDI) measures the degree of inequality in society and how nations deal with inequalities. For example, in small power-distance countries, there is limited interdependence between (a less autocratic) boss and employees, and a preference for consultation, accompanied by small emotional distance, so supervisors or elders can be easily approached. In a small power-distance situation, children are raised to take control of their affairs, to say 'no' very early, to experiment and contradict. Given this explanation of PDI, we would expect less online privacy concern in a small power-distance society and vice versa: more power distance among people is associated with more online privacy concerns.

Individualism vs. collectivism distinguishes cultures that value individual effort over collective work. In collectivist societies, the power of the group is strong. Team effort is highly appreciated, and people are integrated into cohesive in-groups which protect them in exchange for loyalty. Higher values of the Individualism index (IDV) denote the prevalence of individualism over collectivism in society. Hofstede *et al.* (2010) mentioned other studies that have used the IDV index to tackle issues that might be relevant for our research of online privacy concerns. It is worth mentioning that in collectivist societies the internet is less attractive and email less used, because 'people not using Internet have more time

for family and friends and themselves' (Hofstede *et al.*, 2010:123–125). The right to privacy is a key issue in many individualist societies, while in collectivist societies it is seen as a normal right that one in-group member could at any time invade another in-group member's private life. This leads us to believe that online privacy concerns will be greater in a predominantly individualistic environment.

Masculinity in a society denotes assertiveness, as contrasted to femininity. Masculinity is mostly prevalent in societies where emotional gender roles are clearly distinct, and, according to the literature (Hofstede, Hofstede and Minkov, 2010), the former-Yugoslavian republics (including Croatia) are among the masculine societies. The desirability of modest behaviour is associated with femininity. Predominantly feminine societies, such as the Scandinavian countries, tend to find a solution via consensus, and tender, soft values are more often expressed. Feminine societies would opt for a welfare society, while masculine nations strive for a performance society. It is hard to find any intuitive relation between privacy concerns and the masculinity index (MAS): MAS measures societal values, and it should not be confused with the gender of individual respondents which is an important demographic antecedent of online privacy concerns.

Uncertainty avoidance is the extent to which the members of a culture feel threatened by an ambiguous or unknown situation, which should not be understood as risk avoidance. A high Uncertainty Avoidance Index (UAI) denotes a strong tendency in a society to avoid uncertainty. This means that people prefer to have precise instructions and regulations because they feel comfortable in structured environments. A low UAI might in extreme cases denote disrespect for and consternation about rules, but, in less extreme cases, low uncertainty avoidance societies might be more flexible and creative, and have people believing in common sense. The assumed relation between privacy concerns and the UAI is that lower uncertainty avoidance is associated with fewer privacy concerns, and this might be particularly true for nations with proper privacy protection regulations in place.

Long-term orientation (LTO) stands for the fostering of virtues for future rewards, in particular, perseverance and thrift. It is believed that LTO prevails in Asian societies, and that Western type societies are more short-term oriented in relation to the past and present. Privacy concerns in long-term oriented societies are expected to be higher than in short-term oriented environments.

We tested the described potential relations among different dimensions of national culture and privacy concerns using the survey data and the developed indices as described in the following section.

Survey methodology and indices

We used two surveys conducted in Croatia (Table 2.2). Both surveys were based on proportional stratified samples with county and gender as control variables. The first one called 'Privacy survey' was conducted on a nationally representative sample of 506 citizens, as described in detail in Budak *et al.* (2013). For the purpose of this research, we selected three items from the questionnaire, related to the individual level of online privacy concerns. These were the following items:

- Information I send over the internet (email, Facebook and others) could be misused.
- The use of computers and ICT increases the possibility of personal data manipulation.
- I am concerned about the volume of personal information and data stored on computers that might be misused.

These items only partially resemble the scales used in the privacy literature, but their content is suitable for the measurement of online privacy concerns. Items were evaluated on a 5-point Likert scale (ranging from 1 – strongly disagree to 5 – strongly agree) which enabled us to calculate the mean value.

Table 2.2 Survey samples – summary statistics

		Privacy survey (N=506, %)	VSM survey (N=1,500, %)
1.	Gender		
	1.1. Males	50.4	49.8
	1.2. Females	49.6	50.2
2.	Age		
	2.1. 18–24	6.7	13.1
	2.2. 25–34	18.6	21.1
	2.3. 35–44	18.6	20.7
	2.4. 45–54	21.7	22.7
	2.5. 55–65	34.4	22.5
3.	County		
	3.1. Bjelovar–Bilogora	3.0	2.8
	3.2. Brod–Posavina	4.0	3.7
	3.3. Dubrovnik–Neretva	2.8	2.9
	3.4. Istria	4.7	4.9
	3.5. Karlovac	3.2	3.0
	3.6. Koprivnica–Križevci	2.8	2.7
	3.7. Krapina–Zagorje	3.4	3.1
	3.8. Lika–Senj	1.2	1.2
	3.9. Međimurje	2.8	2.7
	3.10. Osijek–Baranja	7.3	7.1
	3.11. Požega–Slavonia	2.0	1.8
	3.12. Primorje–Gorski Kotar	6.7	6.9
	3.13. Sisak–Moslavina	4.4	4.0
	3.14. Split–Dalmatia	10.5	10.6
	3.15. Varaždin	4.2	4.1
	3.16. Virovitica–Podravina	2.2	2.0
	3.17. Vukovar–Srijem	4.7	4.2
	3.18. Zadar	3.6	4.0
	3.19. Zagreb	6.9	7.3
	3.20. Šibenik–Knin	2.6	2.5
	3.21. City of Zagreb	17.4	18.4

At the individual level, the composite measure of online privacy concerns was calculated as the unweighted average of responses on the three selected items. At the county level, the composite measure was calculated as the unweighted average of all individual level composite measures from respondents from the respective county. This measure focuses on information privacy, as this dimension is the most natural to computer-mediated transactions (Preibusch, 2013). The adopted approach obviously abstracts some important dimensions recognized in the literature, such as *collection* and *errors* (Smith, Milberg, and Burke, 1996), or *awareness of privacy practices* (Malhotra, Kim, and Agarwal, 2004). The instrument PRICON[1] used here concentrates on the manipulation and misuse of personal data, which approximates the dimension of *control* of personal information. The main impediment to the conceptualization of privacy concerns that would be more in line with developed measurement scales from the literature was the fact that the survey was not originally designed to encompass all dimensions of the privacy concern latent variable. However, considering the survey constraint, the three chosen items are adequate proxies of general online privacy concerns.

The second survey was conducted in September 2014 on a nationally representative sample of 1,500 Croatian citizens. We used and, for the first time in Croatia, applied the Value Survey Module-94 entirely in line with the VSM-94 methodology developed by Hofstede (1994). Indices of national cultures were calculated using formulas developed by Hofstede to compute five indices of national culture (Table 2.3).

The dimensions can be detected only on the basis of comparative information from at least ten countries or sub-national regions (Hofstede *et al.*, 2010) and this validates our regional set-up of 21 counties. We calculated all measures for each of 21 counties in Croatia and for the aggregate national level (Table 2.4). Values for Hofstede's five indicators range from 0 to 100 (although in some cases, according to the formula, values could be negative or above 100, but here this was not the case). Each of Hofstede's indicators represents a national average calculated on a county basis by using the formulas listed above. This means that Croatian society is predominantly individualistic with a strong uncertainty avoidance and low masculinity index value. The LTO average index value is around the midpoint, so Croatian society as a whole cannot be classified either as long- or as short-term oriented. Power distance is less pronounced in Croatian society. Finally, the index of online privacy concerns (PRICON on a scale from 1 – low privacy concerns to 5 – high privacy concerns) is at the national average, denoting a very high level of online privacy concerns.

The average national levels of cultural characteristics and online privacy concerns are indicative. However, to explore the possible interrelations, we have to use county level data, where each county stands for one region or one sub-society. For methodological consistency, county data were all standardized and then analysed by means of a correlation analysis.

Table 2.3 Hofstede's indices: formulas and items

Formula	Description-statement in the questionnaire

PDI = –35*mean(pdi1)+35*mean(pdi2)+25*mean(pdi3)–20*mean(pdi4)–20

pdi1   In choosing an ideal job, how important it will be for you to have a good working relationship with your direct superior?

pdi2   In choosing an ideal job, how important it will be for you to be consulted by your direct superior in his/her decisions?

pdi3   How frequently are your subordinates afraid to express disagreement with their superiors?

pdi4   To what extent do you (dis)agree that an organization structure in which certain subordinates have two bosses should be avoided at all cost?

IDV = –50*mean(idv1)+30*mean(idv2)+20*mean(idv3)–25*mean(idv4)+130

idv1   In choosing an ideal job, how important will it be to you to have sufficient time for your personal or family life?

idv2   In choosing an ideal job, how important will it be to you to have good physical working conditions (good ventilation and lighting, adequate work space, etc.)?

idv3   In choosing an ideal job, how important will it be to you to have security of employment?

idv4   In choosing an ideal job, how important will it be to you to have an element of variety and adventure in the job?

MAS = +60*mean(mas1)–20*mean(mas2)+20*mean(mas3)–70*mean(mas4)+100

mas1   In choosing an ideal job, how important will it be to you to work with people who cooperate well with one another?

mas2   In choosing an ideal job, how important will it be to you to have an opportunity for advancement to higher-level jobs?

mas3   To what extent can most people can be trusted?

mas4   To what extent do you (dis)agree that when people have failed in life it is often their own fault?

UAI = +25*mean(uai1)+20*mean(uai2)–50*mean(uai3)–15*mean(uai4)+120

uai1   How often do you feel nervous or tense at work?

uai2   To what extent do you (dis)agree that one can be a good manager without having precise answers to most questions that subordinates may raise about their work?

uai3   To what extent you (dis)agree that competition between employees usually does more harm than good?

uai4   To what extent do you (dis)agree that a company's or organization's rules should not be broken, not even when the employee thinks it is in the company's best interest?

LTO = –20*mean(lto1)+20*mean(lto2)

lto1   In your private life, how important is thrift?

lto2   In your private life, how important is respect for tradition?

Source: Authors based on Hofstede (1994).

Table 2.4 National culture indices and online privacy concern composite measure –
    Croatia

Measure	Value
PDI	41
IDV	68
MAS	14
UAI	88
LTO	45
PRICON	4.26

Results and discussion

We calculated Pearson's r correlation coefficients at county level (n=21) in order
to explore the interrelationships between the dimensions of national culture and
online privacy concerns (Table 2.5). The results indicate that there is some corre-
lation between the dimensions of Power Distance and Long-term Orientation and
online privacy concerns (significant at $p<0.1$ level).

   The results could imply that in the regions where less powerful members within
society expect and accept inequality in power distribution, online privacy concerns
would be higher. Also, regions where citizens are more oriented towards future
rewards, and where they show higher levels of perseverance and thrift, are also
regions where the levels of online privacy concerns tend to be higher. In Figures
2.3 and 2.4, the relationships between PRICON and PDI, and PRICON and LTO
are shown.

   Both figures suggest that there is a connection between the level of online
privacy concerns and the two cultural dimensions. The results indicate that coun-
ties that have higher levels of power distance and a long-term orientation tend to
have higher levels of online privacy concerns. While a relatively low R-squared of
0.15 shows that a larger portion of variation is explained by unobserved effects, it
is nevertheless enough to accentuate the need to further explore the culture-
privacy concern nexus.

Table 2.5 Pearson's r correlation coefficients, n=21

	PRICON (r)	*p*
PDI	0.38	0.094
IDV	0.08	0.743
MAS	−0.07	0.760
UAI	0.06	0.780
LTO	0.38	0.093
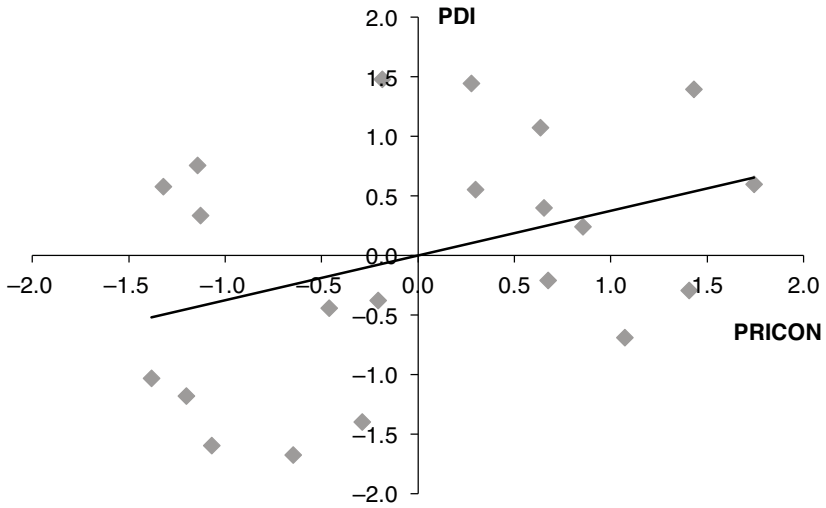
Figure 2.3 PRICON vs. PDI
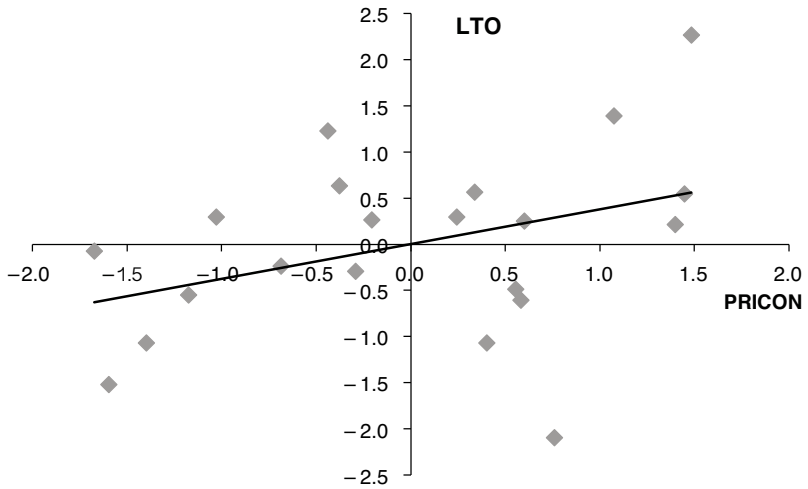
Figure 2.4 PRICON vs. LTO

Concluding remarks and future research

The empirical study presented here examines whether national culture dimensions have an impact on privacy concerns, which ones these are, and which should there-fore be included in a set of socio-psychological factors in an extended model of

privacy concerns. To the best of our knowledge, this is the first research on the interrelations between national cultural dimensions and the level of online privacy concerns.

Our results indicate that there are interrelations worth further exploration, i.e. including some measures of national culture as antecedents of privacy concerns in the online environment. Some measures of culture should be included in an extended model of online privacy concerns, such as Hofstede's Power Distance and Long-term Orientation. There are also various alternative methodologies for measuring national culture in the literature (e.g. Maznevski and DiStefano, 1995, Triandis, 1989, 1995, Schwartz, 1999). Some of them might be an even better methodological choice because of their suitability for calculating measures at the individual respondent level.

This study is limited by several factors that should be addressed in future research. This study has analysed data only at the regional level, because indicators from two different surveys are used. Individual level data might provide additional insights into the interrelations between national cultural dimensions and the level of online privacy concerns. This study has applied one specific conceptualization and measurement of national culture, while further research studies might apply different conceptualizations and measures of national culture in order to better explore the interrelations between national cultural dimensions and the level of online privacy concerns. The same can be said for online privacy concerns. More comprehensive research encompassing a larger diapason of dimensions of online privacy issues is needed.

National culture matters for online privacy concerns, and we will proceed with including some dimensions in the model as antecedents of online privacy concerns. Our intuition goes beyond online privacy concerns: national cultural values play an even more important role for privacy concerns in general and for trust in institutions safeguarding privacy and government regulations. However, this remains to be explored in a new stream of this research, as the analysis conducted above, along with its listed constraints regarding the surveys, has only scratched the surface of this underexplored and vast research area.

Acknowledgement

Note

1   Extended model of online PRIvacy CONcern (PRICON) www.eizg.hr/en-US/
    PRICON-project-(CSF)-1286.aspx

References

Altman, I. (1975) *The Environment and Social Behavior,* Monterey: Brooks/Cole.
Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. (2004) 'International differences in information privacy concerns: A global survey of consumers', *The Information Society, 20*(5): 313–324.

Budak, J., Ani , I. D., and Rajh, E. (2013) 'Public attitudes towards privacy and surveillance in Croatia', *Innovation: The European Journal of Social Science Research, 18*(1–2): 100–118.

Chiou, A., Chen, J.-c. V., and Bisset, C. (2009) 'Cross cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan', in C. Kuanchin, and A. Fadlalla, *Online Consumer Protection: Theories of Human Relativism*, New York: IGI Global, 284–298.

Dinev, T., Masssimo, B., Hart, P., Christian, C., Vincenzo, R., and Ilaria, S. (2005) 'Internet users, privacy concerns and attitudes towards government surveillance – an exploratory study of cross-cultural differences between Italy and the United States', *Proceedings of the 18th Bled eConference: eIntegration in Action, 30,* Bled, Slovenia.

Dommeyer, C., and Gross, B. (2003) 'What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies', *Journal of Interactive Marketing, 17*(2): 34–51.

Gellman, R., and Dixon, P. (2011) *Online Privacy,* Santa Barbara: ABC Clio.

Graeff, T., and Harmon, S. (2002) 'Collecting and using personal data: Consumers' awareness and concerns', *Journal of Consumer Marketing, 19*(4): 302–313.

Henderson, H. (2015) *Online Privacy and Government,* San Diego: Reference Point Press.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work Related Values*, Thousand Oaks: Sage Publications, Inc.

Hofstede, G. (1994) *Value Survey Module 1994 Manual,* Maastricht: IRIC, University of Tilburg.

Hofstede, G., de Hilal, A., Malvezzi, S., Tanure, B., and Vinken, H. (2010) 'Comparing Regional Cultures Within a Country: Lessons from Brazil,' *Journal of Cross-Cultural Psychology, 41*(3): 336–352.

Hofstede, G., Hofstede, G. J., and Minkov, M. (2010) *Cultures and Organizations: Software of the mind* (3rd ed.), New York: McGraw Hill.

Ifinedo, P. (2011) 'Relationships between information security concerns and national cultural dimensions: Findings in the global financial services industry', in H. R. Nemati, *Security and Privacy Assurance in Advancing Technologies*, Hershey-New York: Information Science Reference, 134–153.

Kaasa, A., Vadi, M., and Varblane, U. (2014) 'Regional Cultural Differences Within European Countries: Evidence from Multi-Country Surveys', *Management International Review, 54*(6): 825–852.

Kruger, T., and Roodt, G. (2003) 'Hofstede's VSM-94 revisited: is it reliable and valid?', *SA Journal of Industrial Psychology, 29*(1): 75–82.

Lowry, P., Cao, J., and Everard, A. (2011) 'Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures', *Journal of Management Information Systems, 27*(4): 163–200.

Malhotra, N., Kim, S., and Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model', *Information System Research, 15*(4): 336–355.

Maznevski, M. L., and DiStefano, J. J. (1995) 'Measuring Culture in International Management: The Cultural Perspectives Questionnaire', *The University of Western Ontario Working Paper Series*.

Meier, O. (2004) *Management interculturelle,* Paris: Dunod.

Minkov, M., and Hofstede, G. (2012) 'Is National Culture a Meaningful Concept?: Cultural Values Delineate Homogeneous National Clusters of In-Country Regions', *Cross-Cultural Research, 46*(2): 133–159.

Minkov, M., and Hofstede, G. (2014) 'Clustering of 316 European Regions on Measures of Values: Do Europe's Countries Have National Cultures?', *Cross-Cultural Research, 48*(2): 144–176.

Nemati, H. R. (2011) 'Preface', in H. R. Nemati, *Security and Privacy Assurance in Advancing Technologies,* Hershey-New York: Information Science Reference.

Preibusch, S. (2013) 'Guide to measuring privacy concern: Review of survey and observational instruments', *International Journal of Human-Computer Studies, 71*(12): 1133–1143.

Reed, T. (2014) *Digitized Lives: Culture, Power and Social Change in the Internet Era,* New York and London: Taylor & Francis; Routledge.

Schwartz, S. H. (1999) 'A Theory of Cultural Values and Some Implications for Work'*, Applied Psychology: An International Review, 48*: 23–47.

Smith, H., Dinev, T., and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *Management Information Systems Quarterly, 35*(4): 989–1015.

Smith, J. H., Milberg, S. J., and Burke, S. J. (1996) 'Information privacy: measuring individuals' concerns about organizational practices', *MIS Quarterly, 20*(2): 167–196.

Triandis, H. C. (1989) 'The self and social behavior in differing cultural contexts', *Psychological Review, 96*(3): 506–520.

Triandis, H. C. (1995) *Individualism and Collectivism,* Boulder: Westview Press.

Ur, B., and Wang, Y. (2013) 'A cross-cultural framework for protecting user privacy in online social media', *Proceedings of the 22nd international conference on World Wide Web companion.* International World Wide Web Conferences Steering Committee, 755–762.

Westin, A. F. (1968) *Privacy and Freedom,* New York: Washington and Lee Law Review.

Yao, M., Rice, R., and Wallis, K. (2007) 'Predicting user concerns about online privacy', *Journal of the American Society for Information Science and Technology, 58*(5): 710–722.

3 The acceptance of new security oriented technologies

A 'framing' experiment

Hans Vermeersch and Evelien De Pauw

Introduction

The crisis of 9/11 in the U.S., the London and Madrid bombings in Europe and rapid technological advances have dramatically changed existing paradigms of safety and security. New surveillance oriented technologies have been implemented in an unprecedented way, to prevent crime, track down suspects, victims and witnesses and to guard convicts. The use of these technologies has been legitimized by the 'obligation' to protect society from every thinkable risk.

The tendency towards controlling and limiting risks, aided by new technologies, has been criticized from two perspectives. First, several scholars have warned that Western societies are increasingly evolving towards states of 'overprotection', fuelled by a 'culture of fear' and the idea that 'just because new technologies make new forms of surveillance possible', they should be implemented (Surveillance Study Network, 2006; Vandewalle, De Pauw and Vincent, 2015). Second, the 'silent erosion of privacy' as a result of the use of new technologies by private instances and/or public authorities, often within the grey zones of the law, has been repeatedly criticized.

The 'Panopticon' and associations with 'Big Brother' and 'the Brave New World' abound in popular discourse on surveillance. While these references have some value as a frame for studying the use of new technologies, however, it remains important to evaluate these technologies within a broader perspective. Surveillance, like security, has become the buzzword of our cultural zeitgeist (Aas, Gundhus and Lomell, 2008: 4). Yet, at the same time, the forementioned metaphors are increasingly becoming a liability to the field of research that they helped to promote, and there have been several attempts to break out of the 'panopticon straightjacket' (Boyne, 2000; Lyon, 2006). Scholars of the new generation promote the study of 'technology in action'. They lay focus on its opportunities and more specific consequences its use, without ignoring its negative aspects (Webster, 2012; Taylor *et al.*, 2008).

This so called 'surveillance perspective' (Lyon, 2007; Murakami Wood and Webster, 2009) offers new opportunities for study. Surveillance can be conceptualized as 'goal oriented, and systematic attention for personal data in order to control, govern, manage or protect' (Murakami Wood and Webster, 2009). Surveillance,

defined as such, is not a new phenomenon – all types of governments and instances have tried to monitor citizens – however, it has increasingly been supported and perfected by technology. Observation towers have been replaced by CCTV systems, which were later on upgraded to systems able to deliver high resolution images, record noise, recognize faces and warn operators for suspicious activity. Similar evolutions can be notified with respect to 'access control', 'track and trace'.

New technologies are often implemented without the presence of evidence-based research that legitimizes the hope that 'something will be effective because it appears that it might be effective' or without a careful analysis of potential and unintended consequences (Corbett and Marx, 1991). It has often been assumed, moreover, that 'citizens value security more than privacy' by referring to the 'if you have done nothing wrong, you have nothing to hide' attitude that is common in public opinion.

However, while in general most people tend to deal with privacy issues in a pragmatic way (Westin, 1991), research shows that they do care about privacy and that they are not willing to give public authorities 'carte blanche' when it comes to security. The SurPRISE Project[1] and other projects like PRISMS[2] and PACT[3] have shown that citizens, when extensively informed about the nature of these technologies, find surveillance oriented security technologies (SOSTs) important and necessary to ensure public security. However, simultaneously, they voice concerns and uncertainties due to a perceived lack of control and information, questions of accountability and fears about abuses of power, function and mission creep.

In reality most individuals have little substantial information or knowledge at hand when – in response to a public debate – they form attitudes towards the use of new technologies by public agencies. It has been argued that under such conditions, attitudes may strongly reflect the way these technologies are 'framed' within public discourse and that citizens may rely heavily on the information and cues that are offered within that discourse (Zaller, 1992; Kelley and Mirer, 1974). This paper analyses the sensitivity of citizens for 'framing' effects with respect to the acceptance of the use of new technologies by public authorities. It aims to answer the questions (i) whether or not acceptance depends on the type of frame used and (ii) whether or not pre-existing attitudes (trust in public authorities, privacy concerns, risk perception and technology optimism), that are associated with technology acceptance, moderate the relationship between acceptance and framing of the technology.

Literature

Framing

Frames are 'patterns of selection, emphasis and exclusion (of information) that furnish a coherent interpretation and evaluation of events' (Bali, 2009). As such, a frame references to the way an issue is introduced to the public, with respect to its wording, the images it calls upon and the way it is presented (Chong and Druckman, 2007). When technology is 'framed' – e.g. 'as a tool in the fight against

crime', as a 'threat to privacy', a tool 'to monitor traffic, migration' – citizens are forced to articulate their opinions against the background of these frames.

Research on the effects of frames on opinion formation has a long tradition (Sniderman and Theriault, 2004; Nelson and Kinder, 1996). It has been described as 'a return to the study of the effects of communication content' on opinion (Dorman and Livingston, 1994; Gamson, 1992; Gamson and Modigliani, 1989; Gitlin, 1980; Iyengar and Simon, 1993; Kinder and Herzog, 1993; Kinder and Sanders, 1990; Nelson and Kinder, 1996; Pan and Kosicki, 1993; Patterson, 1993) and has been applied widely by scholars in psychology, political science, and communications studies.

In political communications research, framing typically has been described as the process by which a source (a newspaper or television news story, or perhaps a single individual) defines the essential problem underlying a particular social or political issue, and outlines a set of considerations purportedly relevant to that issue. The effects of such frames have been shown for several policy debates including policy towards ethnic minorities, the welfare state and civil rights (Chong, 1996; Druckman, 2001; Iyengar and Kinder, 1987; Jacoby, 2000; Nelson and Kinder, 1996; Nelson *et al.*, 1997). One study (Nelson *et al.*, 1997), for example, indicates that people find the Ku Klux Klan more acceptable when it is framed as an organization that exercises its right of free expression than when it is proposed as an organization that could be considered as a threat to society.

Based on this kind of studies, 'pessimists' would argue that opinions of citizens towards public issues run only skin-deep: they are the reflection of the information that they are given at a specific moment. The implication is that these opinions are unstable through time and superficial in nature (Zaller, 1992; Kelley and Mirer, 1974). Others, however, have argued that, while 'priming effects' may play a role in opinion formation – especially when the public is not familiar with the topic at hand or lacks the knowledge/skills to evaluate the information available – reality is more complicated (Bali, 2009). Two issues are important in this respect: (i) the question of mixed frames and (ii) the moderating role of pre-existing attitudes.

First, a public debate is seldom 'simple' as such that the people are exposed only to one-sided frames. People receive 'neutral' information and frames and counter frames delivered by conflicting interest groups simultaneously. Framing experiments that are documented in the literature have only compared the effect of one frame compared to a counter frame, while the effects of mixed frames – that may be a more realistic representation of a public debate (Sniderman and Theriault, 2004; Bali, 2009) – are seldom assessed. One could expect that conflicting frames, offered simultaneously, may neutralize framing effects (Sniderman and Theriault, 2004; Chong and Druckman, 2007).

Second, researchers have warned against seeing framing effects as too simple, as a one directional process in which public discourse determines the individual's attitude (Bali, 2009). Frames may influence attitudes, however, people interpret and produce meanings in an active way: they select and weigh the information that is offered to them and may compare it with more or less stable and pre-existing attitudes like socio-political beliefs. This may, in line with cognitive dissonance theory,

result in increasing effects of some frames (that fit pre-existing attitudes) and/or neutralizing or active resistance against frames that contradict pre-existing attitudes (Bali, 2009; Brewer, 2003; Chong and Druckman, 2007). From a researcher's point of view, this would result in frames having a rather small effect that is more conditional rather than direct.

Factors that contribute to technology acceptance

Theories of mass communication increasingly refer to 'framing' as an important aspect of communication by political elites, the mass media, and other agents of political communication. Framing effects reveal how the media may direct public thought and understanding about politics in the absence of ideological biases.

Besides applications within the area of political communication, some scholars have used framing experiments with respect to the public acceptance of technological innovations that may have an impact on our personal live. Schütz and Wiedemann (2008) studied the effect of framing on the perceptions of risks associated with the use of nanotechnology (Schütz and Wiedemann, 2008). One dominant theme is the need to inform the public about facts surrounding new technologies – that is, to make citizens scientifically literate (e.g., Bauer, Allum and Miller, 2007; Miller, 1998). Some researchers argue that new information will presumably enable individuals to more accurately assess the risks associated with new innovations (Druckman and Bolsen, 2001) and form opinions on the acceptability of the use of these technologies. It is assumed that individuals that are scientifically literate may be less susceptible to framing effects.

In this study we apply the concept of framing to public acceptance of SOSTs. The implementation of SOSTs depends on political decision making and decisions are sold to the citizens and/or contested by interest groups, by framing these technologies within the privacy–security debate. Cities who want to implement SOSTs in public space often sell this idea as beneficial to the security of its citizens. Opponents describe its use as a treat towards the privacy. These frames can influence the construction of opinions by citizens, leading to a change in the support for the use of SOSTs.

Scholars who study public acceptance of emergent technologies recognize that individuals form opinions even when possessing little information (e.g., Scheufele *et al.*, 2006) and that attitudes depend on multiple factors beyond factual information. These factors include general values (e.g., Nisbet and Goidel, 2007), trust in science (e.g., Rodriguez *et al.*, 2008), and the framing of the technologies (e.g., Cobb, 2005; Nisbet and Mooney, 2007; Nisbet and Huge, 2007, Scheufele *et al.*, 2006). According to cultural cognition theory 'persons conform their factual beliefs about the risks and benefits of putatively dangerous activity to their cultural appraisals of these activities' (Kahan *et al.*, 2007: 4).

Building on these ideas the impact of the frames on acceptance of SOSTs may depend on values and/or opinions individuals may have. In this study we focus on trust in public authorities, privacy concerns, risk perception and technology optimisms as pre-existing attitudes that may moderate frame effectiveness. We choose

these attitudes as 'candidates' for interacting with frames as (i) studies have repeatedly shown their relevance with respect to technology acceptance and (ii) a clear hypothesis can be formulated on how these variables may interact with frames.

Trust in public authorities. Several studies have indicated that trust in public authorities is an important if not crucial factor when it comes to the acceptability of technology (Knights *et al.*, 2001; Lodge, 2007, Pavone and Degli Esposti, 2010; Bali, 2009). It can be hypothesized that the privacy-frame will be less influential on individuals who trust public authorities to deal with technology in a responsible way.

Privacy concerns have often been studied in relationship with the use of technology (for an overview, see Smith *et al.*, and 2011). Several studies found it an important predictor of support for government policies aimed at increasing safety and security, including the use of new technology. It can be hypothesized that people who score high on privacy concerns will react more strongly when a privacy-frame is used compared to individuals who score low on privacy concerns.

Risk perception with respect to the likelihood of victimization, may be considered a general cognitive assessment of safety (Rountree and Land, 1996). The predominant framework for studying risk perception has been the 'psychometric paradigm' (see Slovic *et al.*, 1980; Slovic, 1992) that argues that perception of the environment or some of its aspects as risky (in contrast to expert risk assessments) is that the indivual's cognitive appraisal of the safety of the environment is important for understanding the construction of opinions on what measures are acceptable to change that environment. While risk perception has been studied in relation to acceptance of technology (Schütz and Wiedermann, 2008), no studies have assessed risk perception as a general cognitive assessment of safety as a factor in the acceptance of new technology in the fight against crime. It is reasonable, however, to hypothesize that individuals that see higher probabilities of becoming victimized by crime will be more eager to support measures to reduce these probabilities. This might be particularly the case when individuals are reminded of the role new technologies can play in the fight against crime.

Technology optimism, may be defined as a positive view of technology and a belief that it offers people increased control, flexibility and efficiency in their lives (Parasuraman, 2000). Several studies have shown that technology optimism is associated with the acceptance of technology. It could be hypothesized that individuals who are optimistic about the possibilities of new technologies may be less concerned about the 'side effects' of technology, leading to decreased sensitivity about privacy related consequences of new technologies.

Research questions and hypotheses

Based on previous research, two research questions (and a set of hypotheses) have been formulated.

- HP1: compared to no-frame:
  - a crime-frame increases the likelihood of technology acceptance
  - a privacy-frame decreases the likelihood of technology acceptance

- a mixed frame cancels frame-effects (and results are more similar to a neutral frame)
- HP2: the effect of frames is dependent on pre-existing attitudes towards the public authorities, privacy concerns, risk perception and technology optimism.

Methodogy

Study design

The study consists of two parts. In the first part, consistent with earlier studies on the effect of frames, four different frames were introduced to the respondents. Respondents were randomized (more information in 'Variables' in this chapter) in four groups that are each 'exposed' to one of the following frames:

(i) A security frame, in which the use of technology is described and promoted as a tool against crime and organized crime.
(ii) A privacy-frame in which respondents are given an description of the technology and are warned against the intrusive character of the technology, potential breaches of privacy that may be the result of its use or abuse.
(iii) A mixed frame that, besides offering a description, stresses the relevance of the new technology in the fight against crime but warns for potential breaches of our privacy.
(iv) A neutral frame that gives an objective description of the technology without references to its potential use and implications with respect to privacy.

Every group was asked to evaluate acceptability (on a scale from '1' meaning 'not acceptable at all' to '7' meaning 'totally acceptable') of the use of four types of technology by public authorities:

(i) The use of smart CCTV within the public space.
(ii) DNA databases that include genetic material of all citizens.
(iii) The use of Radio Frequency Identification (RFID).
(iv) Behavioural profiling.

In the second part of the study design, respondents of all groups had to complete a questionnaire consisting of scales that measured key-variables discussed in the section 'Factors that contributoe to technology acceptance' in this chapter.

Variables

Dependent variable

Total acceptability: sum score of four 'acceptability scores' (RFID, DNA-data files, smart CCTV, behavioural profiling. Acceptability for each form was measured as
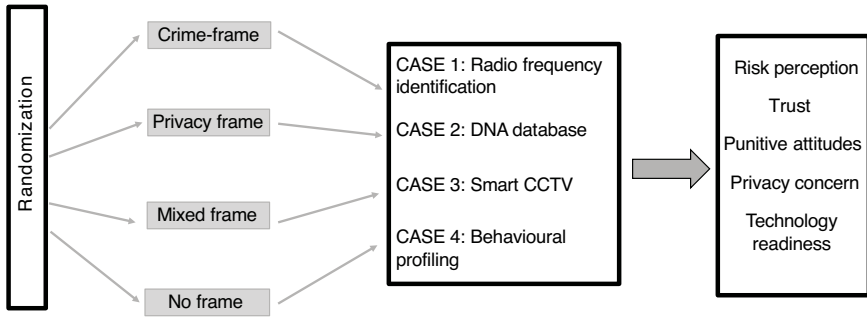
Figure 3.1 Visual representation of the study design

the answer on a '1' ('not acceptable at all') to 7 ('totally acceptable') scale on the question 'Is it, according to you, acceptable that public authorities use this technology?' The total acceptability score was used rather than the individual scores as we have no theory based assumptions to hypothesize that results would depend on the form of technology used.

Independent variables

Trust in public authorities was measured on a 1 ('do not trust at all') to 5 ('high trust') scale by six items that measured trust in specific public authority instances (federal government, federal police, local police, local government, intelligence services…). Cronbach's Alpha for this scale was 0.90.

Risk perception was measured by five items indicating the risk a respondent perceives of being victimized by different forms of crime (aggression, theft, vandalism), on a scale from 1 ('no risk at all') to 5 ('very high risk'). Cronbach's Alpha for this scale was 0.70.

Privacy concerns were measured by items (e.g. 'the public authorities have too much power to track what we do in life') on a scale from 1 ('absolutely disagree') to 5 ('absolutely agree'). Cronbach's Alpha for this scale was 0.72.

Technology optimism was measured by the optimism subscale of the Abbreviated Technology Readiness Index (Victorino *et al.*, 2009; Parasuraman, 2000), that is based on the Technology Readiness Scale (Parasuraman, 2000). This subscale has three items (e.g. 'Technology gives people more control over their daily lives'). Cronbach's Alpha fort his scale was 0.55. Although this is low, corrected item-total correlations varied between 0.25 and 0.43. For this reason we will use this scale, however, with caution.

Frames

As discussed earlier, four types of vignettes were used to frame (security frame, privacy-frame, mixed frame, control frame) the aforementioned technologies. Each vignette consisted of a 'neutral' description of the technology and added information that 'framed' the technology.

The description for smart CCTV, for example is 'In many cities, forms of Smart CCTV are implemented. Some "smart CCTV systems" have the capacity to recognize number plates, record conversations of individuals in the surrounding area. They can "recognize" certain "sounds"/"words"/"noises" and send warnings to operators. Some systems may even recognize faces.' The privacy-frame added to this description is 'Critics argue that these systems are a threat to the privacy of citizens. The possibilities to monitor people are increased substantially in these areas in which such systems are implemented. Conversations between citizens could be monitored by security agents. Abuse of such information is not unthinkable'. The security frame states: 'People who support the use of these systems argue that they are a very useful tool for security agents as they allow to identify situations that are threatening, for example the noise of gun shots, or escalating fights.' The mixed frame was composed by adding both the security and the privacy related information to the neutral description. The neutral frame offered only the neutral description.

Study population

Students of the Department of Applied Social Sciences at VIVES University College were invited to participate in the experiment. Forty percent of the study population (N=438) responded and completed the questionnaire. Seventy-five percent of the respondents were female and the median age was 20 years. As exploratory analyses indicated that the inclusion of gender or age in the analyses did not influence the results, these variables are not included in the final analyses.

Our sample is not a random sample of the Flemish population and earlier studies have indicated that, sociodemographic groups tend to differ in their perspective on safety/security related issues (Heerwegh and Loosveldt, 2009). However the current study does not aim at representing the opinion of the Flemish population on the use of the new technologies by public authorities. The goal of this study is exploratory and aimed at analysing within a clearly defined group, the effect of frames surrounding these technologies, on opinions towards accessibility of use.

Analyses

Anova was used to analyse bivariate associations. General Linear Model (SPSS 20.1) was used to study multivariate associations. The analyses presented in this chapter are limited to the 'sum of accessibility scores of each technology' to avoid an inflation of analyses. The moderating role of frames (interaction-effects) with respect to the association between predicting variables and outcome will be

assessed separately for each predictive variable to avoid high levels of multi-collinearity. Results of the interaction-effects will be presented graphically.

Results

Direct effects: does acceptability differ between groups, depending on frame offered?

The results (Table 3.1 and Figure 3.1) confirm the hypotheses. Frames had a small but consistent effect on the opinion of respondents on the acceptability of technology use by public authorities. This effect, however was only significant for behavioural profiling ($F=2.74$; $p<0.043$) and for the total acceptability score ($F=3.06$; $p<0.028$) indicating that the group exposed to the security frame was more inclined to accept the use of technology than the group exposed to the privacy-frame.

The group that received the 'mixed frame' scored in between the security and the privacy-frame with respect to opinion on acceptability. Outcomes for the 'neutral frame' were, somewhat surprisingly, similar to outcomes of the security frame group. This may be explained, post hoc, by the fact that all four technologies are used primarily (although other applications exist) within the context of safety and security. By consequence it may be impossible to design a neutral frame since mentioning, for example, CCTV in itself already may invoke thoughts and ideas about security.

Does framing affect pre-existing attitudes?

We analysed whether exposure to one of the four frames affected responses with respect to trust in public authorities, privacy concerns, risk perception and technology optimism. No significant differences, however, were found, indicating that the experimental design did not 'contaminate' respondents' answering patterns with respect to pre-existing attitudes. This is an important finding as it means that these pre-existing attitudes themselves are not 'reflections' of framing (and by consequence variable and unstable).

Table 3.1 Frame effects on acceptability for four technologies (and total acceptability scores), results of Anova analysis

	F-statistic	P<
RFID	2.07	0.104
DNA-datafile	0.93	0.427
Smart CCTV	1.73	0.161
Behavioural profiling	2.74	0.043
All technologies (sum-score)	3.06	0.028

Acceptance of use by public authorities (scale 1-7) within different frames

Sum-score for all technologies
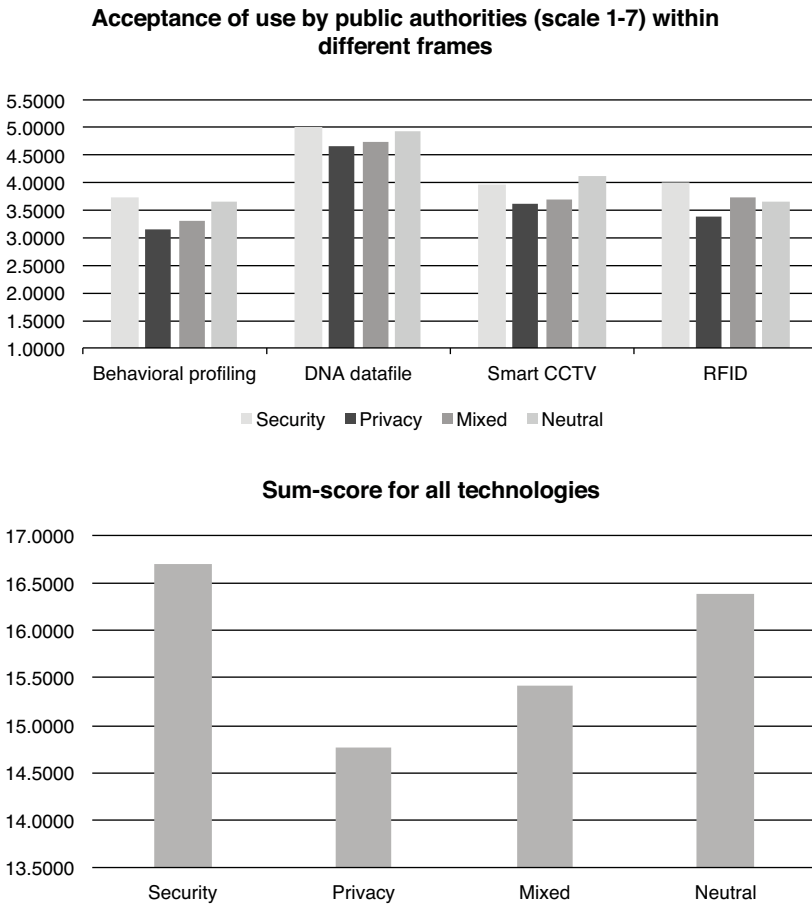
Figure 3.2 Visual representation of the results presented in Table 3.1

Relationship between risk perception, trust, privacy acceptance and total acceptability scores

Trust was negatively associated with risk perception (r=−0.14; p<0.014), privacy concerns (r=−0.31; p<0.001) and positively with technology optimism (r=0.20; p<0.001) and technology acceptance (r=0.32; p<0.001). Technology optimism was negatively associated with privacy concerns (r=−0.17; p<0.002) and positively with technology acceptance (r=0.35; p<0.001). Risk perception was negatively associated with trust (r=−0.14; p<0.014), privacy concerns were negatively associated with technology acceptance (r=−0.35; p<0.001) (visualized in Table 3.2).

Table 3.2 Bivariate associations (Pearson's r) between pre-existing attitudes and technology acceptance

	Risk perception	Privacy concern	Trust	Technology optimism	Technology acceptance
Risk perception	1	0.04	−0.14*	−0.03	0.04
Privacy concern		1	−0.31***	−0.17**	−0.35**
Trust			1	0.20***	0.32***
Technology optimism				1	0.35***
Technology acceptance					1

Notes: (*) $p<0.05$; (**) $p<0.01$, (***) $p<0.001$

Table 3.3 Tests of between-subjects effects' for frames and the interaction-effects with trust, privacy concerns and risk perception with respect to acceptance of technology use by public authorities

	Acceptance of technology use by public authorities					
	F	P<	F	P<	F	P<
Frame	3.58	0.014	3.30	0.021	2.17	0.092
Trust	49.49	0.001				
Privacy concerns			62.31	0.001		
Risk perception					0.62	0.431
Frame * trust	3.05	0.029				
Frame * privacy concerns			3.35	0.019		
Frame * risk perception					2.72	0.044
Adj. R^2	0.15		0.17		0.03	

Trust

Respondents who trust public authorities are strongly inclined to accept the use of technology by these authorities. The interaction between the type of frame and trust (visualized in Figure 3.3) is significant ($F=3.05$; $p<0.029$; Table 3.3) indicating that for when individuals are exposed to a privacy-frame, levels of trust are a stronger predictor of acceptability than when they are exposed to a security frame. By offering a privacy-frame, individuals who are distrustful of public authorities will be triggered to reject use of technologies by public authorities more forcefully.

Privacy concerns

The more respondents are concerned about their privacy, the less they are inclined to support the use of new technologies by public authorities. A significant interaction-effect (visualized in Figure 3.3) between frames and privacy concerns was found ($F=3.55$; $p<0.019$; Table 3.3) indicating that when exposed to a privacy-frame, privacy concerned respondents reacted more strongly (denying public authorities the use of these technologies) than privacy concerned respondents who were exposed to a security frame.
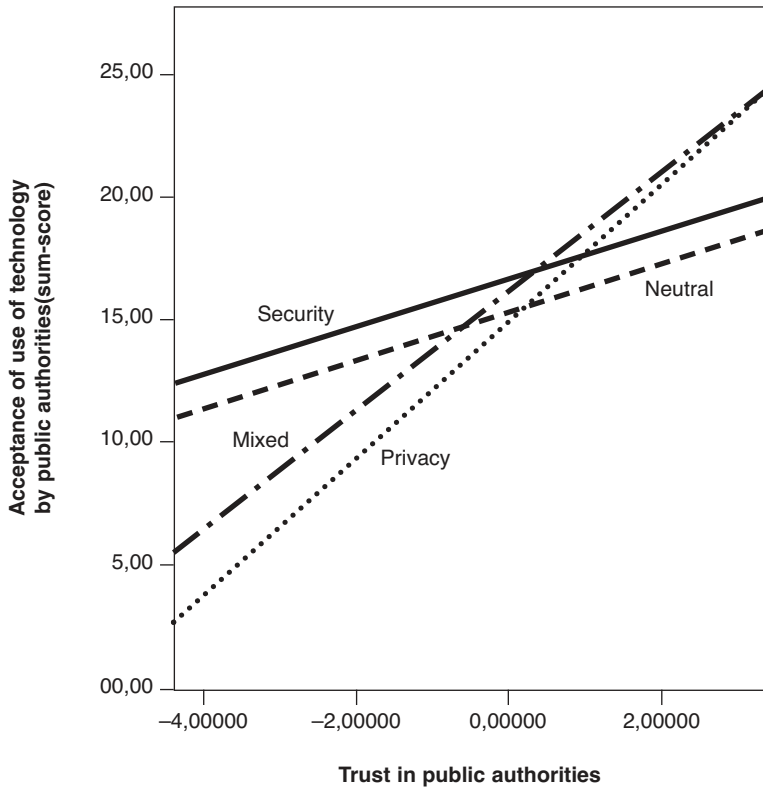
Figure 3.3 Interaction–effect between frames and trust in public authorities

Risk perception

Although no direct association was found between risk perception and opinion on the use of technology by public authorities, a significant interaction–effect (visualized in Figure 3.4) was found ($F=2.72$; $p<0.044$; Table 3.3) indicating that, when exposed to a security frame, respondents who perceived their environment as more risky were more inclined to support the use of these technologies than when exposed to a privacy-frame. In fact, when exposed to a privacy-frame, individuals that were high in risk perception were less inclined to support the use of technology. While this may seem puzzling, it may well be that 'a potential breach of privacy' is interpreted by respondents, high in risk perception as an 'unwanted risk' similar to the risk to become a victim of crime.
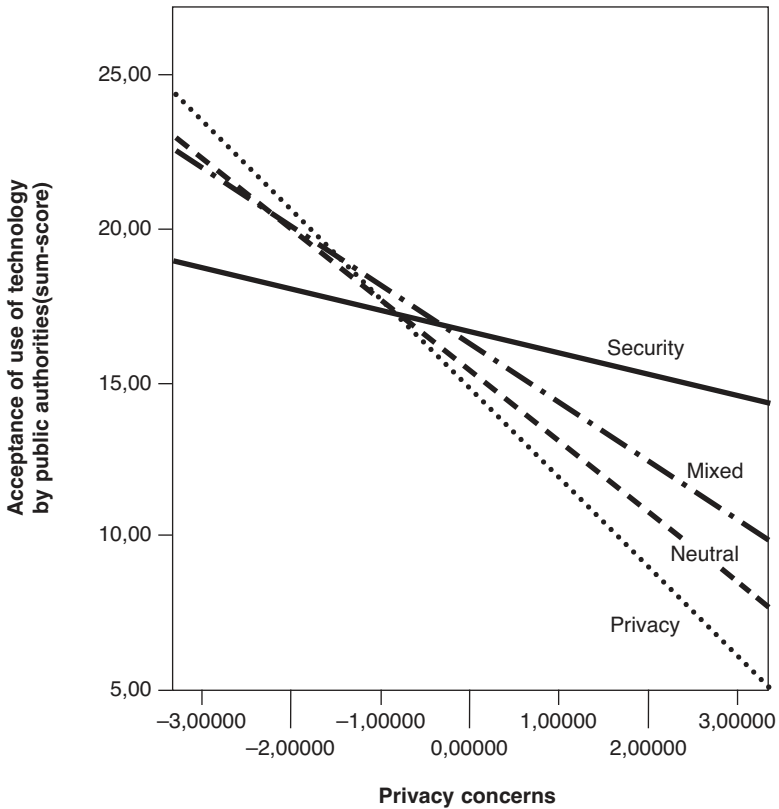
Figure 3.4 Interaction-effect between frames and privacy concerns

Technology optimism

Respondents that were highly optimistic about the use of technology (in general) strongly supported its use by public authorities ($F=48.16$; $p<0.001$; not in Tables) compared to respondents that were low in technology optimism. However, there were no differences between the four framing groups with respect to the relationship between technology optimism and acceptability of technology use.

Discussion and conclusion

Based on a sample of 438 undergraduate students we analysed (i) whether or not acceptance of the use of four types of technology by public authorities depended on the type of frame used to present these technologies and (ii) whether or not pre-existing attitudes (trust in public authorities, privacy concerns, risk perception and technology optimism), that are well-known correlates of technology
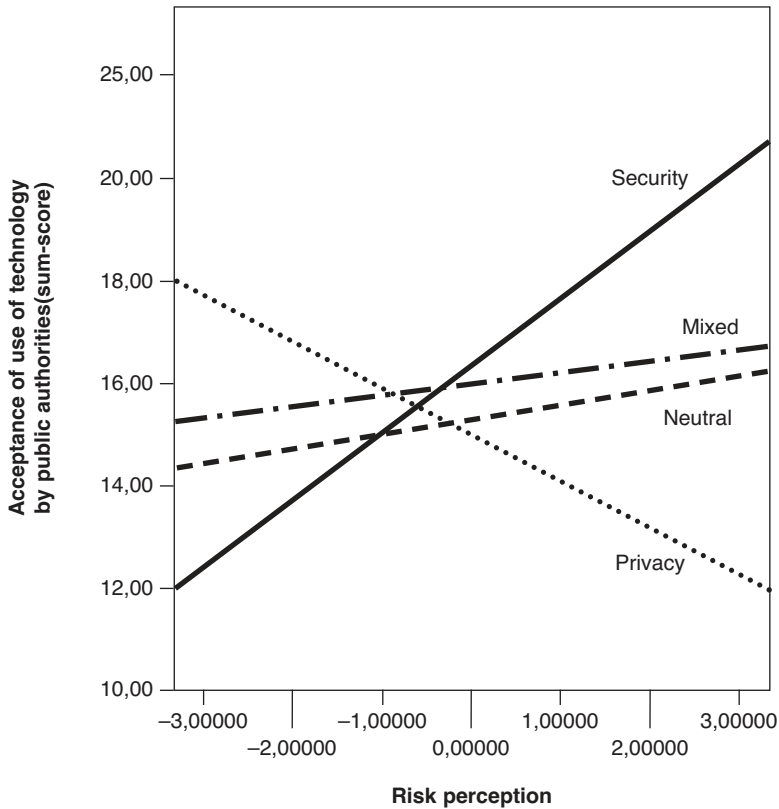
Figure 3.5 Interaction-effect between frames and risk perception

acceptance, moderated the relationship between acceptance and framing of the technology.

The results of our study indicate that the way technologies are 'framed' may influence the opinion of individuals with respect to the use of these technologies by public authorities. Individuals who are exposed to a security frame are more likely to endorse the use of new technologies by public authorities compared to individuals who are exposed to a privacy-frame. A mixed frame (with references to both, security and privacy) invoked responses of acceptability that were in between the privacy and security frame responses. Neutral frames lead to similar results as security frames: it might be that for technology that is primarily, although not exclusively, within a security framework it is impossible for a frame to be neutral as the technology itself invokes cues to security. Although the pattern is consistent across the four technologies, differences between the groups are not always significant. Direct effects of the frames are as such relatively small.

Earlier studies on the effects of framing have shown that frames may influence the inferences of causality that individuals make (Iyengar, 1991). By stressing or highlighting specific elements within a more diffuse debate, they are narrowing that debate to one or two central concerns. It may not be necessary that the information that is delivered by a frame is new to be effective. According to the priming and/or cognitive accessibility model individuals are limited in the capacity to store and process information. This implicates that only a subset of all relevant ideas is involved in the formation of socio-political judgements (Zaller, 1992). Accessibility models stress that information should be available at hand to be influential. Not all information, however, is of equal weight and importance. Moreover the recipients of the information make an interpretation and/or gave different weights to some pieces of information than to others. For this reason, the effect of frames might not be independent from pre-existing knowledge/attitudes. The results of our analyses support this idea.

Individuals who perceive their environment as more risky, as such that they believe they are more in favour of the use of new technologies when exposed to a security frame than when exposed to a privacy-frame. Individuals who are privacy concerned react aversively to the use of new technologies by public authorities when exposed to a privacy-frame, while for individuals who are low in privacy concern, a privacy-frame did not have a similar impact. Last but not least the willingness of individuals within the privacy-frame to support the use of new technologies depended largely on whether they trust the public authorities or not, while within a security frame trust was a weaker predictor of support.

Although framing experiments can only reflect a real public debate in a very simplified way, they may show us how 'sensitive' individuals are for certain arguments. Individuals are sensitive for both arguments, security and privacy, but not always in a way that radically changed their minds. Effects of more general pre-existing tendencies such as trust, privacy concern are not 'overruled' by exposure to a specific frame. Often they are reinforced or somewhat weakened. Respondents, as such, seem particularly sensitive for information that appeals to these pre-existing tendencies. The results of our study do not allow us to share the pessimism of some scholars about the quality and depth of public opinion. Individuals' opinions are more than a mere reflection of the information offered to them at a given moment and as such less variable and superficial than some (Zaller, 1992; Kelly and Mirrer, 1974) may fear.

The interpretation of the results of our study – although consistent and similar to the results of earlier studies on framing (Chong, 1996; Druckman, 2001; Iyengar and Kinder, 1987; Jacoby, 2000; Nelson and Kinder, 1996; Nelson *et al.*, 1997) – are hindered by some limitations. First, our study population consisted of undergraduate students. The data presented cannot be considered as representative for the opinions of the Flemish population. Moreover it remains uncertain how experience with and/or knowledge of technology – which may be higher/lower in other segments of the population – may have affected the results of this study. At least in theory, one could expect that the effects of framing will be more pronounced in groups with less experience with/knowledge at hand of the technology of its implications.

Second, our experimental design did not take into account the contextual aspect that individuals may consider when expressing their opinion with respect to the use of new technology within the security landscape. Findings from the SurPRISE Project, in which the opinion of the inhabitants of the 27 European member states was assessed, indicate that support of new surveillance oriented technologies is strongly dependent on the scope and the goal of the surveillance. If transparency exists with respect to goals, targets, places and priorities, people are more inclined to support its use (Čas, 2014). The use of technology for more commercial goals (e.g. CCTV systems that monitor shopping behaviour aimed at sending personalized advertisements) or within private spaces is far less supported.

Summarizing, this study shows that framing new technologies may influence support for its use by public authorities, however, that influence is more indirect, by moderating the relationship between pre-existing attitudes and support. As such our results support the notion that although individuals are not immune against their effects, framing may reinforce the effects of pre-existing attitudes, rather than dramatically alter technology acceptance within the public opinion.

Notes

1   Surveillance, privacy and security: a large scale participatory assessment of criteria and factors determining acceptability and of security technologies in Europe, FP7, 2012–2015. See Strauß (this volume, Chapter 14).
2   Privacy and Security Mirrors, FP7, 2012–2015. See van den Broek *et al*. (this volume, Chapter 1).
3   Public Perceptions of Security and Privacy, FP7, 2012–2015.

References

Aas, K.F., Gundhus, H.O., and Lomell, H.M. (eds) (2008) *Technologies of insecurity: the surveillance of everyday life*, London: Routledge.

Bali, V. (2009) 'Tinkering toward a national identification system: an experiment on policy attitudes', *The Policy Studies Journal*, 37(2): 233–255.

Bauer, M. W., Allum, N., and Miller, S. (2007) 'What can we learn from 25 years of PUS survey research? Liberating and expanding the agenda', *Public Understanding of Science*, 16(1): 79–95.

Boyne, R. (2000) 'Post-panopticism', *Economy and Society*, 29: 285–307.

Brewer, P.R. (2003) 'Values political knowledge and public opinion about gay rights: a framing based account', 67: 173–201.

Čas, J. (2014) Surveillance, privacy and security: a large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe, Presentation, Joint Conference of the SurPRISE, PACT, PRISMS projects, Vienna, 13–15 November 2014.

Chong, D. (1996) 'Creating common frames of reference on political issues', in D.C Mutz, P.M. Sniderman, and R. A. Brody (eds), *Political persuasion and attitude change*, Ann Arbor, MI: University of Michigan Press, 195–224.

Chong, D. and Druckman, J. (2007) 'Framing public opinion in competitive democracies', *American Political Science Review*, 101(4): 637–655.

Cobb, M.D. (2005) 'Framing effects on public opinion about nanotechnology', *Science communication*, 27(2): 221–239.

Corbett, R. and Marx, G.T. (1991) 'Critique: no soul in the new machine: technofallacies in the electronic monitoring movement', *Justice Quarterly*, 8(3): 399–414.

Dorman, W.A., and Livingston, S. (1994) *News and historical content. Taken by storm: the media, public opinion, and US foreign policy in the Gulf War*, Chicago, IL: University of Chicago Press.

Druckman, J.N. (2001) 'On the limits of framing effects: who can frame?, *Journal of Politics*, 63(4): 1041–1066.

Druckman, J.N. and Bolsen, T. (2011) 'Framing, motivated reasoning, and opinions about emergent technologies', *Journal of Communication*, 61(4): 659–688.

Finn, L., Wright, D., and Friedewald, M. (2013) 'Seven types of privacy', in S. Gutwirth, R. Leenes, P. de Hert, and Y. Poullet (eds) *European Data Protection: Coming of Age,* Dordrecht: Springer, 3–32.

Friedewald, M. (2014) 'Key results of the PRISM Project', Presentation, Joint Conference of the SurPRISE, PACT, PRISMS projects, Vienna, 13–15 November 2014.

Gamson, W.A. (1992) *Talking politics*, Cambridge: Cambridge University Press.

Gamson, W.A. and Modigliani, A. (1989) 'Media discourse and public opinion on nuclear power: a constructionist approach', *American Journal of Sociology*, 95(1): 1–37.

Gitlin, T. (1980) *The whole world is watching: Mass media in the making and unmaking of the new left*, Berkeley, CA: University of California Press.

Heerwegh, D. and Loosveldt, G. (2009) 'Verbeteren mixed mode surveys de representativiteit van de Veiligheidsmonitor?', *Panopticon*, 30(5): 72–75.

Iyengar, S. (1991) *Is anyone responsible? How television frames political issues,* Chicago, IL: University of Chicago Press.

Iyengar, S. and Kinder, D.R. (1987) *News that matters: Television and American opinion,* Chicago, IL: University of Chicago Press.

Iyengar, S. and Simon, A. (1993) 'News coverage of the Gulf crisis and public opinion a study of agenda-setting, priming, and framing', *Communication Research*, 20(3): 365–383.

Jacoby, W. G. (2000) 'Issue framing and public opinion on government spending', *American Journal of Political Science*, 44(4): 750–767.

Kahan, D.M., Braman, D., Gastil, J., Slovic, P., and Mertz, C. K. (2007) 'Culture and identity – protective cognition: explaining the white-male effect in risk perception', *Journal of Empirical Legal Studies*, 4(3):465–505.

Kelley, S. and Mirer, T. W. (1974) 'The simple act of voting', *American Political Science Review*, 68(2): 572–591.

Kinder, D.R. and Herzog, D. (1993) 'Democratic discussion', in G.E. Marcus and R.L. Hanson (eds), *Reconsidering the democratic public*, Pennsylvania, PA: Penn State University Press.

Kinder, D.R. and Sanders, L.M. (1990) 'Mimicking political debate with survey questions: the case of white opinion on affirmative action for blacks', *Social Cognition*, 8(1): 73.

Knights, D., Noble, F., Vurdubakis, T., and Willmott, H. (2001) 'Chasing shadows: control, virtuality and the production of trust', *Organization Studies*, 22(2): 311–336.

Lodge, J. (2007) 'Biometrics: a Challenge for privacy or public policy-certified identity and uncertainties', *Minority, Politics, Society*, 1: 193–206.

Lyon, D. (ed.). (2006) *Theorizing surveillance*, Londen: Routledge.

Lyon D. (2007) *Surveillance studies. An overview,* Cambridge: Polity Press.

Miller, J.D. (1998) The measurement of civic scientific literacy, *Public understanding of science*, 7(3): 203–223.

Murakami Wood, D. and Webster, C.W.R. (2009) 'Living in surveillance societies: the normalisation of surveillance in Europe and the Threat of Britain's bad example', *Journal of Contemporary European Research*, 5(2): 259–273.

Nelson, T.E. and Kinder, D.R. (1996) 'Issue frames and group-centrism in American public opinion', *Journal of Politics*, 58: 1055–1078.

Nelson, T.E., Clawson, R.A., and Oxley, Z.M. (1997) 'Media framing of a civil liberties conflict and its effect on tolerance', *American Political Science Review*, 91(3): 567–583.

Nelson, T.E., Oxley, Z.M., and Clawson, R.A. (1997) 'Toward a psychology of framing effects', *Political behavior*, 19(3): 221–246.

Nisbet, M.C. and Goidel, R.K. (2007) 'Understanding citizen perceptions of science controversy: bridging the ethnographic – survey research divide', *Public Understanding of Science*, 16(4): 421–440.

Nisbet, M.C. and Huge, M. (2007) 'Where do science debates come from? Understanding attention cycles and framing', in D. Brossard, J. Shanahan, and T.C. Nesbitt (eds), *The media, the public and agricultural biotechnology,* Wallingford, UK: CAB International, 193–230.

Nisbet, M.C. and Mooney, C. (2007) 'Thanks for the facts. Now sell them', *Washington Post*, April 15, B3.

Pan, Z. and Kosicki, G.M. (1993) 'Framing analysis: an approach to news discourse', *Political Communication*, 10: 55–75.

Parasuraman, A. (2000) 'Technology readiness intex (TRI): a multiple-item scale to measure readiness to embrace new technologies', *Journal of Service Research*, 2(4): 307–320.

Patterson, Thomas E. (1993) *Out of Order*, New York: Alfred A. Knopf.

Pavone, V. and Degli Esposti, S. (2012) Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security, *Public Understanding of Science*, 21: 556–572.

Rodriguez, K.L., Gambino, F.J., Butow, P.N., Hagerty, R.G., and Arnold, R.M. (2008) 'Its going to shorten your life: framing of oncologist–patient communication about prognosis', *Psycho-Oncology*, 17(3): 219–225.

Rountree, P.W. and Land, K.C. (1996) 'Perceived risk versus fear of crime: empirical evidence of conceptually distinct reactions in survey data', *Social Forces*, 74(4): 1353–1376.

Scheufele, D.A., Hardy, B.W., Brossard, D., Waismel-Manor, I.S., and Nisbet, E. (2006) 'Democracy based on difference: examining the links between structural heterogeneity, heterogeneity of discussion networks, and democratic citizenship', *Journal of Communication*, 56(4): 728–753.

Schütz, H. and Wiedemann, P.M. (2008) 'Framing effects on risk perception of nanotechnology', *Public Understanding of Science*, 17(3): 369–379.

Slovic, P. (1992) 'Perception of risk: reflections on the psychometric paradigm', in S. Krimsky and D. Golding (eds) *Social theories of risk,* Westport, CT: Praeger, 17–152.

Slovic, P., Fischhoff, B., and Lichtenstein, S. (1980) 'Facts and fears: understanding perceived risk', in R.C. Scwing and W.A. Albers, Jr., *Societal risk assessment*, New York: Springer, 181–216.

Smith, H.J., Dinev, T., and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS quarterly*, 35(4): 989–1016.

Sniderman, P. and Theriault, S. (2004) *Studies in public opinion: attitudes, nonattitudes, measurement error, and change*, Princeton, NJ: Princeton University Press.

Surveillance Studies Network (2006) 'Report on surveillance society, 2006', available at Surveillance Studies Network.

Taylor, J. S. (2008) *The public life of the fetal sonogram: Technology, consumption, and the politics of reproduction,* New Brunswick, NJ: Rutgers University Press.

Vandewalle, G., De Pauw, E., and Vincent, J. (2015) 'Gedigitaliseerde veiligheid vandaag vanuit een realistisch perspectief', in G. Vandewalle, S. De Kimpe, E. De Pauw, and J. Vincent (eds), *Panoptisme in de veiligheidketen: een moeilijk evenwicht tussen technologie en mensenrechten? Themanummer Orde van de dag,* Dordrecht: Kluwer, 10–24.

Victorino, L., Karniouchina, E., and Verma, R. (2009) 'Exploring the use of the abbreviated technology readiness index for hotel customer segmentation', *Cornell Hospitality Quarterly*, 50(3): 342–359.

Webster, W. (2012) 'Surveillance as X-ray: understanding the surveillance state', in W. Webster, G. Clavell, N. Zurawski, K. Boersma, B. Sagvari, C. Backman, and C. Leleux (eds), *Living in surveillance societies: the state of surveillance.* LISS, COST, University of Stirling and UOC.

Westin, A. F. (1991) *Harris-Equifax consumer privacy survey 1991*, Atlanta, GA: Equifax Inc.

Zaller, J. (1992) *The nature and origins of mass opinion,* Cambridge: Cambridge University Press.

Zedner, L. (2009) 'Epilogue: the inescapable insecurity of security technologies?', in K. Aas, H. Oppen Grundhus, and H. Lomell (eds), *Technologies of insecurity,* New York: Routledge.

4 Aligning security and privacy

The case of Deep Packet Inspection

*Sara Degli Esposti, Vincenzo Pavone and
Elvira Santiago-Gómez*

Introduction

When surveillance functionalities are embedded into security tools and systems the risk of facing a backlash, due to widespread privacy concerns, may increase dramatically. Speed enforcement cameras, for instance, have produced strong resistance in the UK since 2001 (Wells and Wills, 2009). By the same token, in 2008 the prospect of deploying body scanners in EU airports raised serious public concerns and produced strong public opposition (Bellanova and González Fuster, 2013). As explored by van den Broek *et al.* in this volume, on the one hand, individual privacy concerns may contribute to increase public resistance to surveillance technologies; on the other hand, the perceived trustworthiness of the institutions, or entities, in charge of managing the surveillance system may contribute to decrease public resistance. However, many other factors may also play a role. Thus, at the time of deploying a new surveillance-based security measure, it is hard for developers and product designers to imagine all end-users' reactions and to foresee the kind of concerns the technology will eventually trigger.

Understanding the reasons behind, and the manifestations of, public resistance to surveillance technologies is certainly a complex task. Resistance to surveillance technologies may produce a wide range of public reactions, from simple avoidance to active opposition (Marx, 2003). Cultural, historical, and sociological factors may also influence both public perceptions and privacy and security attitudes (Pavone and Degli Esposti, 2012). Resistance to surveillance is also often based on existing knowledge about technologies (Ball, 2002), which implies that people's educational level and the degree of familiarity with the technology may also contribute to orient public opinion. As pointed out by van den Broek *et al.* in this volume, citizens' political opinions may also play a role in the context of a political demonstration.

Finally, the prevailing tendency to frame privacy and security as antagonistic values in security policy discourses, as pointed out by Strauß in this volume, have also prevented the academic community from achieving a deeper understanding of individual privacy concerns, security attitudes and public resistance to surveillance. To overcome these limitations, the SurPRISE Project was designed to challenge the privacy–security trade-off framework by empirically investigating

factors influencing public attitudes toward surveillance technologies, in line with previous exploratory studies (Pavone and Degli Esposti, 2012).

This chapter aims at shedding light on the complex phenomenon represented by public resistance to, or acceptance of, surveillance technologies used to ensure human security, by offering insights on a particular surveillance technology, which is Deep Packet Inspection (DPI). We rely on both quantitative data gathered in six European countries and qualitative data gathered in the UK to draw our conclusions. Based on the analysis of the data, we offer evidence of the detrimental effects that a technology's perceived degree of intrusiveness exercises on a technology's perceived effectiveness. In other words, we find empirical support for the claim that security and privacy, being part of a broader concept of human security, are compatible rather than antagonistic dimensions. In addition, we offer preliminary evidence of the negative effects caused by the adoption of blanket-surveillance security strategies on end–users' perceptions.

Digital surveillance, individual privacy concerns and technological acceptance

For a long time, dominant interpretations of opinion pool data on individuals' privacy concerns have led the academic community to believe in the existence of a *privacy paradox*, which can be summarized in a simple statement: 'despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances' (Smith *et al.*, 2011, 993). However, recent studies have challenged this interpretation and questioned the assumption that people adopt a cost-benefit approach when it comes to privacy risky data sharing decisions (Turow *et al.*, 2015).

Frequently users do not fully understand they are sharing their personal data for free services and apps. Often users feel they have no choice but sharing their data and, as a result, they feel resigned (Turow *et al.*, 2015). Many people tend to believe that the regulatory system in place protects their right to privacy and intimacy (Hoofnagle and Urban, 2014), even in the absence of their active mobilization, as it happens in the case of food labelling or medical treatments. Very often people inaccurately believe that the law protects them from third-party data sharing activities (Hoofnagle and Urban, 2014). In the case of location apps, users are also often unaware of the monitoring functions embedded into the same device. When users become aware of the data processing functionalities of mobile apps they might feel betrayed and, as a result, outraged (Shklovski *et al.*, 2014, Xu *et al.*, 2011). This might be the reason why, when confronted with the prospect of losing control over their personal data, the vast majority of users of online services express their concerns. For instance, as reported by van den Broek *et al.* within this volume, lay people consider especially unacceptable that Internet Service Providers (ISPs) sell customer data. Therefore, the *privacy paradox* (Acquisti, 2010) not only appears to be an interpretation far too simplistic, unable to map the complex set of emotions generated by modern digital surveillance practices (Shklovski *et al.*, 2014), but it also shifts the responsibility of data and privacy protection to individual citizens, away from the corresponding public authorities.

When lay people discover dataveillance (Degli Esposti, 2014; Clarke, 1988), they tend to react in a negative way. Sometimes, they perceive digital surveillance as something inevitable, an intrinsic part of the digital revolution; as a consequence they feel resigned and tend to succumb to it just because they do not want to miss the relational and job opportunities the Web offers (Turow *et al.*, 2015). Without these opportunities, many individuals, and especially the 'digital natives', are likely to feel unable to achieve full integration in our society. A minority of people, nonetheless, try to avoid, evade or circumvent surveillance by adopting different strategies, from the intentional provision of inaccurate information, to the adoption of anonymization and privacy-preserving tools.

Recent scandals showing the ability of governments and private firms to constantly monitor citizens and consumers have exacerbated the situation making people feel even more powerless, vulnerable and exposed (Ball, 2009). From an organizational perspective, mass surveillance has become so cheap, and its applications so numerous, that it is just easier to find arguments to justify its adoption, and contribute to its proliferation, than to question it (Hoofnagle *et al.*, 2012). Digital technologies have transformed surveillance performed by security agencies from a time-consuming and expensive practice into a technological routine so convenient that the asymmetry of power between citizens and the State has increased dramatically (Bankston and Soltani, 2014).

Within this scenario, it becomes especially urgent and necessary to renew current efforts to analytically explore how citizens interpret surveillance-oriented security technologies (SOSTs), i.e. those technologies that are being introduced in order to improve human, public or national security, and what, in the common pursuit of higher security, they expect from these technologies. If living in a surveillance society (Murakami Wood, 2009) might generate a sentiment of resignation and a sort of passive behaviour, we should nonetheless distinguish between those who actually support the adoption of certain surveillance measures, from those who are not happy with these solutions, but have not been able to demonstrate their dissent yet. Moreover, in current times characterized by a growing mistrust towards security agencies and public institutions (Gandy, 1989, Verble, 2014), understanding and rethinking the relationship between privacy, security and surveillance becomes extremely important for the future of democratic societies (Bauman *et al.*, 2014).

To shed light on these issues, this chapter focuses specifically on public perceptions of Deep Packet Inspection (DPI), and relies on both qualitative and quantitative data to investigate the complex articulation of arguments, factors and priorities influencing citizens' acceptance of surveillance measures used for security purposes.

The distinction between public acceptance and acceptability of DPI

Within this study, we use quantitative data to study those factors influencing *public acceptance of DPI*, while we tried to use qualitative data to explore *public acceptability of DPI*. Unfortunately, within this study we could not gather enough qualitative data

to fully explore the issue of public acceptability of DPI. Nevertheless, some considerations regarding this topic are included in the next section and a clear conceptual distinction between acceptance and acceptability is provided in the next paragraphs.

In order to clarify our terminology, a clear distinction between public acceptance and acceptability of technology needs to be made. We consider that a technology is accepted (i.e. *public acceptance of technology*) when it is received neutrally, or favourably, and the population of the region, or country, where the measure is adopted not only does not engage in any form of collective, or individual, action meant to create disruptions to the deployment and implementation of the technology by complaining, protesting, refusing to use the solution or opposing it in any way, but actively supports its deployment. According to this definition public acceptance is the opposite of public resistance.

In contrast, we say that a technology is acceptable (i.e. *public acceptability of technology*) when it has the potential of being endured, because the measure is tolerable, adequate and conforms to approved societal or ethical standards. While technological acceptability represents a forward-looking concept which entails some ethical criteria, which help us judge the appropriateness, or legitimacy, of a technology, acceptance is a backward-looking idea and can only be used to assess the extent to which a technology, which has been already adopted in a certain social and cultural context, has triggered public opposition or acquaintance.

Although in policy documents (EC, 2012), and in the academic literature (Siegrist, 2008, Venkatesh *et al.*, 2003), the construct most widely used is public acceptance, the idea of acceptability deserves to be further investigated as it may help identify controversial aspects of technologies in phase of design and as it may suggest criteria or guidelines for improving the design and management of technological systems. Nonetheless, we expect that technologies which are considered *acceptable* by the public are also technologies *accepted* by the public. Although acceptance and acceptability are two interrelated ideas, public acceptance does not necessarily imply acceptability from a legal or human rights perspective. Surveillance technologies may enjoy high public acceptance but still run contrary to established human rights, or national constitutional principles, or to existing regulation. Sometimes public acceptance can be the result of repression, lack of freedom of expression or simple inertia or lack of information.

Finally, we should remember that security technologies differ from consumer technologies because they are used to monitor and protect the public, but they are not chosen or operated by the public. In the case of security technologies, which are not chosen by citizens, but by security agencies and public authorities, we consider that the study of SOSTs' acceptability is especially important and should be developed further in future empirical studies. Although SOSTs are used to protect citizens and to prevent, or respond to, security threats, citizens are not involved in the design and selection of security measures. This lack of participation in the decision-making process reduces drastically the impact of public opinion on the development of security technologies. By better understanding the criteria lay people use to assess the acceptability of SOSTs, scholars could help governments and security agencies develop more sensible solutions (Hess, 2014).

The data collection

Data presented in this chapter were gathered as part of the SurPRISE project, funded by the *Seventh Framework Programme for Research and Innovation*, between January and March 2014, during 12 citizen summits held in nine European countries, involving approximately 200 citizens per country. The SurPRISE citizen summits were full-day events. Participants received information before and during the event, discussed topics related to specific SOSTs in small groups of six to eight persons, and filled in an electronic questionnaire along the day. As concluding activity each group of citizens was asked to formulate recommendations for policymakers to be used. Summit participants had also the chance to write their thoughts on individual postcards, and participants' opinions were also annotated by table moderators and note takers. More information on the SurPRISE citizen summit methodology can be found in previous publications (Degli Esposti and Santiago-Gómez, 2015).

During each summit two out of three specific SOSTs were discussed. These SOSTs were: Smart CCTV, Deep Packet Inspection (DPI), and smartphone location tracking. Within this chapter we will rely on evidence related to the case of DPI. Qualitative data used in this chapter were gathered during the citizen summits held in England. In contrast, quantitative data here analysed come from six EU countries, which are Austria (sample size n = 220), Italy (n = 180), Norway (n = 113), Spain (n = 163), Switzerland (n = 204) and the UK (n = 244).

Deep Packet Inspection

Given the importance of digital communications, interactions and relations, this article focuses on lay people's opinions of a specific surveillance technology, which is Deep Packet Inspection (DPI). DPI is a type of data processing that looks in detail at the contents of the data being sent. On the Internet, any information sent or received is collected into *packets*, which have a label on them called a *header* that describes what these packets are, who sent them, and where they are going: just like a letter flowing through a postal network. DPI is a method of *packet* filtering which allows examining the content of a packet rather than simply read its header by deeply analysing packet contents, including information from all seven layers of the *Open Systems Interconnection* (OSI) model. As DPI makes it possible to find, identify, classify, reroute or block packets with specific data or code payloads, it has been compared to a postman opening one's letters and reading their contents (SurPRISE, 2014).

As many ICT technologies, DPI has several applications. Internet service providers (ISP) can use DPI to allocate available resources to streamline traffic flow, or to apply different charging policies, traffic shaping, or offer quality of service guarantees to selected users or applications (Antonello *et al.*, 2012). DPI has been used by major network operators in the U.S. and Canada to block or restrict the speed of peer-to-peer file sharing traffic by their customers (Mueller and Asghari, 2012). In enterprises, it is used to ensure network security, and to support quality of service and terms of

use, copyright enforcement, target marketing and behavioural advertising to online customers (Corwin, 2011). DPI represents a basic component of network security as it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in anti-virus solutions (Anderson, 2007).

DPI is also used in the fight against major crimes such as child pornography, transnational organized crime and terrorism (Person, 2010). However, DPI has been also used by Libyan and Syrian Governments to spy and capture rebels, and it is used by the Chinese Government as a censorship tool (Fuchs, 2013). The Snowden's revelations also demonstrated that DPI has been used by the NSA to spy on both citizens and public authorities of several countries around the world (Lyon, 2014). It is important to consider that, by the time the citizen summits took place, DPI had begun to receive remarkable media attention, due to the NSA scandal and Snowden's revelations. For this reason, most users were aware of the existence of this technology.

Summit participants' perceptions of Deep Packet Inspection

Citizen summit participants had the chance to learn about DPI before and during the events. They received a booklet before the event and watched a short documentary film on DPI during the event which helped them understand this specific technology. Most citizens in all the six countries where DPI was discussed were confident about their understanding of DPI functions and operations. Moreover, in all countries except the UK, more than half of the participants said to be fairly knowledgeable about the way DPI was used.
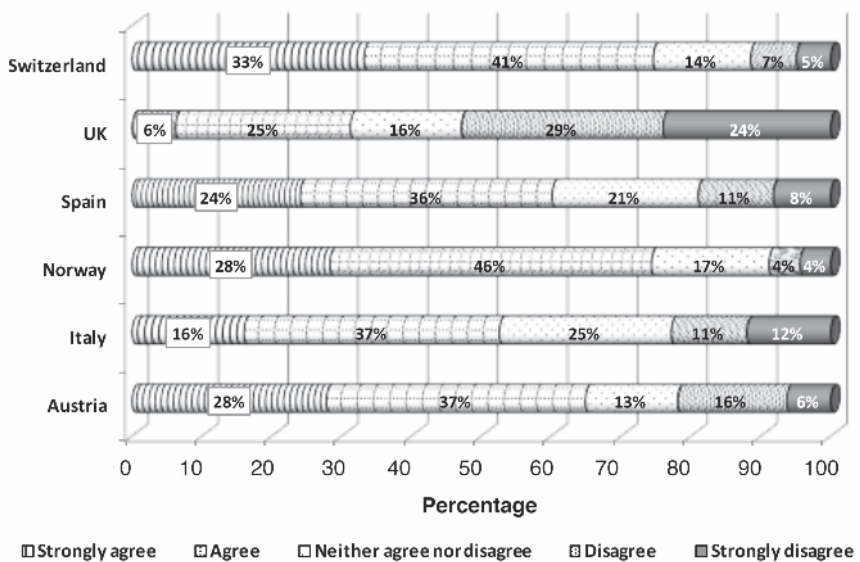
Figure 4.1 Agreement with the statement 'I understand what DPI is'

Although British participants had some doubts about the functioning of DPI, they were able, nonetheless, to engage with the topic and discuss its advantages and drawbacks. As reported in the following quote, extracted from one table discussion, DPI was considered to have useful security applications, though also to be problematic in terms of regulation and accountability.

> *F4*: Overall it was felt that DPI would be useful against cyberbullying, child pornography, terrorist attacks and other security related issues. However, it's hard to regulate who uses this information and for what purposes and international agreement on how to regulate this seems impossible.
>
> (Table moderator's reflections)

Nearly half of the participants in all countries considered DPI an effective national security tool, even though regulatory instruments were considered in general insufficient to tackle the problem of preventing inappropriate uses of DPI. As shown in Table 4.1, only 19 per cent of respondents agreed with the statement 'laws and regulations ensure that DPI is not misused'. As expressed in the following statement made by a citizen participant, the main problem is that Internet users rely on services offered by organizations subject to different laws and regulations from the ones enforced in the user' country.

> *AbB30-C5*: National security. I'm happy to have it but it needs more control. How do I get junk mail when I don't give people my details? I noticed a difference when I started using Yahoo mail. Because of today I know this is because of the lack of rules or different rules in America.

Nevertheless, laws, regulations and legal procedures are interpreted by the public as a possible solution to ensure the correct adoption of SOSTs. As reported in the following statements, legal guarantees contribute to set standards for the acceptable use of SOSTs.

> *AbB11-C5*: There should have to be a warrant to hack into my email, a criminal investigation reason for it.
> *AbB28-C5*: None but there should be regulations about it to protect us.

Despite the fact that DPI was considered useful in improving national security by almost half of the participants (48 per cent), two third of them said DPI was nevertheless highly intrusive (71 per cent). Figure 4.2 highlights the difference between the perceptions of British and Austrian participants on the matter. A higher proportion of British respondents considered DPI an effective security measure (UK: 58 per cent; Austria: 28 per cent), while a higher proportion of Austrian people considered DPI intrusive (Austria 56 per cent; UK: 16 per cent). For a more in-depth discussion on the effect of culture on privacy and security attitudes see Budak, Rajh and Recher within this volume.

By looking at the data collected during the citizen summits, we can see that DPI
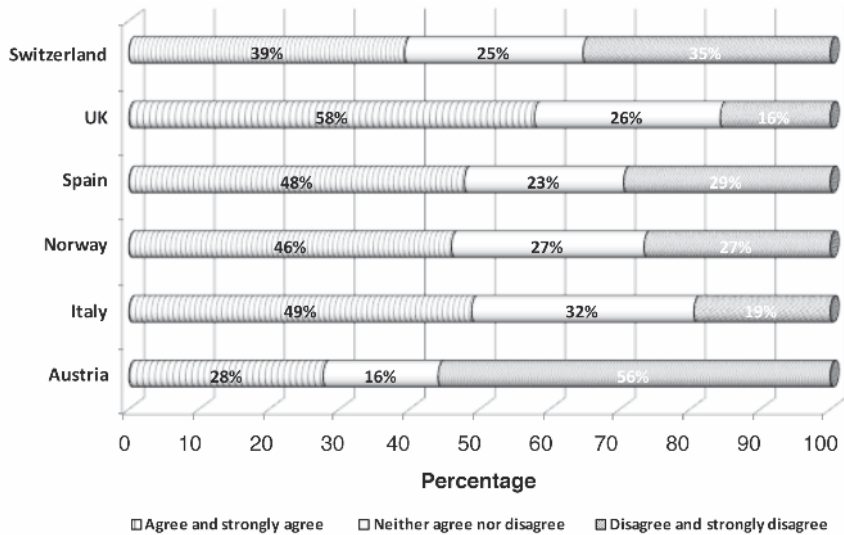
Figure 4.2 Agreement with the statement 'In my opinion, DPI is an effective national security tool'

Table 4.1 Level of agreement with each statement

	DPI		sCCTV		SLT	
	Freq.	*Per cent*	*Freq.*	*Per cent*	*Freq.*	*Per cent*
1. Laws and regulations ensure that DPI is not misused	195	19%	260	24%	278	28%
2. I believe that DPI improves national security	507	48%	645	59%	505	51%
3. I believe that DPI is intrusive	750	71%	553	51%	549	55%
4. I think that the level of intrusiveness is acceptable given the benefits DPI offers	372	35%	517	48%	483	49%
5. None of the above	22	2%	28	3%	25	2%
6. DK/NA	13	1%	12	1%	9	1%
Total number of respondents	1050		1087		994	

was perceived to be the most intrusive measure (71 per cent), more than smart CCTV (51 per cent) or smartphone location tracking (55 per cent). One of the reasons behind this difference in perceptions is that people feel to have no control over the way Internet is governed and managed. We quote the following conversation as an evidence of this assertion.

AbB34-C5: Of the two, DPI and Smart CCTV, I prefer the Smart CCTV. More control over that. Nearly everyone in this room uses the Internet and we have no control over it.

AbB35-C1: There will be terms and conditions on websites.

AbB36-C5: But nobody reads them and it's not enough. I think there should be a section for our own terms and conditions. No control.

At the time of balancing intrusiveness against effectiveness of DPI, only one-third of participants considered the level of intrusiveness of DPI acceptable (35 per cent). In contrast, nearly half of the participants said to consider the intrusiveness of smart CCTV (48 per cent), and smartphone location tracking (49 per cent), reasonable given the benefits these technologies offer. This variation may be explained by the fact that people tend to perceive the Internet as a private space, rather than as a public space. The fact that the activity is performed while people are at home, or at work, which are considered intimate spaces, wherein confidentiality is safeguarded, may generate some confusion and make people underestimate the risks of being online. The following reflection made by a note taker and the statement made by a study participant offer some insights into some lay people's perceptions on the matter.

RhBSum: Interestingly, they saw a big difference between the privacy concerns with smart CCTV and DPI. They felt that when you are outside the house, you must expect to be watched by others. However, inside the house and online, people feel as though their actions are private and personal.

(Note taker's reflections)

AbB9-C5: I was naïve to think until today that some of my information on the Internet was private and now I know I can be hacked. This conference has made me realise. I can be compromised financially. There is no control.

Digital communications are also expected to resemble analog communications; which are characterized by attributes such as mail correspondence confidentiality. Because of these expectations, participants tended to perceive DPI as a more deceptive, subtle and invasive measure than the other technologies analysed. Compared to smart CCTV systems, which are positioned in public places, DPI operates in what are considered private spaces during activities, such as surfing the net or sending emails, that are also perceived as private (Degli Esposti and Santiago-Gómez, 2015). As any automated digital system, DPI goes also virtually undetected by users when it is used to spy on people.

F4: [DPI] It's an unseen invasion of privacy, worse than CCTV because it is more personal (online banking, etc.) and open to fraud. There is very little public awareness. Worries were expressed about government covering up the use and purposes of DPI. Overall the pros do not outweigh the cons.

(Table moderator's reflections)

The lack of transparency on the use and purpose of DPI generated a feeling of frustration and resignation among participants, as pointed out in other studies (Turow *et al.*, 2015). While the use of CCTV systems is advertised in public spaces, no information about when, how, and by whom DPI is operated is made available while users are surfing the Web. Even smartphone location tracking was perceived more favourably. Thus, DPI raises more concerns and generates negative reactions even among British participants, who were on average the more willing to support the adoption of surveillance measures.

> 'I don't know what I will do. I'm paranoid even though I do nothing wrong'.
> 'It is out of our hands, there is nothing we can do'.
> 'The majority will just have to accept it if they want to use the Internet'.
> 'Up until now, I didn't realize they monitor our Internet'.
>   (Statements made by participants and reported by Note Taker no. R01)

These perceptions are exacerbated by the fact that everyone goes online (see Figure 4.3). The large majority of participants said they use the Internet 'all of the time' (minimum 39 per cent in Italy; maximum 70 per cent in the UK). In other terms, the Web is now a space of social and economic interaction which is constitutive of everyday life. It is increasingly difficult to try to live offline. This is an important consideration, because it implies that any problem produced by technologies that intrude our privacy and human rights in cyberspace can no longer be simply dismissed as something that can be solved by 'not going online'.
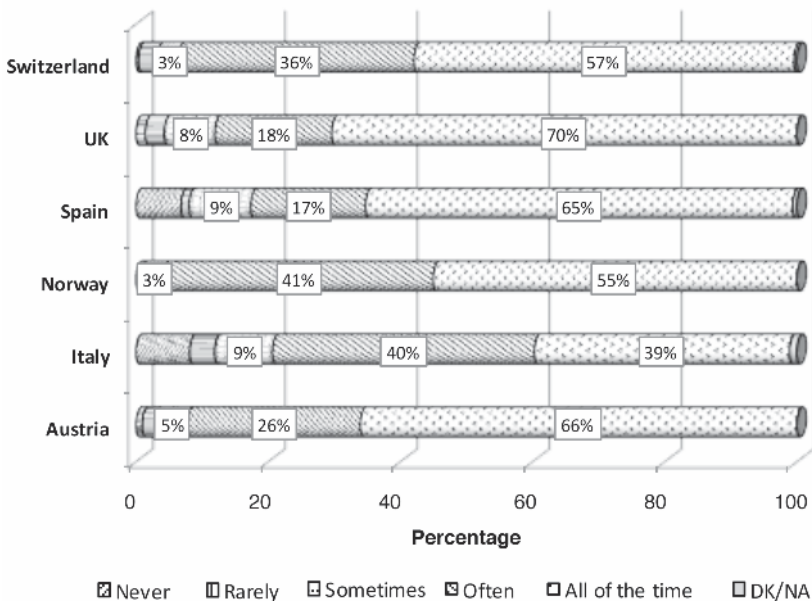
Figure 4.3 Distribution of answers to the question 'How often do you use the internet?'

Within this context, it is worth noticing that almost two-thirds of EU households have Internet access at home and that nowadays people are more likely to access the Internet through a combination of both home and mobile phone connections (EC, 2014); these considerations help us understand the extent to which Europeans are constantly exposed to the risk of Internet surveillance. As a result, the majority of participants in five countries out of six said to worry about Internet security, while most Hungarians were indecisive or not concerned (see Figure 4.4).

The rise in the number of activities performed on the Web makes it difficult for people to simply avoid the digital space as they would avoid going to a certain neighbourhood or to any other geographical space. Nonetheless only a small proportion of people (22 per cent) declared to be absolutely sure they were not willing to change their behaviour because of DPI, while a largest proportion of people said that, in principle, they would not change their online behaviour because of DPI (40 per cent). On the other hand, one-third of respondents were said to be willing to act in a different way when they were online (31 per cent), and some participants said they would even avoid going online (6 per cent). See results displayed in Figure 4.5.

Becoming aware of DPI and concerned about it, however, do not constitute *per se* sufficient conditions for people to actively oppose, or avoid, technologies such as DPI. As shown in Figure 4.6, obtaining more information on how to protect one's privacy is the top priority for the majority of participants (55 per cent). Only a small proportion of respondents would be willing to actively resist DPI (10 per cent), campaign against it (11 per cent), or support those who protest against its use
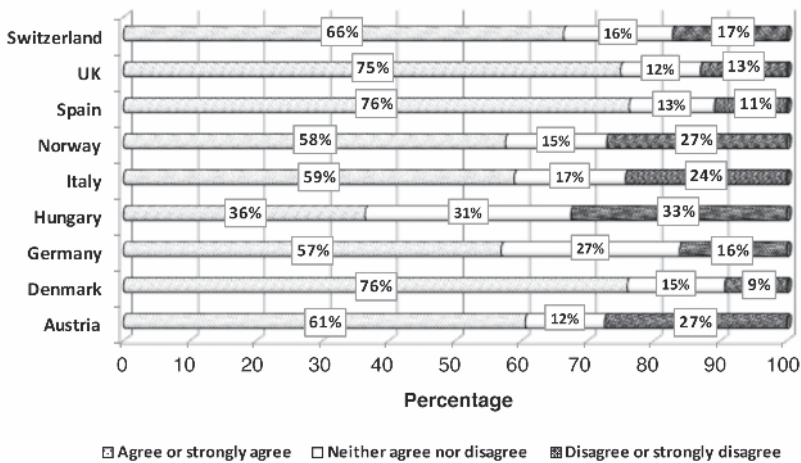
Figure 4.4 Level of agreement with the statement 'I worry about security when I am online'
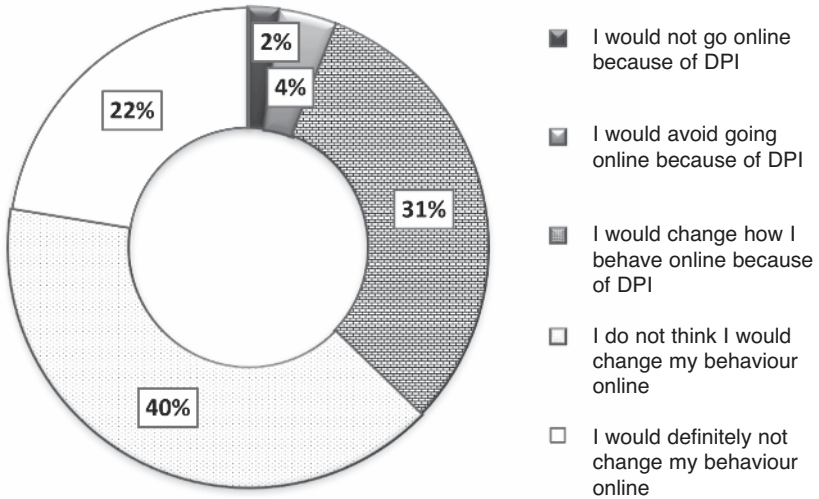
Figure 4.5 Active avoidance of DPI

(13 per cent). The most likely form of resistance would probably be enacted through individual actions on personal digital devices (Lyon, 2007).

When it comes to the topic of the adoption of DPI as a national security measure, as shown in Figure 4.7, the public is divided between those who are in favour (46 per cent), those who are against it (34 per cent), and those who are undecided (19 per cent).
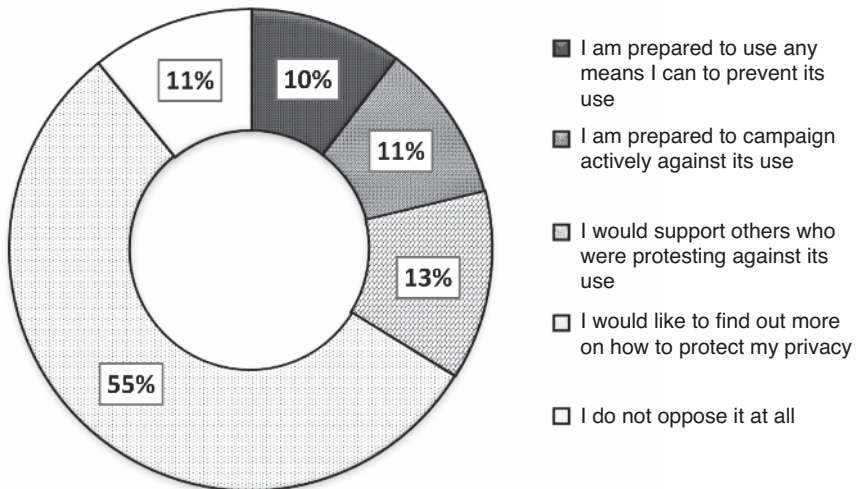
Figure 4.6 Challenging the use of DPI for security purposes
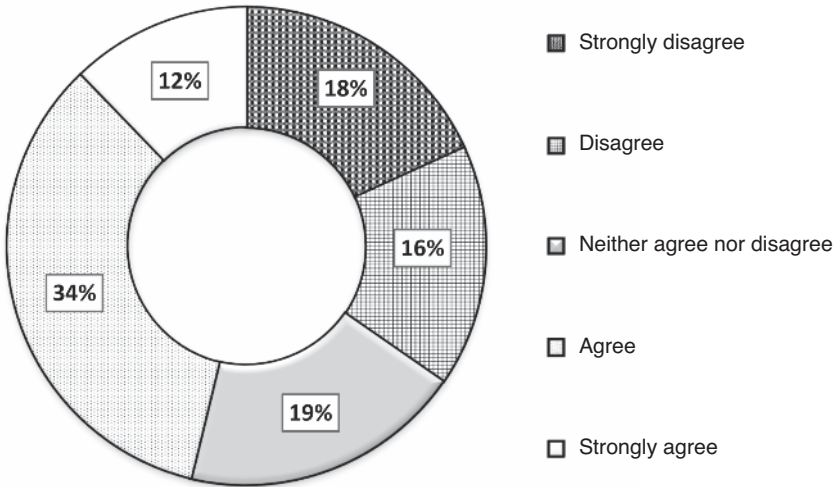
Figure 4.7 Agreement with the statement 'Overall I support the adoption of Deep Packet Inspection as a national security measure'

To conclude, DPI can be considered a very ambiguous technology: Internet users recognise its benefits in the security area, but they are also concerned about online surveillance. For this reason, as shown in Figure 4.5, they would like to know more about how to protect their privacy online and would welcome more effective regulation on the matter. Nonetheless they do not succumb to the chilling effect (Askin, 1972) and tend to refuse to change the way they behave online because of DPI. The lack of information, knowledge and transparency contribute to the emergence of an apparently static scenario, which is characterized by frustrated users who are concerned about their privacy and feel powerless and resigned. As a result, considering that most of the times citizens are monitored by SOSTs without having a chance to opt out, assessing SOSTs' acceptability in advance becomes absolutely necessary. In fact, more qualitative studies are necessary to study under which conditions, and for what purposes, the use of technologies like DPI can be considered acceptable by the citizens. As previously said, we could not investigate DPI acceptability in depth because of limitations in the qualitative data gathered, so in the next section we move to explore and discuss factors influencing public acceptance of DPI.

Factors influencing public acceptance of DPI

Within this section we analyse survey data gathered during the citizen summits. The aim is to investigate factors influencing public acceptance of DPI. We use the statement 'Overall I support the adoption of Deep Packet Inspection as a national

security measure' to measure the dependent variable. We have taken into consideration the following independent variables:

- DPI's perceived effectiveness (EFF);
- DPI's perceived intrusiveness (INT);
- Social proximity (SPRO);
- Privacy risks (RISK);
- Security operators' degree of trustworthiness (THR).

Each independent variable has been measured with one or more questionnaire item. Exact formulation of the questions is reported in Table 4.2.

We have used median regression (Koenker and Bassett, 1978) to test the effect of the independent variables on public acceptance of DPI. Most notably, the outcomes show how DPI's perceived effectiveness and system operators' trustworthiness play a relevant positive role in determining public acceptance. The fact that DPI is used only to investigate criminal activity also increases the chances of supporting the use of DPI. In contrast, the fact that DPI is perceived to intrude into a person's life, and that it entails risks due to errors, such as misinterpretation of one's behaviour, decreases the likelihood of supporting its adoption. In other words, the perceived effectiveness of DPI in contributing to the fight against terrorism and other major crimes, contributes positively to the acceptance of DPI. However, and for the same reason, the perceived intrusiveness of the technology produces concern and rejection. In between these two basic relations, there exist other variables that also influence acceptance in one way or another. For instance, the trustworthiness of public authorities using DPI contributes positively to the acceptance of DPI, and so does the perception that DPI is being used against specific crimes, like child pornography and terrorism, and against a specific human target, i.e. criminals and suspects (SPRO). Conversely, the perceived risk of abuse, or misuse, negatively influences the acceptance of DPI.

Table 4.2 Questions measuring perceived effectiveness, intrusiveness, social proximity, trustworthiness and various privacy risks

I.V.	Questionnaire item
EFF1	In my opinion, DPI is an effective national security tool
EFF2	When I am online, I feel more secure because DPI is used
EFF3	DPI is an appropriate way to address national security threats
INT1	The idea of DPI makes me feel uncomfortable
INT2	I feel DPI is forced upon me without my permission
SPRO	DPI does not bother me as long as it only targets criminals
RISK1	DPI worries me because it could reveal sensitive information about me
RISK2	DPI worries me because it could result in my behaviour being misinterpreted
RISK3	DPI worries me because it could reveal the content of my communications
RISK4	DPI worries me because it could violate my fundamental human rights
TRU1	Security agencies which use DPI are trustworthy

Table 4.3 Median regression

[D.V.] ACC1: 'Overall I support the adoption of Deep Packet Inspection as a national security measure'	*Coef.*	*Std. Err.*	*t*	*P>t*	*[95% Conf. Interval]*	
EFF1: 'In my opinion, DPI is an effective national security tool'	.465	.034	13.65	0.000	.398	.532
INT2: 'I feel DPI is forced upon me without my permission'	−.132	.042	−3.12	0.002	−.215	−.049
SPRO: 'DPI does not bother me as long as it only targets criminals'	.153	.029	5.26	0.000	.096	.210
RISK2: 'DPI worries me because it could result in my behaviour being misinterpreted'	−.083	.036	−2.32	0.021	−.154	−.013
TRU1: 'Security agencies which use DPI are trustworthy'	.305	.035	8.82	0.000	.237	.373
Constant	.597	.168	3.54	0.000	.266	.928

Notes: Number of observations = 864
       Pseudo R2 = 0.3574

Apart from studying the direct relationship between the independent variables and the dependent variable, we have also studied relationships among independent variables listed in Table 4.2, in order to explore whether they influence each other and in what ways. In doing this, we have used a non-parametric statistical technique called Kendall's rank correlation (Kendall, 1970), which provides a distribution free test of independence and a measure of the strength of dependence between two variables.

By looking at rank correlation coefficients, four major results emerge. First, and contrary to what one would expect, perceived intrusiveness and perceived effectiveness are negatively related. We had imagined that DPI would be considered effective precisely as a result of its intrusiveness. In contrast, people who perceive DPI as highly intrusive are less willing to consider the technology to be effective, probably because they do consider that DPI is more effective when it is used to tackle specific crimes, and not when it is implemented as part of a massive surveillance strategy. As a matter of fact, and this is the second confirmed result, if DPI were used just to monitor and investigate criminal activity, rather than being used to screen the communications of all online users, summit participants would be more inclined to consider DPI as an appropriate security measure. Third, it is precisely the privacy risks associated with DPI, such as misinterpretation of users' online behaviour, human right violation, and unauthorized disclosure of confidential communications that make people consider DPI as highly intrusive. Finally, the fact that security agents who manage DPI are considered to be trustworthy by citizens plays an important role not only vis-à-vis its acceptance, but also in relation to its perceived intrusiveness. Agents' trustworthiness contributes to both increase

Table 4.4 Kendall's rank correlation

	EFF1	EFF2	EFF3	INT1	INT2	SPRO	RISK1	RISK2	RISK3	RISK4	TRU1
EFF1	0.774										
EFF2	0.279★	0.725									
EFF3	0.445★	0.344★	0.776								
INT1	−0.279★	−0.300★	−0.291★	0.730							
INT2	−0.142★	−0.200★	−0.169★	0.269★	0.518						
SPRO	0.281★	0.244★	0.326★	−0.224★	−0.104★	0.782					
RISK1	−0.154★	−0.179★	−0.191★	0.258★	0.187★	−0.138★	0.642				
RISK2	−0.136★	−0.143★	−0.181★	0.208★	0.144★	−0.102★	0.245★	0.668			
RISK3	−0.157★	−0.191★	−0.192★	0.272★	0.193★	−0.131★	0.342★	0.264★	0.628		
RISK4	−0.180★	−0.194★	−0.226★	0.237★	0.187★	−0.126★	0.273★	0.287★	0.331★	0.631	
TRU1	0.233★	0.210★	0.257★	−0.221★	−0.148★	0.257★	−0.211★	−0.159★	−0.178★	−0.185★	0.765

Note: ★ Significance level 1%

the likelihood of accepting DPI and of reducing its perceived privacy risks and, thus, its perceived intrusiveness.

Discussion and conclusion

Surveillance-based security measures are conceived and designed to fight crime and reduce violence. Despite this legitimate purpose, these technologies bring new risk of human rights infringement, or potential negative consequences for citizens, which have to be taken into consideration at the time of assessing these solutions. Human rights risks and potential externalities can be reduced by means of organizational and procedural measures, and through the investigation of public perceptions and understanding of these measures.

Drawing from the quantitative data proceeding from 12 citizen summits, and from the qualitative data proceeding from the UK citizen summit, this study has explored the topic of public acceptance of Deep Packet Inspection (DPI). According to our results, study participants express deep concerns about the widespread use of DPI by security agencies, but, at the same time, acknowledge the potential contribution of DPI in the fight against major crimes. In general, DPI is considered a very intrusive technology, especially because it operates in what it is perceived to be a private space. The lack of transparency and information on the use of DPI on the Internet contribute to transform DPI in the least accepted technology among the SOSTs assessed during the Surprise citizen summits. Although the perceived trustworthiness of security operators, and the perceived effectiveness of DPI, contributes positively to increase its acceptance, the risk of abuse, or misuse, makes it a very controversial technology. This is an especially relevant issue, because DPI operates on the Web, where people perform most of their activities and communications nowadays. However, online users enjoy their freedom on the Web and are not willing to give up their rights to free expression and self-determination because of the potential chilling effect produced by technologies like DPI.

The more citizens become aware of the existence of online surveillance, the more likely they are to realize that they need to know much more about how to protect their privacy online. The complexity of the situation people face – on one side the need to be online, and on the other one, a certain feeling of frustration, or resignation, generated by the perceived lack of knowledge and control over digital technologies and personal data – is misleadingly described by the so-called 'privacy paradox'.

On the base of our analysis we argue that technology assessment, especially in the security area, needs to go beyond cost-benefit analysis and take into consideration the interplay between technological attributes, such as accuracy and effectiveness, and non-technological considerations related to system operators' level of competence and integrity. Technological systems, in fact, operate always within specific socio-cultural contexts and the characteristics of the context influence not only the way technology is operated and regulated, but also the way it is perceived and judged. This is why the societal knowledge offered and used by study participants should not be neglected: their concerns often reflect the reality

of specific socio-cultural contexts, wherein the technology is implemented and regulated. When assessing a technology social, economic, and institutional features are crucial to properly assess the impact and benefits of a given technology. For instance, in the view of the citizens participating in this study, DPI is intrusive as much as it is effective: to the contrary, the degree of intrusiveness of this technology is considered an indicator of its lack of effectiveness. A more focused, and therefore less intrusive, use of interception of Internet traffic would make citizens perceive the latter as more effective.

In many ways, these considerations suggest that the trade-off between privacy and security is, in fact, a false one. The right to the integrity of our communications, relations and information is a key element of human security, and citizens consider it as important as the right to physical integrity and protection from violence. This understanding of security, which involves both digital security and physical security, suggests that framing our right to the integrity of our communication, relations and personal information as 'privacy' in opposition to 'security' is effectively diverting attention from the fact that governments are giving priority to the protection of physical security at the expenses of other, equally fundamental, elements of human security. Moreover, the approach prevents public scrutiny and hides the fact that current approaches prioritize the territorial integrity of the State and the physical security of the citizen, at the expense of other conceptions of security.

Following this way of reasoning, more security (in terms of investments, technologies, etc.) can sometimes results in less security (in terms of perceived public security). For instance, the effectiveness of DPI is often assessed against more traditional security measures, such as the number of police officers infiltrated or police intelligence fieldwork, from a cost-benefit perspective. In this way, DPI is not being assessed on the basis of the impact it has on other aspects of human security, such as, the integrity of people's movements and relations or the risk of data leaks. The societal knowledge offered by the citizens participating in this study, can help question current approaches to security precisely along these lines. There is a clear need to develop new security approaches that do not rely on the trade-off, and, rather, approach security from a systemic perspective, i.e., a view that considers simultaneously the totality of security needs of the society and that approaches individual security from a more sophisticated and comprehensive human security perspective where all aspects of individual security are taken into account and where every security measure introduced is assessed against the overall security balance of the society (Pavone *et al.*, 2016).

Security measures, both technological and non-technological, need to foster public safety both in objective terms, by reducing crime, and in subjective terms, by helping people feeling secure and protected. With this chapter, we hope to contribute to this long awaited transition from the old privacy–security trade-off model, to the development of a new win-win security paradigm, where surveillance is minimized and where all aspects of human security, including those today presented as part of the privacy dimension, are intimately aligned.

Bibliography

Acquisti, A. (2010) Background Paper #3: The Economics of Personal Data and the Economics of Privacy. The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, December 1, 2010, 9:30–18:00 2010 OECD Conference Centre. OECD.

Anderson, R. (2007) 'Deep packet inspection technologies', in Tiptin, H.F. and Krause, M. (ed.) *Information Security Management Handbook,* 6th edn, Boca Raton, FL and New York: Auerbach Publications.

Antonello, R., Fernandes, S., Kamienski, C., Sadok, D., Kelner, J., Gódor, I., Szabó, G. and Westholm, T. (2012) 'Deep packet inspection tools and techniques in commodity plat- forms: Challenges and trends', *Journal of Network & Computer Applications,* 35: 1863–1878.

Askin, F. (1972) 'Surveillance: The Social Science Perspective', *Columbia Human Rights Law Review,* 4: 59–88.

Ball, K. (2002) 'Elements of surveillance: A new framework and future directions', *Information, Communication & Society,* 5: 573–590.

Ball, K. (2009) 'Exposure', *Information, Communication & Society,* 12: 639–657.

Bankston, K. S. and Soltani, A. (2014) 'Tiny constables and the cost of surveillance: Making cents out of *United States v. Jones', The Yale Law Journal Online,* 123: 335–357.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R. B. J. (2014) 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology,* 8: 121–144.

Bellanova, R. and González Fuster, G. (2013) 'Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices', *International Political Sociology,* 7: 188–209.

Clarke, R. (1988) 'Information technology and dataveillance', *Communications of the ACM,* 31: 498-512.

Corwin, E. H. (2011) 'Deep packet inspection: Shaping the Internet and the implications on privacy and security', *Information Security Journal: A Global Perspective,* 20: 311–316.

Degli Esposti, S. (2014) 'When big data meets dataveillance: The hidden side of analytics', *Surveillance & Society,* 12: 209–225. Available at: http://ojs.library.queensu.ca/index.php/ surveillance-and-society/article/view/analytics (accessed 21 December 2016).

Degli Esposti, S. and Santiago-Gómez, E. (2015) 'Acceptable surveillance-orientated secu- rity technologies: Insights from the SurPRISE Project', *Surveillance & Society,* 13: 437–454. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and- society/article/view/acceptable_technologies (accessed 21 December 2016).

European Commission (EC) (2012) 'Security Industrial Policy: Action Plan for an innova- tive and competitive Security Industry', COM (2012) 417 final, Brussels. Online. Available at: www.statewatch.org/news/2012/jul/eu-com-security-industry-com-417- 12.pdf (accessed 19 December 2016).

European Commission (EC) (2014) 'E-Communications and Telecom Single Market Household Survey', Special Eurobarometer 414, Brussels. Online. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_414_en.pdf (accessed 19 December 2016).

Fuchs, C. (2013) 'Societal and ideological impacts of Deep Packet Inspection surveillance', *Information, Communication & Society,* 16: 1328–1359.

Gandy, O. H. (1989) 'The surveillance society: Information technology and bureaucratic social control', *Journal of Communication,* 39: 61–76.

Hess, D. J. (2014) 'Publics as threats? Integrating science and technology studies and social movement studies', *Science as Culture,* 24: 69–82.

Hoofnagle, C. J. and Urban, J. M. (2014) 'Alan Westin's privacy homo economicus', *Wake Forest Law Review,* 49: 261–317.

Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J. and Ayenson, M. D. (2012) 'Behavioral Advertising: The offer you cannot refuse', *Harvard Law & Policy Review,* 6: 273–296.

Kendall, M. G. (1970) *Rank Correlation Methods,* London: Griffin.

Koenker, R. and Bassett, G. J. (1978) 'Regression quantiles', *Econometrica,* 46: 33–50.

Lyon, D. (2007) *Surveillance Studies: An Overview,* Cambridge: Polity Press.

Lyon, D. (2014) *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, Cambridge: Polity Press.

Marx, G. T. (2003) 'A tack in the shoe: Neutralizing and resisting the new surveillance', *Journal of Social Issues,* 59: 369–390.

Mueller, M. L. and Asghari, H. (2012) 'Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States', *Telecommunications Policy,* 36: 462–475.

Murakami Wood, D. (2009) 'The "surveillance society": Questions of history, place and culture', *European Journal of Criminology,* 6: 179–194.

Pavone, V. and Degli Esposti, S. (2012) 'Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security', *Public Understanding of Science,* 21: 556–572.

Pavone, V., Santiago Gómez, E. and Jaquet-Chifelle, D-O. (2016) 'A systemic approach to secu- rity: Beyond the trade-off between security and liberty', *Democracy and Security,* 12: 225–246.

Person, A. N. (2010) 'Behavioral advertisement regulation: How the negative perception of deep packet inspection technology may be limiting the online experience', *Federal Communications Law Journal,* 62: 435–464.

Shklovski, I., Mainwaring, S. D., Skladttir, H. H. and Borgthorsson, H. (2014) 'Leakiness and creepiness in app space: Perceptions of privacy and mobile app use', in *Proceedings of the 32nd annual ACM conference on Human factors in Computing Systems, Toronto, Canada*, New York: ACM Press.

Siegrist, M. (2008) 'Factors influencing public acceptance of innovative food technologies and products', *Trends in Food Science & Technology,* 19: 603–608.

Smith, H. J., Dinev, T. and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS Quarterly,* 35: 980–1015.

SurPRISE (2014) SurPRISE Documentary Film: DPI (Deep Packet Inspection).

Turow, J., Hennessy, M. and Draper, N. (2015) *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*, Philadelphia, PA: The Annenberg School for Communication, University of Pennsylvania.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view', *MIS quarterly*, 27: 425–478.

Verble, J. (2014) 'The NSA and Edward Snowden: surveillance in the 21st century', *SIGCAS Computers & Society,* 44: 14–20.

Wells, H. and Wills, D. (2009) 'Individualism and identity: Resistance to speed cameras in the UK', *Surveillance & Society,* 6: 259–274. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3284/0 (accessed 21 December 2016).

Xu, H., Luo, X., Carroll, J. M. and Rosson, M. B. (2011) 'The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing', *Decision Support Systems,* 51: 42–52.

5   Beyond the trade-off between privacy and security?

Organizational routines and individual strategies at the security check[1]

Francesca Menichelli

Introduction

In his Collège de France lectures of the late 1970s, Foucault (2010) identifies the control over mobility as one of the crucial problems of government. Essentially, as the target of government shifted from the individual to the population, a new political rationality emerged, that identified the management of this aggregate as a problem. This allowed for two imperatives – increased prosperity of the state and the maintenance of peace and internal order – to be mutually satisfied. However, while the growing economic interdependency has globally pushed towards greater facilitation of both trade and travel – as witnessed in the opening of borders through agreements such as Schengen in Europe and NAFTA (North American Free Trade Agreement) in North America – a contrasting appeal to security, calling for the tightening of security measures, has increasingly emerged.

Airports embody this tension and offer a tangible representation of the juxta-position between stringent security for some and enhanced mobility for others. In this regard, the politics of airport security can be seen as concerned with a very specific question that pertains to the location of the balance between the two poles of security and mobility. This brings two important, yet directly linked, points to the fore: first, the governance of security in the airport is a problem of contextual balancing; second, security is a notion that is locally negotiated between the actors interacting on site. With an initial consideration of these points it becomes possible to investigate the conduct of specific actors; more specifically, this chapter focuses exclusively on how passengers experience security checks at the airport, in which terms they understand their participation to the screening process and whether they think that such procedures are actually to do with security or not. The relevance of this work is twofold. On one hand, due to restrictions to access, airports are infrequently chosen to conduct field-work, so the present chapter contributes to overcome the lack of in-depth empirical studies on the making of security in airports. On the other, it also touches upon a series of important, and timely, issues – mobility, security, surveil-lance, technology – with relevant policy implications and a direct impact on people's lives.

The chapter will first detail the themes that emerged in the course of the interviews with passengers, using quotations to show how a tension exists in how passengers understand security checks. While interviewees agreed that security checks are necessary, reservations were raised on a number of issues, particularly in terms of the accuracy of security controls and the unbalanced nature of the inter-action between screeners and passengers. It will then critically examine these findings, to try to understand how security procedures have become normalized over time, yet are problematized on two different levels; individually, in terms of the discomfort and anxiety they raise in passengers, collectively, because of their opacity and perceived arbitrariness. Finally, the chapter will end by understanding these results in light of the security/mobility nexus that currently defines politics of screening at the airport.

To be mobile or to be secure?

During the inquiries into political power that he embarked upon from the late 1970s, Foucault (2009, 2010) introduced the concept of governmentality as the new art of governing that moves away from 'principles (…) derived from the traditional virtues (wisdom, justice, liberality, respect for divine laws and human customs) or from common skills (prudence, reflected decisions, care in surrounding oneself with the best advisers)' (Foucault 2010: 472) and is instead concerned with the management of the population. Knowing that negative factors cannot be eradicated, but only limited and contained, the essential mechanism at play here is maximizing 'the positive elements for which one provides the best possible circulation, and (…) minimizing what is risky and inconvenient' (Foucault 2010: 34). The need to ensure free mobility is clearly central, and it is in this regard that we can identify one of the core problems of government in the control and management of flows, trajectories and movement, both of goods and people.

The development of the concept of governmentality can be read as a genealogy of European nation-states as viewed through a lens that focuses on governing practices (Valverde 2007) rather than on conventional historical accounts. In this vein, we can also consider with Torpey (2000: 3) that the regulation of movement was an intrinsic part of the process of state formation, so much so that the establishment of a successful state monopoly on the legitimate means of movement can be seen as 'an essential aspect of the "state-ness" of state'. Torpey's study of the history of the passport traces how, in the course of time, states have been using documents to identify people and, consequently, to control their movements. Passports are here seen as part of a 'regime of identification' that relies on an 'extensive administrative infrastructure' (Torpey 2000: 7) comprising techniques and bureaucracies deployed in order to identify people and, crucially, to distinguish between nationals and foreigners. The development of passport controls is, thus, explicitly linked to the institutionalization of the idea of the nation-state as a homogeneous unit, and, in marking the shift from private to public control on movement, identifies one of the 'essential aspect[s] of the transition from feudalism to capitalism' (Torpey 2000: 8).

It can be argued that Torpey's work integrates and completes Foucauldian

accounts of governmentality in that it provides a detailed discussion of how specific techniques of identification 'have played a crucial role in the development of modern, territorial states resting on distinctions between citizens/nationals and aliens' (Torpey 2000: 5). What these accounts have in common is a shared understanding of the centrality of the issue of mobility for liberal regimes, so much so that it can be argued that under liberal governmentality freedom is effectively reframed as (speed of) movement (Bigo 2011: 31).

Economically, this is reflected in the creation of free trade areas and the increasingly interdependent nature of a global system of production and consumption for which the free circulation of goods, services, capital and, to an extent, labour is central. Juridically, while borders have not disappeared, they have become, at least in certain areas of the world, open, as testified by the abolition of national borders between Schengen states. Within this general framework, the facts of September 2001 have proven to be a powerful catalyst for a competing discourse of closure, enhanced security measures and control, which has challenged the very idea of unrestrained movement (see Lyon, 2003a). However, these developments must be understood as the outcome of longer-term political strategies and decisions whose beginnings can be traced back to the post-war period.

In international relations, authors such as Buzan pointed well in advance of 9/11 to the possibility of societal and identity issues coming to be understood as security threats – with the collapse of communism possibly paving the way to 'the pushing of Islam to the front rank of the opposition to Western hegemony' (Buzan 1991: 441). In much the same way, the work carried out within surveillance studies has convincingly shown how many of the changes brought about by 9/11 in the large-scale deployment of surveillance techniques and measures had been in the making for a long time, with the attacks accelerating their roll-out and facilitating their acceptance (Ball, Haggerty and Lyon 2012). Security measures in airports are a case in point. 'The data mining technologies had been available for some time in commercial settings, but until 9/11 no plausible reason existed for deploying them – and the customer data they analyse – within a national security apparatus. The drive toward large scale, integrated systems for identifying and checking persons in places such as airports and at borders, urged for years by technology companies, received its rationale as the twin towers tumbled' (Lyon 2003a: 5).

While in the immediate aftermath of the attacks it seemed as if borders would be hermetically sealed and travel would be slowed indefinitely, what has in the end been established is a system in which stringent security for some coexists with enhanced mobility for others. Despite the obvious difficulties in terms of access and the sensitivity of airport studies in an age of generalized anxiety (see Salter 2008: xvii), this is one of the reasons that make the airport a site well worth investigating, as it offers a clearly defined site where the forces and the competing interests active in the field of security and surveillance are openly represented. Its study can therefore give us meaningful hints as to how to address the juxtaposition between mobility and security in wider contexts as it can be argued that 'airports may mark the future of what is to come within public spaces' (Adey 2004: 1375).

On a more theoretical level, the system of airport security can at the same time be seen as part and parcel of wider transformations in the field of governance, particularly in relation to the institutionalization of emergency as the normal paradigm of government (Agamben 2005). As much as we are led to believe that the tightened levels of security in place within airports are an exceptional answer to an equally out-of-the-ordinary threat, which find their justification in what has been termed a 'logic of exceptionality' (Salter 2007), we are now nevertheless experiencing a bureaucratization of such logic (Larsen and Piché 2009) and its spreading into the wider society. Only rarely does this have anything to do with security, as several authors have rightfully pointed out (among others, see: Bajc 2005; Schneier 2003, 2008; Webb 2007). It is in light of these developments that we can frame David Lyon's argument for identifying the tension between security and mobility as the crucial dilemma faced by contemporary governments (Lyon 2007: 122).

Conceptually, this chapter considers security as the outcome of the interaction between the various public and private actors that are at work in the airport and, as such, a contested and locally negotiated notion; in turn, this allows us to consider the governance of security in the airport as a problem of balancing, and to analyse it accordingly. To this end, two choices have been made: the analysis is empirically based and focuses exclusively on passengers' experiences of undergoing security screening. The decision to concentrate all attention on the procedures for passenger screening was borne out of the observation that 'free movement [of people] cannot be managed in the same way as goods and services' (Bigo 1998: 150) and that, potentially, this practice has the strongest impact on the life-chances of people (Lyon 2003b).

Context, methods and scope of the research

This chapter is part of a larger project which sought to investigate how people experience security checks, how they understand their participation to the screening process and how they relate to screeners. In turn, this helped to shed light on the notions of security and privacy that people practically develop while they are at the airport and, crucially, on the thresholds of acceptability that they use to draw the line for their involvement in security control. Air travel was chosen because it is a very well-defined domain in which security and privacy play very important roles, both in terms of discourses and narratives, of practices and attitudes, and one with which an increasing number of people are familiar. Methodologically, the project relied on open-ended interviews with passengers and screeners, on-site observations, along with an analysis of current legislation and other relevant documents.

As for the context of the study, Brussels airport[2] is the largest airport in Belgium, with around 230,000 registered movements in 2014. Owing to the presence in the city of European and international institutions and all the organizations that revolve around them, there are very specific traffic patterns that had to be taken into account both in the design and the development of the fieldwork. Eighty-five per cent of the flights are to other European countries, and the vast majority of the 22 million passengers going through the airport are from Europe (78.2 per cent vs

21.8 per cent), with almost 17 per cent of the total amount using Brussels as a hub airport. Sixty-seven point eight per cent of commercial flights have Schengen destinations (Brussels Airport Company 2014). Most of the inbound passenger traffic is concentrated between Sunday evening and Monday morning, when bureaucrats come back to work, while outbound traffic reaches its peak between Thursday evening and Friday, when the same people commute home.

While the qualitative nature of the research made it possible to sideline traditional concerns on sampling and statistical representativity, the specificities of the context impacted on the choice of interviewees. In order to come to as close as possible to an understanding of passengers' experiences when flying in and out of Brussels airport, it was decided to interview people with European passports who use the airport frequently – at least once a month, but typically more. This was done to reflect the passenger data available for Brussels airport. The first respondents were selected because they fell within the relevant demographic – frequent flights all across Europe, mainly for business. Subsequent selection was carried out via snowball sampling.

The small number of interviewees is due to the exploratory nature of the research. This was part of a wider project (PRISMS – Privacy and Security Mirrors) which sought to challenge the traditional trade-off model between privacy and security in favour of an evidence-based perspective that would better reconcile privacy and security, trust and concern. The interviews themselves – along with the observations carried out on site – were conducted with the goal of contextualizing the results of the quantitative survey conducted across EU member states for the same project (see Friedewald *et al.* 2015); taken together, findings from the survey and the qualitative research were then integrated into the development of the decision support system, the final product of PRISMS. Despite the limitations of the study, the data collected in the course of fieldwork tell an interesting story independently of how they were used in the wider project, in that they contribute to shed light on how passengers make sense of security practices, while filling the gap between scientific considerations on the political, legal and ethical issues raised by security practices on one hand (among others, see: Zedner 2008), and journalistic accounts of the idiosyncrasies of an opaque, complex and at time baffling system (among others, see Harrington 2014).

In terms of questions, rather than entering the field with a questionnaire, a broad list of issues of relevance was compiled and was used to guide the interview through a combination of directive and non-directive questions (Hammersley and Atkinson 1983). The dimensions explored in the interviews had to do with perceptions of security, travel patterns and behaviours, and the impact of security measures on those. Eventually, 12 semi-structured, open-ended interviews were conducted, seven with female respondents and five with male respondents, ranging in length from 10 to 20 minutes, with people from Belgium, Italy, Romania, Sweden and the United Kingdom. All were conducted in English, recorded and transcribed.[3] For readers' clarity, excerpts from interviews will be in indented throughout the text.

Does security work?

Looking at the transcriptions, a clear narrative emerges from the interview. On a general level, interviewees are in unison arguing that, despite the time and frustration involved, security measures, in one kind or another, are necessary when flying. It is useful to frame the normalization of exceptional measures of control, and their resulting acceptance, as a successful example of securitization. There are two steps to this process. First of all, an issue must be presented as posing an existential threat to the very functioning of society, and therefore requiring the implementation of special emergency measures to deal with it. However, a 'discourse that takes the form of presenting something as an existential threat to a referent object does not by itself create securitization (…), but the issue is securitized only if and when the audience accepts it as such' (Buzan, Waever and de Wilde 1998: 25). Under this light, the support enjoyed by security measures in airports indicates a successful process of securitization, with all interviewees agreeing that, nowadays, airport security is a necessary response to attacks carried out against civil aviation. However, this acceptance is very limited, and contingent upon the efficiency and, crucially, consistency of a given security measure. An experience that resonates among the interviewees is the puzzlement felt when something goes through security once, but gets taken away the next time one is boarding a flight.

Thinking about security control in terms of necessity implies considerations about its efficiency. If the process itself cannot be avoided, then at least it should be made as easy and hassle-free as possible to go through it. Not wasting time is, to some interviewees, the number one concern they have when they have to catch a flight. Under this light, technology comes to play a relevant role, as it is seen as something that can eliminate the need for human screeners, thus making the entire process faster and, at the same time, less prone to errors.

> If the right technology was available, it would be great. Just putting your hand luggage on the belt, without having to take out laptops and liquids and then again, having the right technology, not having to take out all of your items, such as watches and belts and so on and just go through it. A screening that even if more thorough would allow me not to have to go through the process of having to take all items out of my pockets.
>
> (Interviewee 3)

In spite of the acceptance of security control, the concurrent theme of 'efficacy' emerged from the interviews, with interviewees expressing uncertainty as to whether, in their current state, regulations actually guarantee and increase security. Doubts revolve around two main questions. On the one hand, it is not clear why some items cannot be carried on board, with the regulation on the transportation of liquids in one's hand luggage uniformly mentioned as particularly bothersome.

> [Security at Brussels airport is] Poor. Maybe it's my impression with security in general. It's that I find it (…) it's being done because it has to be done. It

doesn't make me feel more secure, let's put it this way. Because I don't see that there is consistency, either within the airport or between European airports, to take a measurable comparison. I have been able to go through with a bottle of water in an airport and not in another.

(Interviewee 4)

On the other hand, those interviewees who experienced first-hand inaccuracies in how security checks are carried out openly question whether security delivers.

They once took a nail file from me and I don't care. The weird thing is, I had been on five flights with that same file and they took it right before I got on the last plane, which (…) I didn't care. I can get another file. (…) What bothers me is that apparently it could be a threat and they never took it, so that means that they are not always as strict as they should be, or maybe on the other hand there was this one guy that was too serious about it. That made me feel less secure, knowing that the rules can be applied in different ways. (…) It gave me the impression that rules can be random sometimes, and that would simply surprise me and that makes me think that other rules are maybe too much, like the water for example.

(Interviewee 2)

The implication that arises from this is the need for more information, in the double meaning of providing people clear details about what they can and cannot take on board with them, and as key to increased participation of passengers in the making of security. The lack of clear information on objects allowed as part of one's carry-on luggage means that it is hard for the passenger to know what the expected behaviour at the lane is, which in turn makes it harder to prepare beforehand and the whole process more time consuming. At the same time, not knowing exactly why specific rules are in place and what their actual effect on security levels is, is seen as negatively affecting the willing participation of passengers to the checks, particularly when it comes to the much despised regulation on liquids.

I think if people felt that their contribution to security makes people feel safer, they would be much more helpful. Lots of people are getting annoyed by, for example, having to put everything in a transparent bag and not taking water… If they don't feel that that actually contributes to security. (…) If people could see [statistics], then they would realize that this actually makes sense, to take off your shoes, not to take water. Because now, once in a while, you hear a rumour, like that they are going to lift the ban on liquids, so where does this come from? Is it based on measurables or is it because they feel it is costing too much money? This kind of things.

(Interviewee 4)

Does security make sense?

This last passage opens the door to a further series of considerations centred on the idea of the proportionality of security measures to the threat being addressed and the risk posed by specific situations and items. Some of the interviewees saw this as a way of questioning whether the effort, time and money spent on security are justified, while others emphasized the negative implications in terms of unpleasantness, intimidation, suspicion and discrimination.

> I still wonder if [security practices] are necessary or not. I understand that some security is needed, but are we still in danger, or something might happen? Because I don't think that shoes can be a danger, or water can be a danger.
>
> (Interviewee 10)

The interviews take this line of reasoning in two different directions. On the one hand, the illusory nature of total security is explicitly argued, because no matter how stringent measures can get, something or someone is always going to slip through. At the same time, though, the potential for reassurance of security control is also acknowledged, particularly for those who might find flying scary and stressful. Under this light, acceptance is more easily given, though this is coupled with persistent doubts as to the actual efficacy of security procedures.

> I know it has to be done to avoid possible problems, but also to show people that you are doing something. Because people get very scared of travelling and this kind of thing seem to happen more on planes. So this is also a way of calming down your travellers. So I can accept that it's a system to provide more security and I don't mind going through it.
>
> (Interviewee 9)

> – [The rationale of security measures] Maybe to give passengers a safe feeling, too. Because it might have that effect. Since the thing with the [nail] file, I have decided that people can still slip through with anything that can kill someone. You can kill someone in various ways. It might give you a false sense of security.
> – Is that a bad thing?
> – Of course not. A feeling of security is positive, unless it's crazily overstated.
>
> (Interviewee 2)

These quotations all point to what Schneier calls security theatre, that is 'security primarily designed to make you *feel* more secure' (Schneier 2008: 174. Emphasis in original). This idea stems from the understanding that while security is 'both a reality and a feeling' (Schneier 2008: 174), it can be hard for people to estimate correctly what the actual chances are of something happening, therefore opening

the door to the possibility of feeling less secure than it is actually the case. This is something that has been long acknowledged in psychology (see: Slovic 1987) and that can have serious and long-lasting consequences on people's behaviour; after 9/11, it took three years for global passenger traffic to go back to 2000 levels (IATA 2011). As is clear from the excerpts above, security theatre is not necessarily a bad thing, particularly when actual risk and perceived risk diverge dramatically. Given the low probability of terrorist attacks, security measures in airports can arguably be described as a form of security theatre; however, this does not come without risks of its own.

The unbalanced nature of the relationship between screeners and passengers, and how this power differential might impact on people's behaviour during security control was an area the research wanted to explore more in depth. In order to address this issue, interviewees were asked whether they had ever witnessed a confrontation taking place between a screener and passenger, whether they had ever had one, and finally, if they would feel comfortable in speaking up to security personnel, should they feel they were somehow being mistreated. While interviewees were split in half as to whether they would feel comfortable in speaking up to a screener, none recalled being either a witness to an argument and only one said she had complained during security control, which means that, even for those who answer back, this has so far largely remained a hypothetical scenario.

> – I would speak up, but there are some consequences. If you are running late for your flight, I don't think it's a good idea because it can steal time to your connection, or whatever. I have spoken up several times, mostly about attitude and about tone and about the clarity of the information.
> – And what happened to you?
> – Not much. As I said, they keep talking to you; they maybe ask you to go aside, explain, and then you might lose your place in the queue, or they might check you more carefully. Open your luggage fully.
>
> (Interviewee 6)

On the opposite side, others were not as certain they would speak up, mentioning the intimidating nature of the screening process and explicitly saying they would be afraid such behaviour might result in further problems, delays and, ultimately, missing one's flight. Additionally, some of the interviewees explicitly talked about the discomfort and intimidation experienced when going through security.

> It's like they assume that you might be a danger and that's what annoys me. They don't start with the assumption that you are innocent, at least that's the feeling I have. And that's where I feel that it's going too deep.
>
> (Interviewee 4)

> They are very intimidating. I feel like security in airports is a very serious something. (…) I am not sure if I would speak up to them. Right now, I'll say 'yes, I would', but on the spot I am not so sure that I would. (…) I'm not afraid

of the consequences. I think, I am sure, that there is some sort of law that protects me at that point. But maybe in the exact situation I would not be as self-assured because the situation is intimidating to me as a passenger.

(Interviewee 2)

Conclusions

It is clear from the interviews that, after more than a decade of visible and more and more stringent controls, security has finally come to be seen by passengers as a normal, unavoidable yet cumbersome, part of travelling. Not only is this true for the entire system of security at the airport, but for specific measures as well. The body scanner – currently not adopted by security at Brussels airport – is in this regard a case in point. While there was agreement among the interviewees that it is too intrusive, it is highly possible that its implementation on a large scale could win people's reservations, particularly if framed within a discourse stressing the advantages to be had in terms of both increased security and time saved.

However, we should not conflate, nor mistake, resignation with acceptance. As much as the necessity of security controls was acknowledged by the majority of respondents, their overall attitude could be best described in terms of a very qualified, contextual and contingent – in a word, limited – tolerance. Two dimensions proved to be particularly problematic. As far as the interaction with screeners at the barriers is concerned, interviewees explicitly talked about the discomfort, stress and anxiety they experience when passing through security, and the feeling of being considered guilty, rather than innocent, until proven otherwise. The discretion held by the screeners and the potential for discrimination this opens the door to also emerged as a concern, and in this regard it is significant that some of the interviewees sarcastically pointed to physical traits of theirs – for example, blond hair or fair skin – as a sign of trustworthiness. However, this is likely to be a luxury only available to the 'right' – i.e. Caucasian – kind of passengers, with those of a different ethnicity being denied even the possibility of defensively using irony as a distancing strategy. Both academic and popular literature have devoted a great deal of attention to the risks of airport profiling (for the former, see Chandrasekhar 2003, and Harcourt 2006. For the latter, see Syed 2010, and Khan 2013) and, while no such system is formally in place at Brussels airport, the risk of disproportionately targeting minority persons on the part of security systems is well known, and not limited to airports. This is particularly troubling from a political and ethical point of view, and even more so at a time when much attention is focused on the threat of radicalization, and on the role security agencies might play in fostering this response in high-risk individuals.

On a more general level, the opacity and arbitrariness of the system as a whole was also explicitly criticized, and more vehemently than any issue that might arise out of what happens during the screening. Because terrorist attacks against civil aviation are, luckily, few and far between, it is hard for passengers to reconcile the efforts towards security with a threat that is perceived as remote and unlikely, while the inconvenience that controls do bring about – in terms of time wasted, by

throwing away bottles of water in hand luggage – is very much present in the here and now of anyone who passes through them. As some of the interviewees concisely argued, if more information was to be made available on actual threats and the precise rationale for specific measures, this would probably increase people's willingness to participate in security control. However, the key point of the whole system is secrecy, as it is assumed that making information freely available would give the potential terrorist an edge. This results in the paradoxical character of airport security, with screeners complaining that they have to deal with uninformed passengers (Christiaens, Menichelli and Gutwirth 2015), while passengers complain that they are not given adequate information on the why, the how and the how long of specific security measures.

In light of these findings, some basic policy recommendations can be offered, regarding the provision to passengers of clear information about security measures, particularly the most contested ones, and offer clear and viable alternatives to those people who – for various reasons – might want to opt out of them. Additionally, it is important that efforts are made in order to downplay the potential for discomfort and intimidation, particularly when screeners deal with passengers from minority backgrounds. In addition to their relevance in terms of policy, these suggestions are also helpful in moving the discussion beyond the confines of the fieldwork that was detailed in previous pages, so as to frame the findings that emerged in light of the security/mobility nexus that currently characterizes the politics of screening at the airport.

The politics of screening at the airport are the result of two concurrent balancing acts. On a macro level, the capitalist push for global mobility comes head to head with the imperatives of national security; on a micro level, in every airport a variety of public and private actors come together in order to guarantee both safety and security of people and goods. At each of these levels, tensions invariably come up, so that what security comes to mean at any given moment, in any given place is the contingent outcome of negotiations between relevant stakeholders, and a matter to be analysed through empirical exploration. Despite their importance though, the voices of passengers and the terms in which they understand their participation to security are rarely presented. This chapter offers a first glimpse into these dimensions. On a theoretical level, the chapter thus contributes to an exploration of the meanings attached to the notion of security and of what it does, for whom, how and why. In doing so, it combines the understanding of security as a linguistic act with an attention to the day-to-day routines and everyday practices involved in its production and enforcement.

The two notions of security theatre (Schneier 2003 and 2008) and security meta-rituals (Bajc 2007) can also be profitably employed to characterize the provision and reception of airport security. What Schneier and Bajc both point to is the ritualistic and dramaturgical dimension of security. At times and circumstances of heightened uncertainty, with authorities expected to do something to protect citizens, security measures can provide reassurance and project a sense of order. However, along with their symbolic relevance, these measures can also have troubling and far-reaching implications in terms of privacy and discrimination. This

makes it all the more necessary to make the balancing act between security and freedom of movement as open, fair and transparent as possible.

The tension between the two poles of security and mobility is vividly experienced by the respondents, who, in the course of their interviews, would often detail the individual strategies they have developed in order to pass through security as quickly as possible, so as not to waste any time. Despite all precautions, though, problems can sometimes arise and it is in these moments of rupture that the individual more explicitly questions how controls are carried out. The respondents find it hard to reconcile everyday objects – with bottles of water being a case in point – with the threat these supposedly represent for air travel and because the entire system is built on a complete lack of transparent communication, it ends up being easily perceived as arbitrary and rigid. A possible solution to this predicament might be the opening up of a frank debate on the rules governing the system of airport security. In addition to increasing passengers' participation, on a more general level this would also pave the way for a much-needed discussion on the nature and meaning of security, on the political and ethical implications raised by the tools and strategies that we use to guarantee it, and its relationship with privacy.

As PRISMS has demonstrated, things are more complex than the trade-off model would have us believe, and it is no longer possible to ignore questions of cultural, social and geographical variation when we talk about security and privacy. In order to fully consider these dimensions, the in-depth investigation of specific sites proves vital, as it allows us to better understand how security practices and the responses to them are shaped. Under this light, the vivid and nuanced description of how passengers experience security checks that this chapter has presented provides a complementary view to the EU-wide survey that was carried out as part of the overall project, in the process bringing together different research methods to investigate how security is produced, contested, negotiated and understood by different people in different contexts. This is where qualitative research can offer a meaningful contribution to the study of security, privacy and their impact on people's lives.

Acknowledgements

Notes

1   The fieldwork on which this chapter is based was carried out within the remit of PRISMS while the author was a researcher at LSTS (Law Science Technology and Society research group), in the Law Faculty of Vrije Universiteit Brussel.
2   Fieldwork was conducted in Brussels in the spring and summer of 2014. The final draft of this chapter was submitted at the end of February 2016, just a few weeks before the attacks at the same airport and in the centre of the city on 22 March 2016.
3   Only one of the interviewees was a native speaker of English, while for everyone else English was a second language. The passages quoted throughout the text are not translations, but transcriptions of actual exchanges.

References

Adey, P. (2004) 'Surveillance at the airport: surveilling mobility/mobilising surveillance', *Environment and Planning A*, 36(8): 1365–1380.

Agamben, G. (2005) *State of Exception*, Chicago, IL: University of Chicago Press.

Bajc, V. (2007) 'Surveillance in public rituals: security meta-ritual and the 2005 U.S. presidential inauguration', *American Behavioral Scientist*, 50(12):1648–1673.

Ball, K., Haggerty, K. and Lyon, D. (eds) (2012) *Routledge Handbook of Surveillance Studies*, London: Routledge.

Bigo, D. (1998) 'Frontiers and security in the European Union: The illusion of migration control', in M. Anderson, M. and Bort, E. (eds) *The Frontiers of Europe*, London: Pinter.

Bigo, D. (2011) 'Freedom and speed in enlarged borderzones', in V. Squire (ed.), *The Contested Politics of Mobility: Borderzones and Irregularity*, Abingdon: Routledge.

Brussels Airport Company (2014) Brutrends 2014. Online. Available at www.brusselsairport.be/en/cf/res/pdf/corp/en/brutrends2014 [8 February 2016].

Buzan, B. (1991) 'New patterns of global security in the twenty-first century', *International Affairs*, 67(3): 431–451.

Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*, Boulder, CO: Lynne Riener.

Chandrasekhar, C.A. (2003) 'Flying while brown: Federal civil rights remedies to post-9/11 airline racial profiling of South Asians', *Asian Law Journal*, 10(2): 215–252.

Christiaens, J., Menichelli, F. and Gutwirth, S. (2015) 'To fly or not to fly – imposing and undergoing airport security screening beyond the security–privacy trade-off', PRISMS Deliverable 4.2. Available at: http://prismsproject.eu/wp-content/uploads/2012/04/PRISMS-D4-2.pdf [27 April 2016].

Foucault, M. (2009) *The Birth of Biopolitics. Lectures at the Collège de France 1978–1979*, New York: Picador.

Foucault, M. (2010) *Security, Population, Territory. Lectures at the Collège de France 1977–1978*, New York: Picador.

Friedewald, M., van Lieshout, M., Rung, S., Ooms, M., Ypma, J. and van den Broek, T. (2015) 'Report on statistical analysis of the PRISMS survey', PRISMS Deliverable 10.1. Available at: http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3674278.pdf [27 April 2016].

Glaser, B. and Strauss, A. (1967) *The Discovery of Grounded Theory*, Chicago, IL: Aldine.

Hammersley, M. and Atkinson, P. (1983) *Ethnography: Principles in Practice*, London: Tavistock.

Harcourt, B. (2006) 'Muslim profiles post 9/11: Is racial profiling an effective counterterrorist measure and does it violate the right to be free from discrimination?', *John M. Olin law and Economics Working Paper no. 288*. Available at: www.law.uchicago.edu/files/files/286.pdf [12 February 2016].

Harrington, J. E. (2014) 'Dear America, I saw you naked', *Politico*, 30 January 2014. Available at: www.politico.com/magazine/story/2014/01/tsa-screener-confession-102912 [10 February 2016].

IATA (2011) 'The impact of September 11 2001 on aviation', Special Report. Available at: www.iata.org/pressroom/Documents/impact-9-11-aviation.pdf [15 February 2016].

Khan, A. (2013) 'Airport profiling: A familiar story for Muslims', *The Huffington Post*, 19 May 2013. Available at: www.huffingtonpost.com/azeem-khan/racial-profiling-muslim_b_3303582.html [12 February 2016].

Larsen, M. and J. Piché (2009) 'Exceptional state, pragmatic bureaucracy, and indefinite

detention: The case of the Kingston immigration holding centre', *Canadian Journal of Law and Society*, 24(2): 203–229.

Lyon, D. (2003a) *Surveillance after September 11*, Cambridge: Polity.

Lyon, D. (ed.) (2003b) *Surveillance as Social Sorting: Privacy, Risk, and Digital discrimination*. Abingdon: Routledge.

Lyon, D. (2007) *Surveillance Studies: An Overview*, Cambridge: Polity.

Salter, M.B. (2007) 'Governmentalities of an airport: heterotopia and confession', *International Political Sociology*, 1(1): 49–66.

Salter, M.B. (2008) 'Introduction: Airport Assemblage'. In M. B. Salter (ed.) *Politics at the Airport*, Minneapolis, MN: University of Minnesota Press.

Schneier, B. (2003) *Beyond Fear*, New York: Copernicus Books.

Schneier, B. (2008) *Schneier on Security*, Indianapolis, IN: Wiley.

Slovic, P. (1987) 'Perception of risk', *Science*, 236(4799): 280–285.

Syed, N. (2010) 'Airport screening for "flying while Muslim"', *CNN*, 3 February 2010. Available at: http://edition.cnn.com/2010/OPINION/01/29/syed.muslim.while. flying/ [12 February 2016].

Torpey, J. (2000) *The Invention of the Passport*, Cambridge: Cambridge University Press.

Valverde, M. (2007) 'Genealogies of European states: Foucauldian reflections', *Economy and Society*, 36(1): 159–178.

Webb, M. (2007) *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*, San Francisco, CA: City Lights Books.

Zedner, L. (2008) 'The inescapable insecurity of security technologies?', in K.F. Aas, H.O. Gundhus and H.M. Lomell (eds) *Technologies of Insecurity: Surveillance and securitsation of everyday life,* Abingdon: Routledge, 257–270.

Part II

Emergent security and surveillance systems

6 The deployment of drone technology in border surveillance

Between techno–securitization and challenges to privacy and data protection[1]

Luisa Marin

Introduction: the EU and the techno-securitization of borders

It is commonly acknowledged by scholars that the Europeanization of national migration policy is caused by national failures in the domain, and that European migration policy can be explained through the theory of securitization. According to the latter, migration and migrants are framed, in political discourses (Weaver, 1995), by security actors (Bigo, 2000) and through practices (Balzacq, 2008), as security threats. This conceptual framing of migrants as security threats has led Member States and the EU to react to defend internal security from those alleged external threats. Globalization has turned the world into a 'global village', where goods, capitals and information circulate across the globe. However, this has not helped to decrease persistent inequalities between regions of the world. Western states, or the states of the Global North, have consolidated their interest in regulating the human dimension of globalization, i.e., human mobility. At EU level, the governance of human mobility aims at controlling the overall phenomenon of human migrations essentially by increasingly limiting legal migration and consequently fighting against irregular migration. This has attracted a number of criticisms, captured by the label 'Fortress Europe' and depicting Europe as an inaccessible fortress.

Within this process, border surveillance has gained relevance too. The EU and Member States are investing in technological applications, ranging from biometrics to databases, to drones and satellites. The aim is to deploy the most effective technological means in the attempt to face the security threats allegedly coming from outside and to make such controls more efficient. In the past few years, we have witnessed a consolidation of securitization discourses and practices, namely with a stabilization of the trend of deployment of all the available technological tools in border surveillance, which is here framed as techno-securitization (Marin, 2011; Marin 2016a). Just to mention some of the latest developments, the legislative package on Smart Borders, consisting of an Entry-Exit System (E-ES) and of a Registered Travellers Programme (RTP) has been presented (European

Commission, 2013a and European Commission, 2013b). It is currently being discussed in the legislative process. The Smart Borders package is meant to facilitate movement for selected categories of (low risk) travellers and to store biometric data of third-country nationals on entry and exit from the EU, in order to map the 'overstayers'. Alongside this, the European Border Surveillance System (EURO-SUR) has been created. As suggested by some scholars, the EU and Member States are consolidating (or transforming) the 'high-tech fortress' (Marin, 2011) or 'cyber-fortress' (Guild *et al.*, 2008) around Europe.

UAVs (Unmanned Aerial Vehicles) or RPAS (Remotely Piloted Aircraft Systems), simply known as drones, are part of this process. In the context of border surveillance, this techno-securitization takes shape in a militarization of border surveillance through the deployment of warfare assets and technologies for civilian purposes. It is functional to the extra-territorialization of border controls, in a never-ending attempt to move (the controls on) the borders outwards and, ultimately, to prevent undesired migrants from reaching Europe (Marin, 2016a). In this perspective, and thanks to the surveillance technologies they can carry, drones can contribute to the attainment of the objectives of EU border controls, i.e., to reducing the number of migrants illegally entering the EU, by preventing undocumented and undesired migration and, of course, also contributing to the fight against cross-border crime. Drones can provide information to border guards present on the ground, be it by sea or by land, and therefore help to make border surveillance a proactive policy, rather than a reactive one. These ground patrols, thanks to the information acquired by drones, could then take control of migrants. In the case of migration by sea, they could support them in case of distress, taking them to the nearest port, but also re-direct them to international seas or to the authorities of cooperating third countries, if bilateral agreements so provide.

This chapter will focus on the deployment of drone technology (DT) in border surveillance. The aim is to explore how it affects the relation between security on the one side, and privacy and data protection on the other side. Having introduced the theory of techno-securitization, the chapter then presents and analyses the impact of drone technology on the techno-securitization of borders. It starts by examining how the metamorphosis of the drone from a battlefield tool to a civilian asset is taking place, and then it focuses on the EUROSUR border surveillance network and on actual cases of deployment of drones in border surveillance operations. The analysis of the current practices aims to provide information on the deployment of drones and, second, to elaborate on the impact of DT on privacy and data protection obligations. What challenges for privacy arise from the current regulation on surveillance at the borders? Is the legal framework equipped for those challenges? The chapter concludes by recalling the challenges posed by the techno-securitization of its borders for privacy and data protection.

The deployment of drones in border surveillance and their contribution to pre-emptive techno–securitization

The metamorphosis of the drone: from warfare drone to a border defence drone

If the literature so far has been focusing on the deployment of drone technology in warfare, the 'metamorphosis' of war drones into a civilian 'tool' is more recent and still ongoing: therefore, it is only starting to receive the attention it deserves in the scholarly debate (Custers, 2016; Završnik, 2016). The current work aims at filling this gap in the literature, namely elaborating on the deployment of drones in border surveillance and their impact on the function of border surveillance, in the perspective of the relation between security on the one side and privacy and data protection on the other.

How did we get to the transfer of drone technology to the civil domain? Drones are best known for the targeted killing programmes carried out by Israel and the US in Middle East theatres of war, with CIA's famous 'personality strike' and 'signature strike' programmes. These triggered reactions within the international community for their dubious compatibility with the principles of proportionality, precaution and necessity in relation to civilian casualties (Alston, 2010; Rosén, 2013). Alongside this, targeted killings with drones have been accused of changing warfare, by lowering he threshold to engage with it (Alston, 2010; Human Rights Watch, 2012). However, drones were first developed as surveillance instruments and have been used for intelligence and reconnaissance since the Vietnam war; attack drones being the armed variant of drones, UAVs are, first of all, intelligence, surveillance, target acquisition and reconnaissance (ISTAR) devices/tools.

So, what is the peculiarity of drones and what makes them attractive for civilian and commercial uses? If the topic of the commercial exploitations of drones will remain out of the scope of this research, this section will focus mainly on border surveillance, as one of the main governmental exploitation of drones.

One of the main assets of drones – in addition to their being unmanned or remotely piloted aircrafts – is that they perform tasks usually characterized as the '3 Ds': dull, dirty and dangerous. From the technical viewpoint, they are surveillance tools and they enable the coverage of vast and remote areas that would be more difficult to reach with traditionally piloted aircrafts. For example, a Predator can fly for up to 20 hours. Drones can be equipped with cameras and thermal detection sensors. These can find small objects at a distance of 60,000 feet and detect humans moving across woods, also under foliage (Haddal and Gertler, 2010). Therefore, the attractiveness of drones is that they enable enhanced surveillance, compared to manned aircraft. Their value also lies in the amount of information and data that they can be allowed to collect, and in the use of those data from the deploying or, more correctly, the benefiting agency.[2]

Second, piloting at a distance makes it possible to keep pilots' lives safe, away from risks related to weather and other natural hazards. Another advantage of the unmanned drone is that the aircraft can stay airborne according to logic and necessity totally independent from human fatigue and pilots' shifts. This remoteness is

often seen as a benefit for the agency deploying the drones. However, it does not consider that other lives might be exposed to risks deriving from the operation of an aircraft instead of the deployment of a manned guard, for example (Gertler, 2012). One risk is the dehumanization of the surveilled (Marin, 2016b; Finn *et al.*, 2014).

Other reasons put forward to defend the deployment of drones in border surveillance concern economic arguments. Proponents of drone technology in border surveillance (in Europe: industry stakeholders, national administrations, Frontex, European Defence Agency and European Commission) argue that this technology is potentially cheaper than surveillance carried out with traditional manned aircraft.[3] Second, once developed and implemented, drones would make border surveillance operations less expensive, both in terms of human resources and material assets deployed, allowing for a rationalization of the resources employed (Gertler, 2012). In times where public agencies face financial restrictions, this economic argument is always attractive. Its actual validity is however strongly challenged by the American experience, where drones acquisition programmes have been suspended for financial reasons caused by inaccurate forecasts on the overall maintenance expenditures for drones.[4]

Surveillance networks in border surveillance: EUROSUR

The actual deployment of drone technology in border surveillance by EU Member States started late in comparison with the US, which have been using drones in border surveillance since 2004 (Marin, 2016b). However, it is rapidly increasing (Hayes *et al.*, 2014). The next section will first present the legal framework enabling the deployment of drones in border surveillance, and the ensuing sub-section will present practices and examples of the same. Here drones are considered a crucial technology, alongside others, in order to reshape surveillance of the maritime environment.

EUROSUR is a surveillance system whose aim is to sustain better border management of the EU's external borders. Surveillance is carried out by Frontex with the Member States' border authorities (European Commission, 2011; European Commission, 2013c). In a broader perspective, EUROSUR is part of the creation of a Common Information Sharing Environment (CISE) for the enhancement of maritime security. Drone deployment in border surveillance at EU level is part of a policy that aims at strengthening the surveillance of external EU borders – first, as a tool to control irregular migration, and second, within the context of EU's integrated maritime policy, which is setting up a Common Information Sharing Environment (CISE) since 2009. For this reason, shortly after the creation of Frontex, the Member States, the Council and the European Commission examined the feasibility of EUROSUR as 'a common technical framework to support Member States' authorities to act efficiently at national level, command at national level, coordinate at European level and cooperate with third countries in order to detect, identify, track and intercept persons, attempting to enter the EU illegally outside border crossing points' (European Commission, 2008: 1). In December

2013, less than 2 months after the Regulation was passed, EUROSUR was already operational for 18 EU member states at the southern and eastern external borders and Norway.

EUROSUR is composed of the National Situational Pictures, of the European Situational Picture and of the Common Pre-Frontier Intelligence Picture (CPIP). These give an overview or representation of the situation at and outside the EU borders, including information on prevention of unauthorized migration and cross-border crime. In particular, the CPIP (Art. 11, EUROSUR Regulation) aims at providing the national coordination centres (NCC) with 'effective, accurate and timely information and analysis on the pre-frontier area.' Among others sources, the CPIP is composed of information collected by Frontex, including information and reports provided by its liaison offices; information collected via third parties; and information collected from authorities of third countries, on the basis of bilateral or multilateral agreements and regional networks via the NCC. This indicates that EUROSUR is to be used as a platform to share information and to develop the intelligence dimension of border surveillance. Here drones, among other technologies such as satellites and ship monitoring systems, would play a central role in acquiring information on what happens at and outside the borders. Increased information will lead to so-called 24/7 blue/green situational awareness and implies the technical capacity of having full information on what happens at the borders (Marin, 2016a). Drones are of vital importance for EUROSUR since they will enable acquisition of crucial information, thanks to infra-red cameras, mobile phone jammers, thermal imagining devices and video cameras (Nolin, 2012).

EUROSUR strengthens Frontex's role as 'the' intelligence hub for border surveillance. In particular, article 12 of the EUROSUR Regulation mandates Frontex to 'coordinate the common application of surveillance tools in order to supply the national coordination centres and itself with surveillance information on the external borders and on the pre-frontier era on a regular, reliable and cost-efficient basis' (Art. 12 EUROSUR Regulation). Frontex provides the national coordination centres, at their request, with information on the external borders of the requesting state and on the pre-frontier area. Frontex can elaborate this information by analysing data collected from ship reporting systems, satellite imagery and sensors mounted on any vehicle, vessel or craft. This legal basis enables Frontex to combine and analyse the data collected from ISR drone operations.

The main purpose of EUROSUR is to share information and therefore to develop and strengthen intelligence and risk management at the external borders and in the pre-frontier area with a focus on prevention. Drones are therefore an important technology enabling a shift toward risk-oriented and preventive border surveillance, as an epiphany of the techno-securitization process of borders.

Drone deployment in border surveillance in Europe: some examples

Let us now turn to some examples and practices of drone deployment in border surveillance. In this context, the information is scarce and research in this domain can only attempt to sketch some insights.

Italy, for example, is a country that deploys drones for border surveillance and security purposes. Considering that one of the layers of EUROSUR is given by the (many) National Situational Picture(s), we can think that information acquired by one country (e.g., Italy) with the deployment of drones can be used to feed the EUROSUR system. Italy owns 12 UAVs, 6 MQ-1 Predators and 6 MQ-9 Reapers or Predator B; these MALE (medium altitude long endurance) drones can stay airborne for about 20 hours. Since October 2013, drones have been part of the technical equipment of the *Mare Nostrum* operation.[5] According to the information available, drones have been deployed in the area of Lampedusa, north of the Libyan shores and also at the Southern Libyan border (with Niger, Chad and Sudan). Patrolling the sea close to Libyan borders took place within the context of the EUBAM mission, terminated in 2014 due to the war in Libya. EUBAM was a civilian mission under the Common Security and Defence Policy, aimed at supporting the Libyan authorities in improving and developing the security of the country's borders. The mission supported Libya in developing border management and security through transfer of know-how and capacity building at the operational and strategic levels (advising, training, mentoring). Patrolling the Southern Libyan border was made possible by a bilateral (Italy–Libya) Technical Agreement (TA) of cooperation of November 2013, authorizing, among other things, border surveillance activities with drones.[6] The Predators and Reapers, launched from the Sigonella Italian and NATO Air Base, in Sicily, patrolled the Southern border, probably in order to collect information and ensure earlier detection of migrants (Amnesty International, 2014).

Another example of drone deployment is offered by the EU NAVFOR MED (later renamed SOPHIA) operation. Formally speaking this is not a border surveillance operation but a 'military crisis management operation contributing to the disruption of the business model of human smuggling and trafficking networks in the Southern Central Mediterranean (…)' (Art. 1 Council Decision of 18 May 2015 (CD CFSP 2015/778 of 18 May 2015). It is a Common Security and Defence Policy (CSDP) operation, discussed and agreed upon after the Lampedusa disaster of 18 April 2015. This was the most dramatic accident after the one of 3 October 2013, in which between 700–900 migrants lost their lives at sea. It represents a turn in border controls and in the management of irregular migration through fighting human trafficking and smuggling. The goal of the mission is to disrupt the business model of smugglers and traffickers, and possibly to prevent migrants becoming the 'objects' of criminal activities. For this purpose it makes a systematic effort to identify, capture and dispose of vessels and assets used or suspected of being used by smugglers or traffickers. This is done in accordance with applicable international law, including UNCLOS and any UN Security Council Resolution' (Article 1, CD). It operates alongside Frontex coordinated JO Triton, and it coordinates with it.[7]

It is organized in phases: phase 1 concerns surveillance and assessment of human smuggling and trafficking networks in the Southern Central Mediterranean; phase 2 entails boarding, search, seizure and diversion, on the high seas and in territorial waters, of vessels suspected of being used for human trafficking or smuggling; phase

3 entails the disposal of vessels and related assets and apprehension of traffickers and smugglers. Both the second and the third phases require a UN Security Council Resolution. The progress of the operation, which according to international law requires the consent of the coastal state, is uncertain because of the situation in Libya. At the time of writing operation SOPHIA has terminated its phase 1 and phase 2A, in international waters. Phase 2B would take place in territorial waters, for which there is a need for consent by the Libyan government. However, the situation in Libya presents/creates legal and political challenges that do not allow the operation to move forward. The EU is currently supporting the formation of a Government of National Accord in Libya which might represent a partner allowing the further progress of the operation toward phase 2B and 3 (European External Action Service, 2016).

Without dealing here with the legal issues concerning this operation, one has to stress that drones are also being used in this operation, at least both by Italy and by the UK, currently for surveillance and reconnaissance. If the operation at one point moves forward, drones – technically speaking – could also be used to destroy vessels. In this case too drones, together with other heavy defence means, are used for ISR operations and appear functional to a pre-emptive turn in border surveillance and in the management of migration. This turn requires fighting traffickers and smugglers with military technology, such as satellites, sensors and drones. EUNAVFOR MED is certainly a step in this direction. It is not formally a border surveillance operation, but it aims at transferring defence instruments, assets and technology to the borders and beyond: it is defence assets placed to defend the borders. It therefore represents a consolidation of the militarization of border surveillance and a further step in the direction of its externalization to the countries of departure, contributing to the techno-securitization of borders.

Having presented the rationales for deploying drones in border surveillance (and defence), alongside the legal framework for the surveillance of borders and some practices of it, the section concludes that by using drones, governmental agencies aim at strengthening surveillance, intelligence and coordination toward anticipatory border surveillance and prevention of migration. This section illustrates that drones are a key surveillance technology in this process; together with other technologies, such as satellites, drones are functional to a process of techno-securitization of borders.

The chapter will now focus on drones' impact on privacy and data protection issues.

Enhanced surveillance by drones and its impact on privacy and data protection rights

Drones, privacy and data protection

Starting from the consideration that borders are the legal and physical spaces where states exercise control on individuals in order to maintain their sovereignty, does the deployment of drones affect privacy and data protection? This section examines to what extent enhanced border surveillance can represent an issue, and also

to what extent the legal framework addresses the high potential of surveillance of drones. It does not aim at offering comprehensive research but rather sketches some of the issues for privacy and data protection deriving from the deployment of drones (Marin and Krajčíková, 2016; Finn *et al.*, 2014).

The deployment of drones for (border) surveillance potentially challenges the privacy and data protection rights of individuals found by the surveillance devices drones carry (high resolution optical camera, infra-red thermal camera, GPS, to name some): they should be considered as mobile CCTV. The privacy and data protection risks relate to the collection of images, sounds and geo-location concerning identified and identifiable persons (Art. 29 Working Party, 2015).[8]

Drones being a sense-and-detect technology, they can indeed collect and transmit information to the drone operator, including visual data.[9] It can be information about fishermen, tourists, migrants or more generally anyone finding himself or herself in the Mediterranean. At the same time, drones make it possible to interfere with private premises (for example, a boat sailing on the sea) due to the capacity of the technology they carry to collect data without the need for a direct line of sight. Here the challenges to privacy are multiple: first of all, drones represent a risk for the privacy of persons and for their data protection rights. Second, drones represent a risk for drone users because they have – in principle – to comply with respect for privacy and data protection obligations.

As to persons' privacy rights, drones first of all make it difficult for individuals to know that they are the subjects of surveillance: there is a lack of transparency on the types of processing because of the impossibility of seeing drones from the ground; there is a difficulty about knowing the equipment on board, and monitoring for what purposes data are collected and by whom. In short, surveillance by drones complicates the exercise and enforcement of rights as constructed by the European and national regulations (Art. 29 Working Party, 2015). Such technologies could also enable the collection of data for a long period of time and across large areas; this triggers the risk of 'bulk data gathering and possible unlawful multi-purpose uses' (Art. 29 Working Party, 2015: 8). The deployment of new technologies such as drones potentially represents a major interference with privacy and brings a risk of function creep. In a regulatory perspective, it is therefore important that legislators and regulators monitor the risks and consequences of the deployment of drones for surveillance. This also applies in the case of processing personal data for law enforcement purposes. Drones, together with the surveillance technology they can carry, represent 'game changers' in the direction of an anticipatory policing (Sandvik, 2016; Milivojevic, 2016). Mass data collection is functional to new practices of policing directed toward continuous surveillance, enabling determination of targets from a review of the lives and activities of a specific population (Art. 29 Working Party, 2015). So, all the more in the case of governmental activities, drones should only be used if less intrusive instruments are not suited to the achievement of such purposes. In any case, drones should not be used to conduct indiscriminate surveillance, bulk data processing, data pooling and data profiling. The legislator should avoid drones being used for signalling targets based on data analysis.

The normative framework of privacy and data protection

Border surveillance must be placed in the broad context of law enforcement functions. It is especially sensitive because of its implications for transparency of operations, enforcement of rights and also possible cooperation with third countries. Having mapped (some of) the issues related to privacy and data protection in this domain, let us turn to the normative framework, in order to see whether the legal framework covers those issues adequately.

These questions are relevant because in the EU legal order, respect for privacy and the right to protection of personal data have fundamental rights status and are codified in Articles 7 and 8 of the Charter of Fundamental Rights (hereinafter: FR) of the EU. Alongside this, Article 16 of the TFEU enshrines EU competence on data protection. Within the legislation, the Data Protection Directive 95/46/EC (hereinafter: DPD), and the Framework Decision 2008/977/JHA (hereinafter: the DPFD) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters are core instruments. They have inspired the constitutional guarantees of the Charter of FR. The DPD and the DPFD are now in the process of being repealed by the General Data Protection Regulation and by the Police and Criminal Data Protection Directive: at the time of writing, the 'trilogues' meetings have been concluded and an agreement on a text has been reached.

The DPD is the backbone of data protection at EU level. Its scope covers 'the processing of personal data wholly or partly by automatic means'. By contrast, it does not cover 'processing operations concerning public security, defence and state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in the areas of criminal law' (Articles 3 and 13, DPD). So, the DPD allows Member States to restrict the scope of the obligations and rights protected by the DPD, if this is necessary in order to protect, among other matters, national security, public security, and for the 'prevention, investigation, detection and prosecution of criminal offences' (Article 13, para. 1, letters a), c), d), DPD).

It is not so clear how to relate border surveillance with reference to this law enforcement exception of the DPD. It is clear that border surveillance is connected to the protection of public security, and also to the prevention, detection and prosecution of crimes connected to irregular migration, smuggling and illegal trafficking. However, we should consider that this represents an exception from the application of the DPD. Alternatively, it could be framed as a limitation of the fundamental right of data protection, and any limitation to EU fundamental rights has to respect the rule of law and the proportionality principles. Second, after the *Digital Rights Ireland* judgment,[10] it should be noted that the protection of public security might not entail a generalized surveillance and storage of data of individuals without a clear relation to investigations on crime. With the *Schrems* judgment,[11] the Safe Harbour Decision, allowing for simplified transfer of personal data between EU and US commercial companies, was annulled because of its lack of compliance with privacy and data protection obligations, in light of factual

elements that emerged after Snowden's revelations. These judgments have the important meaning of requiring that surveillance measures (namely, the data retention directive) as well as data exchange agreements are embedded into the traditional guarantees of the rule of law and respect for fundamental rights, and that the trade-off between security and privacy cannot be achieved by sacrificing guarantees of privacy and data protection (van Lieshout *et al.*, 2013). Third, even if border surveillance might fall within the scope of the law enforcement exception of the DPD, both the Frontex Regulation and the EUROSUR Regulation bear provisions aimed at anchoring the processing of personal data to the national and European frameworks on data protection. To conclude, there is a need to clarify the legal framework for border surveillance activities and, vice versa, to anchor the latter activities to a legal framework capable of protecting rights but at the same time guaranteeing adequate exercise of law enforcement powers. According to the European Convention of Human Rights and to the Charter of FR, restrictions to FR must be provided for by law and must respect the requirements of necessity, of being apt to fulfil the objectives of general interests and of proportionality. The recent militarization of border surveillance, the externalization of border controls policies to TC and the further expansion of defence functions toward border control issues represent a further threat to the embedding of these operations into a strong legal framework, and might therefore, jeopardize those rights. In the future, this domain will be covered by the new Police and Criminal Data Protection Directive and this will guarantee some uniform standards, even when Member States act in purely internal situations (Finn *et al.*, 2014).

Having sketched the general framework, the domain of border surveillance offers specific provisions on data protection. Borders are not the place to invoke 'the right to be left alone'. However, the right to data protection is nevertheless a fundamental right that is separate from the right to privacy; it regulates the relation between public authorities and individuals and limits the powers of the former to the respect of rights of the latter (González Fuster and Gutwirth, Chapter 10, this volume). To this purpose, the EUROSUR Regulation and the techno-securitization of borders, by enabling extensive surveillance, potentially limit the privacy and data protection rights of the individuals involved. In the EUROSUR system, in principle 'any exchange of personal data in the European situational picture and in the common pre-frontier intelligence picture should constitute an exception' (EUROSUR Regulation, recital 13). However, Article 13 guarantees that the processing of personal data within EUROSUR is anchored to the European and national frameworks for data protection, and carried out with respect for the principle of purpose limitation. Moreover, sensitive issues remain in the cooperation of Frontex with third-country authorities (TCA) in the framework of border surveillance. In this context too, the exchange of personal data should constitute an exception. Furthermore, 'it should be conducted on the basis of existing national and Union law and should respect their specific data protection requirements'.[12] This means that data collected for EUROSUR can be transferred to TCA. This still begs the question of the fate of those data and of the persons they refer to once in the hands of TCA. Connected to this, another important challenge to data

protection emerges from the cooperation of Member States with neighbouring TC. Member States can include information gained from cooperation with TC in the national situational picture and exchange information according to Art. 20 of the EUROSUR Regulation. Article 20 provides that exchange of personal data shall be strictly limited to what is absolutely necessary for EUROSUR. Though strictly limited, the exchange of personal data is still possible, and this triggers, again, the question of the fate of those data, once in the hands of TC institutions. How can the European institutions (Commission *in primis*) and the Member States monitor the respect of data protection provisions, after they have exchanged data, e.g., with Tunisian or Libyan authorities? The threat of function creep is here. The fact that some of these agreements are secret does not help accountability and the exercise of rights. The *Schrems* judgment is of relevance here and it recalls the strict boundaries for the transfer of personal data toward TC. Cooperation with TCA does not guarantee respect for data protection principles as implemented within the EU, and, more radically, brings more fundamental challenges on the respect of human rights of migrants (Marin and Krajčíková, 2016).

Another threat represented by the deployment of drones is the so-called chilling effect: the extended and continued surveillance of broad areas could deter migrants' vessels from using a specific route and perhaps could push them to use a more dangerous route, further endangering the lives of migrants. Drones can technically follow the routes of selected vessels, take images of what the crew is doing and prevent a cell phone from receiving a signal. To sum up, the EUROSUR Regulation embeds border surveillance into the network of national and European data protection provisions. However, it cannot be forgotten that large-scale surveillance in the Mediterranean can also cause a 'chilling effect' or self-disciplining effect or even affect society's expectations and interpretations of privacy. For this reason, it is important that public and independent authorities monitor the deployment of new technological 'eyes in the sky' and surveillance systems and their impact on privacy and data protection; on the other side, law enforcement agencies should provide information on their actions in compliance with transparency and accountability.

Conclusions

The chapter has presented one of the law enforcement domains, border surveillance, where security and privacy are in conflict. As in other justice and home affairs policies, in border surveillance too the EU and Member States are investing in technological and military applications in order to strengthen the security of the maritime environment. The aim is also to prevent irregular migration and crime.

Drones are already playing a role in this context and we should expect that this technology will be developed in the future, so that their deployment will increase. Italy deploys them already and Frontex has shown interest in them and is supporting R&D in the domain. Compared to manned aircraft, drones can stay airborne for longer times and therefore can provide more complete and accurate information on what happens at sea. The proponents of this technology suggest that there

are also economic advantages: namely drones are deemed to be cheaper compared to manned aircrafts, but it is not really straightforward to calculate these economic advantages.

Drone deployment is part of a process that is consolidating a shift in border surveillance from an emergency-driven policy to an intelligence and risk management approach of border surveillance. The creation of EUROSUR, enabling national and European agencies to share information on what happens at their borders, is to be read in this process. Drones seem to be a crucial 'game changer' in the shift from reactive border surveillance toward anticipatory border surveillance, which also seems to postulate, to some extent, the cooperation of third countries.

The chapter has shown that the deployment of drones raises several issues. Drones should be considered as mobile CCTVs and therefore their deployment should be accompanied with adequate assessment of their implications. Second, in the current legislative setting, data protection issues in this domain are subject to national legislations: the domain of law enforcement and criminal law is indeed representing a derogation to the European Data Protection Directive. Currently, there might be divergences and different rules in place at national level. In the future, the domain will be covered by the draft Police and Criminal Law Data Protection Directive and this will represent a common ground to which all national law enforcement agencies will have to adhere.

Second, in spite of the guarantees of the EUROSUR Regulation (EUROSUR's primary aim is not to collect personal data). In the Regulation there are avenues for sharing data with TCA, both for Member States but also for Frontex. Indeed, EUROSUR provides for a common pre-frontier intelligence picture to be fed with information received by TCs, which is a problematic issue, in light of the level of rule of law and protection of rights of migrants in those states. Once the data are transmitted to the third countries, there is a risk of function creep that can hardly be controlled from Europe. So, even if constrained by fundamental rights provisions on data protection, increased surveillance of borders, and the possibilities for cooperation with third-country authorities, challenge the safeguards provided by the European legislations. Third, it is important that transparency is safeguarded, as without transparency the enforcement of rights is prejudiced. The chapter therefore suggests that with the deployment of drones in border surveillance there are several instances of tensions between privacy and data protection, which are at the core of the European and national legal orders. For these reasons, it is important that the deployment of new technologies in law enforcement domains is adequately monitored in order to assess their implications.

Notes

1   The author thanks the editors for useful comments on a previous draft of the chapter. The usual disclaimer applies.
2   The deploying and benefiting agencies could be different actors. For example, a deploying agency might well be the Air Force, while the benefiting agency might be the Ministry of Interior.

3 In Gertler (2012, p. 5) one can read: 'Congress has noted that, "while the acquisition per unit cost may be relatively small, in the aggregate, the acquisition cost rivals the investment in other larger weapon systems'." Second, while a Predator vehicle costs $4.5 million, the Predator system, including four air vehicles and control equipment, costs over $20 million (Gertler, 2012).

4 Marin and Krajčíková (2016, p. 110) (quoting Sternstein, 2012), about problems experienced in the US: in 2012 the fleet was unused for 63 per cent of the time. This was due to a lack of budgeting for drone operations as well as associated costs for drone maintenance and drone-related equipment. For more recent data, confirming the same problems with the US Drone Border Patrol Program, see Hoffman 2015.

5 *Mare Nostrum* is an operation of a military nature with humanitarian and security purposes, launched by the Ministry of Defence in cooperation with the Ministry of Internal Affairs. It was launched in the aftermath of the Lampedusa disaster of October 2013, in which more than 360 migrants lost their lives in one day. It was in operation until October 2014, and was discontinued due to the high costs involved in the operation financed by Italy and, in the view of the Italian government, the lack of participation by other European states. Recognizing the effort carried out by Italy, the Member States and the EU agreed to replace *Mare Nostrum* with the Frontex coordinated Joint Operation (JO) *Triton*, which nevertheless had a less extended (up to 30 miles from the Italian coast) and a different operational area compared to *Mare Nostrum,* until the disaster of 18 April 2015.

6 An earlier agreement on bilateral cooperation of 28 May 2012 also had as its main goal the training of Libyan authorities, also through operation 'Cyrene'.

7 'Moved to prevent further loss of life at sea and to tackle the root causes of this humanitarian emergency', 'the European Council committed to strengthening the Union's presence at sea, to preventing illegal migration flows and to reinforcing internal solidarity and responsibility' (CD, recital 2).

8 Personal data are defined as 'any information relating to an identified or identifiable natural person', according to the DPD.

9 Visual data are personal data, as stated by the European Court of Human Rights in *Peck v. UK*, Application No. 44647/98, judgment of 28.1.2003, para. 59.

10 Court of Justice (Grand Chamber), Judgment of 8 April 2014, Joint Cases C–293/12 and C–594/12 *Digital Rights Ireland Ltd* v. *Ireland*, nyr.

11 Court of Justice (Grand Chamber), Judgment of 6 October 2015, C–362/14 *Maximillian Schrems* v. *Data Protection Commissioner*, nyr.

12 Recital 13 of the Preamble, EUROSUR Regulation.

References

Alston, P. (2010) 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions', available at www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (last accessed 13 August 2015).

Amnesty International (2014) 'Amnesty International's Submission to the Council of Europe Committee of Ministers: Hirsi Jamaa and Others v. Italy (Application No. 27765/09)', available at www.amnesty.eu/content/assets/Doc2014/B1525_-_second_submission_Hirsi_-_11_Feb_2014.pdf (last accessed 2 May 2016).

Art. 29 Data Protection Working Party (2015) 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones', 01673/15/EN WP 231, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (last accessed 2 May 2016).

Balzacq, T. (2008) 'The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Politics', *Journal of Common Market Studies*, 46(1): 75–100.

Bigo, D. (2000) 'When Two Become One: Internal and External Securitizations in Europe', in M. Kelstrup and M.C. Williams (eds), *International Relations Theory and the Politics of European Integration: Power, Security and Community,* London: Routledge.

Council Decision (CFSP) 2015/972 of 22 June 2015 on a European Union Military Operation in the southern Central Mediterranean (EUNAVFOR MED), *Official Journal of the European Union L* 157, 23 June 2015, p. 51, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0972 (last accessed 14 November 2016).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal matters, *Official Journal of the European Union L* 350, 30 December 2008, 60–71.

Custers, B. (ed.) (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*, The Hague; TMC Asser Press.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such Data, *Official Journal of the European Communities L* 281, 23 November 1995, 31–50, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (last accessed 14 November 2016).

European Commission (2008) 'Examining the creation of a European Border Surveillance System (EUROSUR)'. COM(2008) 68 final, 13.2.2008, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008DC0068&from=EN (last accessed 2 June 2015).

European Commission (2011) Proposal for a Regulation of the European Parliament and the Council establishing a European Border Surveillance System (EUROSUR), COM(2011) 873 final, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur_final.pdf (last accessed 30 July 2014).

European Commission (2012a) Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en (last accessed 2 May 2016).

European Commission (2012b) Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM(2012) 10 final, 25.1.2012, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en (last accessed 2 May 2016).

European Commission (2013a) Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to Register Entry and Exit Data of Third Country Nationals Crossing the External Borders of the Member States of the European Union, COM(2013) 95 final, 28.2.2013, available at: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf (last accessed 29 April 2016).

European Commission (2013b) Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Program, COM(2013) 97 final, 28.2013, available at: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v14.pdf (last accessed 29 April 2016).

European Commission (2013c) 'EUROSUR: Protecting the Schengen External Borders Protecting Migrants' Lives', available at: http://europa.eu/rapid/press-release_MEMO-13-1070_en.htm (last accessed 10 September 2014).

European External Action Service (2016) 'EUNAVFOR MED Op SOPHIA – Six Monthly Report 22 June–31 December 2015', available at: https://wikileaks.org/eu-military-refugees/EEAS/EEAS-2016-126.pdf (last accessed 2 May 2016).

Finn, R., Wright, D., Jacques, L. and De Hert, P., (2014) Study on Privacy, Data Protection and Ethical Risks in Civil RPAS Operations. Final Report. Publications Office of the European Union, available at: http://ec.europa.eu/DocsRoom/documents/8550 (last accessed 20 April 2016).

Frontex (2014) *Border Surveillance*, available at: http://frontex.europa.eu/research/border-surveillance (last accessed 23 April 2015).

Gertler, J. (2012) 'U.S. Unmanned Aerial Systems', Washington, DC: Congressional Research Service, available at: www.fas.org/sgp/crs/natsec/R42136.pdf (last accessed 2 May 2016).

Guild, E., Carrera, S., and Geyer, F. (2008) 'The Commission's New Border Package: Does It Take Us One Step Closer to a "Cyber Fortress Europe"?', CEPS Policy Brief No. 154, available at: www.ceps.eu. (last accessed 10 June 2015).

Haddal, C.C. and Gertler, J. (2010) 'Homeland Security: Unmanned Aerial Vehicles and Border Surveillance', Washington, DC: Congressional Research Service, available at: www.fas.org/sgp/crs/homesec/RS21698.pdf (last accessed 2 May 2016).

Hayes, B., Jones, C. and Toepfer, E. (2014) *Eurodrones, Inc.* Amsterdam: Transnational Institute, London: Statewatch, available at: www.statewatch.org/news/2014/feb/sw-tni-euro-drones-inc-feb-2014.pdf (accessed 29 April 2016).

Human Rights Watch (2012) 'Losing Humanity. The Case against Killer Robots', available at: www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf (last accessed 5 February 2016).

van Lieshout, M., Friedewald, M., Wright, D., Gutwirth, S. (2013) 'Reconciling Privacy and Security', *Innovation: The European Journal of Social Science Research*, 26(1–2): 119–132.

Marin, L. (2011) 'Is Europe Turning into a "Technological Fortress"? Innovation and Technology for the Management of EU's External Borders. Reflections on Frontex and EUROSUR', in M.A. Heldeweg and E. Kica (eds), *Regulating Technological Innovation: Legal and Economic Regulation of Technological Innovation*, Basingstoke: Palgrave Macmillan, 131–151.

Marin, L. (2016a) 'The Humanitarian Drone and the Borders. Unravelling the Rationales Underlying the Deployment of Drones in Border Surveillance', in B. Custers (ed.) *The Future of Drone Use*, TMC Asser Press.

Marin, L. (2016b) 'The "Metamorphosis" of the Drone: Challenges Arising from the Deployment of Drone Technology in Border Surveillance. An Exploratory Study', in D. Bowman, E. Stokes and A. Rip (eds) *Embedding and Governing New Technologies: A Regulatory, Ethical and Societal Perspective*, Singapore: Pan Stanford Publishing.

Marin, L. and Krajčíková, K. (2016) 'Deploying Drones in Policing European Borders: Constraints and Challenges for Data Protection and Human Rights', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Milivojevic, S. (2016) 'Re-bordering the Peripheral Global North and Global South: Game of Drones, Immobilising Mobile Bodies and Decentring Perspectives on Drones in Border Policing', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Nolin, P. C. (2012) *Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance. Special Report*. Canada: NATO Parliamentary Assembly.

Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), *Official Journal of the European Union L 295* (6 November 2013), 11–26, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1052 (last accessed 14 November 2016).

Rosén, F. (2013) 'Extremely Stealthy and Incredibly Close: Drones, Control and Legal Responsibility', *Journal of Conflict & Security Law*, 19(1): 113–131.

Sandvik, K.B. (2016) 'The Political and Moral Economies of Dual Technology Transfers: Arming Police Drones', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Weaver, O. (1995) 'Securitization and Desecuritization', in R. Lipschutz (ed.) *On Security*, New York: Columbia University Press, 46–86.

Završnik, A. (ed.) (2016) *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

7 Perceptions of videosurveillance in Greece

A 'Greek paradox' beyond the trade-off of security and privacy?

Lilian Mitrou, Prokopios Drogkaris and George Leventakis

Introduction: video surveillance as 'normality'

In Greece, the use of closed-circuit television (CCTV) for a variety of security purposes emerged gradually throughout the 1990s, mainly in the banking sector. However, over the past decade the use of CCTV systems was expanded and was not limited to monitoring and managing traffic flows or banks. Video surveillance in public and/or publicly accessible places was not any more an exceptional or occasional phenomenon (Samatas, 2008). Since the mid-2000s CCTV systems have been deployed by a variety of public and private entities and persons. The deployment of CCTV has become increasingly common not only with regard to protection of critical infrastructures in the transport sector (particularly airports, railways, metro systems and power stations), but also in spaces dedicated to public gatherings, public areas and shopping centres as well as small shops, offices, schools, playgrounds etc.[1]

The exponential growth of CCTV in Greece has not taken place in a social vacuum. It reflects a worldwide trend as in less than two decades CCTV has been transformed from a local initiative into a phenomenon that penetrates the urban life in every major city.[2] Similar to most late modern societies (Webster *et al.*, 2011), where CCTV is a 'defining feature' (Norris, 2012), in Greece video surveillance has also become a 'normality' to deal with security concerns. Cameras are sometimes regarded as a 'panacea for all public and private troubles' (Samatas, 2008). CCTV systems are presented as a new and cost-effective way to prevent and deter crime, prosecute offenders and reassure citizens who are preoccupied with their safety.

The widespread use of such devices has generated media and public interest. While the use of cameras by the police has been contested,[3] the remarkably rapid diffusion of CCTV in Greece has developed in parallel with concerns and protests. There have been reactions about citizen-state relations, the efficiency of video surveillance, the empowerment of police authorities to the detriment of the institutional role of the Hellenic Data Protection Authority (hereafter DPA), the impact of their use on informational privacy and other fundamental rights.[4] Prima facie,

CCTV (systems) are deployed and perceived in Greece more as *ad hoc* 'safety and security tools' for 'protection' and 'crime prevention and enforcement'. Such systems are not primarily understood as a form of surveillance, i.e. as a process of monitoring, collecting of information and systematic classification and social sorting (Lyon, 2001). Despite reactions, CCTV seems to have been met with some acceptance, if not popularity, among politicians, practitioners and the general public.

The value which individuals place on privacy and security, when it comes to surveillance, is at the heart of the privacy/security trade-off debate. The use of CCTV in public and publicly accessible places, such as public transport and metro stations, is suitable for exploring citizens' preferences, when elements of privacy and security are in conflict with each other. The relevant theme of the PACT project[5] explored whether there is empirical evidence that suggests that privacy/security is a false dichotomy or EU citizens view it as a zero-sum game (Amicelle *et al.*, 2012).

The PACT project has questioned the trade-off relationship by investigating perceptions of security and privacy and respective preferences therefore. The survey used stated preference experiments to estimate people's preferences and willingness to pay for security and surveillance measures. To capture the nuanced nature of security, surveillance and privacy the PACT survey has focused on three different contexts: (a) travelling on the metro or railway, (b) choosing an internet service provider (ISP) and (c) selecting a health-data records device/service. In the context of travelling on the metro or on a train and use of CCTV surveillance technology ('travel scenario') participants were asked to consider scenarios relating to the presence of CCTV cameras, security checks, and type of security personnel at rail or metro stations.

The measurement of the value that individuals are willing to place upon privacy or security is rendered more complex by considering attitudes that relate to each national history and culture (Budak *et al.*, 2016). Citizens' preferences vary across countries and among individuals (Potoglou *et al.*, 2014). Country specific effects concern mainly the use of CCTV and storage of CCTV data, the presence of security personnel and security checks in the travel context. Contrary to preferences registered in most EU member countries, respondents in Greece prefer real-time monitoring while indicating a strong disinclination for storage of CCTV data. The unique approach of CCTV systems use and security measures in Greece has raised the question of whether it has to be interpreted as specificity, a 'Greek (privacy) paradox' or as confirmation of the hypothesis that the preferences for security and privacy (and the respective trade-off relationship) are highly context dependent; this context being manifold and ranging from the present socio-economic environment back to political and institutional history.

This chapter presents the findings of the PACT travel survey with reference to the findings of other related and/or similar surveys (Eurobarometer, Greek surveys, and findings of other projects, such as PRISMS).[6] Further, we provide an overview of the recent history of CCTV systems deployment in Greece. Taking into consideration that the level of privacy and data protection regimes may shape the extension, diffusion and intensity of CCTV (Hempel and Töpfer, 2004), we discuss legal perceptions with regard to privacy in public and security as well as the

constitutional and regulatory framework. In order to better understand the 'Greek paradox', we focus on historical experiences and factors, such as the recent political history marked by dictatorships, which have fed the distrustful attitudes between citizens and the state-public institutions and reproduced a 'negative surveillance culture' (Samatas, 2004). In this context we present the tolerant attitudes of Greeks towards private surveillance systems. In the final section we discuss to what extent risks, uncertainties and fears in an environment of economic and social crisis are mirrored in privacy perceptions and attitudes and how these attitudes relate to the approach to the security–privacy trade-off.

Statistics and preferences: converging, diverging and contradictory results

PACT's empirical work investigated public perception of security and privacy across 27 Member States (MS) of the European Union (1,000 respondents per MS). To enable collection of the empirical evidence, a survey questionnaire was designed and deployed in the Member States. The PACT survey investigated hypotheses related to privacy and security preferences against different demographic groups (urban versus rural settings, low-income versus high-income households, people with low versus high level of educational attainment etc.). The survey's respondents were also assigned to different categories on the basis of their familiarity and experiences in the contexts in which they provided their preferences for security and privacy. As respondents' attitudes, such as concern and trust, were taken to play a significant role in their preferences related to privacy and security, a range of attitudinal indicators has been identified in order to measure security–privacy concerns, and respondents' levels of trust.

The survey aimed at testing whether respondents preferred security and surveillance technologies without threats to their privacy over those which could pose threats to privacy. Stated preference discrete choice experiments have been designed to support subsequent analysis of preference data using discrete choice models. The questionnaire contained stated preference choice exercises.

In the 'travel survey' that formed a key part of the PACT pan-European survey, respondents were asked to consider scenarios relating to the presence of CCTV cameras, security checks and the type of security measures in the metro and other public transport stations. Participants had to assess and express their preferences with regard to the type of CCTV camera, the storage period, the access to the footage captured by the camera as well as the type of security personnel at stations (Patil *et al.*, 2015).

In general, the researchers have observed similar preferences across EU countries, where respondents are in favour of CCTV cameras that store data for a certain amount of time and which can be accessed by Law Enforcement Agencies within the country. Respondents were more likely to choose travel situations involving CCTV cameras at stations; they were even in favour of advanced CCTVs that can detect faces (Patil *et al.*, 2015). The second most favourable option was CCTV cameras that could detect abandoned bags, followed by systems that could

recognise suspicious movements of people and, finally, standard CCTV (Potoglou *et al.*, 2014). Greece belongs to the few countries (Bulgaria, Czech Republic, Denmark, Hungary, Latvia, Poland, Portugal and Slovakia) that do not reject the use of such surveillance systems; however the preference for CCTV cameras is weaker compared to other countries in the European Union.

As far as the storage of CCTV data is concerned, the most favourable preference was fifteen days' storage time, followed by seven days and three days. In contrast to preferences in most EU27 countries, respondents in Greece indicated a strong disinclination for storage of CCTV data, preferring real-time monitoring (Patil *et al.*, 2015). According to the findings of the survey, Greece is the sole country whose participants prefer settings with CCTV footage only used in real time versus those settings in which the footage is stored for a specific number of days. Furthermore, in contrast to all other countries, respondents from Greece preferred unarmed police personnel and rejected the idea of private personnel (Patil *et al.*, 2015).

The results of PACT correspond to those of Eurobarometer no. 359, a large survey conducted in 2010–2011, regarding citizen's behaviours and attitudes concerning identity management, data protection and privacy.[7] While a majority of Europeans were not concerned about their behaviour being recorded in a public space (62 per cent), Greece was the only country where a majority of respondents were concerned about this issue (54 per cent) and in particular by all situations mentioned in the survey (public places: streets, subways, airports) (European Commission, 2011).

Similar attitudes are also registered in the Survey of PRISMS project with regard to crowd surveillance: Greeks, Austrians and Germans are the most sceptical concerning the monitoring of demonstrations and similar events (van den Broek *et al.*, 2016). The average score on the police survey vignette is much lower meaning more acceptance, being 2.72 with the lowest average being 2.699 (Greece) (van den Broek *et al.*, 2016).

Some years earlier, a survey of users of public transport regarding CCTV has produced indeed mixed results. In this survey, conducted in Greece in 2007 (a week after an attack against the USA Embassy and violent clashes between anarchists and riot police in central Athens), nearly two-thirds of respondents were in favour of police using CCTV on roads in Athens for security purposes[8]. The results of this poll were interpreted as 'a substantial shift in public opinion which until then had viewed the surveillance system as an intrusion on people's privacy' (Samatas, 2008). The same results were generalized to suggest that 57 per cent of Greeks thought that cameras protect people rather than violate their personal or political rights. It is important to note that 70 per cent of the respondents said that rights and freedoms were often not protected (Panousis, 2010). According to the same survey, Greeks were in favour of CCTV systems use in banks (92 per cent), football stadiums (87 per cent), public services buildings (71 per cent), streets in town centres (67 per cent), shops (66 per cent), schools (59 per cent), universities (53 per cent), parks and squares (51 per cent) and public transport (50 per cent).

Similar perceptions and preferences have been confirmed by a survey conducted

during 2008–2009 (online and offline) by the University of Crete among 178 students. According to the results of the online survey, 82 per cent of the respondents regard the 'widespread use of security cameras in public and private places' as embarrassing. However, it is noteworthy that in the offline survey (class discussions) this percentage decreased significantly to less than 50 per cent as more than half of the students declared that they felt secure and were not disturbed by the use of security cameras in public and private areas. Moreover, 53 per cent of the students (24 per cent totally) agree that cameras for traffic control should be used by the police for security reasons and public order, while 45 per cent 'disagree' and 31 per cent 'disagree totally' (Samatas, 2013).

A short history of CCTV in Greece

In 2000, the Hellenic DPA set out guidelines restricting the use of CCTV in public and publicly accessible places. Before 2000, storage and transmission of an image of an individual by closed-circuit television was viewed as processing of personal data, in terms of the Greek Data Protection Law 2472/1997 (article 2 par. d) but there were no specific provisions with regard to video surveillance at place. According to the respective DPA's Directive (1122/2000), recording and processing of personal data with the use of closed-circuit television that operates permanently, continuously or at fixed intervals, is not allowed in principle, as it offends the individual's personality and private life. The DPA has regarded CCTV recording as lawful only for the protection of individuals or goods or for traffic monitoring and only under the condition that the deployment of a CCTV system complies with the principles of purpose specification, necessity and proportionality, while laying down legal and technical restrictions.[9]

The first massive use of CCTV systems in public places was related to the security challenges of the Athens Olympic Games in 2004. Indeed, the first Olympic Games after the terrorist attacks of 11 September 2001 have been a 'catalyst' for the exponential growth of CCTV systems in public areas. An integrated surveillance system was meant to shield the 2004 Olympic Games against the threat of terrorist attacks. The central surveillance integration security system, the so-called C4I, was designed to include a large-scale surveillance integration security network composed of 30 subsystems[10] and to provide the possibility of continuous online linking and processing, evaluation, classification, and identification of personal data, rendering the Olympic Games 'a showcase for "superpanoptic" surveillance capabilities' (Samatas, 2007). In 2004 the DPA approved the request to operate the C4I system during the 'operational phase' of the Olympics and Paralympics.

As expected, the government urged legalizing the operation of this CCTV system even after the Games were over and requested the extension of the processing purposes in order to cover as many activities taking place in public (from traffic control to marches and assemblies) and as many targets as possible.[11] The Hellenic DPA (Decision 63/2004 and Decision 58/2005) has permitted CCTV use only for the primary purpose of traffic management and laid down very detailed conditions for this use and rejected the extension of the processing purposes.

The main argument of the DPA was that due to the multiple purposes to be fulfilled through such a system, it was not possible to assess the necessity, adequacy, relevance and proportionality of the processing (Hellenic Data Protection Authority, 2004). Moreover, a second critical parameter was that the installation and implementation of any extensive system that monitors public space preventively, permanently and systematically is not possible without the existence of a specific law which would regulate in detail the guarantees, terms and limitations of the relevant right. The general data protection law could not be considered as legal ground, as it lacked the criterion of speciality required also by the European Court of Human Rights as a condition for restrictions of the right to a private life (Katrougalos, 2011). On the other hand, the government contested the DPA's decisions, arguing that national security trumps the privacy of citizens, and took the issue to the Council of State, the country's highest administrative court, in order to annul that DPA decision.

There was an attempt to fill this vacuum in 2007, at first with the issue of an *ad hoc* dictum of the Public Prosecutor of the Hellenic Court of Cassation[12]. According to the Public Prosecutor, the recording by the police authorities of any illegal activity in public space is possible at all times, as it aims at the revelation of essential truth in penal trial and the punishment of crime, which constitutes a value of constitutional statute. Moreover, 'the protection of private and personal life is conceivable only while it is manifested through a legal activity, and not when it is manifested trough illegal behaviour and criminal acts' [*sic*]. This approach has led to an 'institutional' conflict between the Public Prosecutor and the Greek DPA (Anthopoulos, 2011).

In November 2007 the President and five members of the DPA resigned in protest against the government which prohibited the control of compliance with a DPA ruling during a public demonstration. However, the governmental plans seemed to be supported by the public opinion: in the aforementioned survey conducted in 2007 only one in three respondents had said that they felt CCTV systems intrude more than they protected, and only a quarter of the respondents said that the cameras installed in 2004 should be removed whereas 61 per cent said they should be used.

This approach was reinforced by an amendment of the Data Protection Law in 2007 (through Art. 8 of Law 3625/2007 amending article 3(2) section c of the Law 2472/1997), which excluded from the supervision of the DPA the personal data processing by the competent public authorities via CCTV for the purposes of state security, defence and public safety. This was a provision that has raised serious issues and concerns regarding its compliance with the constitutional right to (personal) data protection (Art. 9a of the Greek Constitution). The existence of an 'independent authority' is explicitly stated as an institutional guarantee of the right to data protection, which means that the legislator could not limit the DPA's powers to the point that it practically abolishes it (Mitrou, 2001).

This legislation, which acknowledged the legitimate use of cameras during public demonstrations and manifestations, has initiated the public and theoretical dialogue concerning public surveillance in Greece. Public debates and protests

were also fuelled by the provisions of the Law 3783/2009 (Art. 12 (1) that exempted from the scope of the national Data Protection Law 2472/1997, thus also from DPA supervision, all competent public authorities processing personal data via a closed-circuit television ('CCTV') system which had been installed in public spaces in Greece for the purposes of state security, defence and public safety.

Following the public controversy and taking into account the criticism and the concerns expressed, the government attempted (by Law 3917/11) to create a more specific legal ground for the use of the CCTV in public places. It defined terms and conditions for deployment of CCTV for the protection of state security, public safety and security, prevention of crime and law enforcement (national defence, protection of the democratic regime, prevention and prosecution of crimes related to a threat to public order, crimes concerning property, traffic control, drugs, etc.) by security and Law Enforcement Authorities. It also laid down 'proportionality' as the guiding principle.

However, the application of these rules depends on the issuing of a so-called Presidential Decree which, on the basis of a consultative, non-binding Opinion of the DPA, should specify all the 'details' regarding competent authorities, procedure, retention time etc., a decree that has not been issued yet. As far as it concerns video surveillance for all other purposes, the DPA issued in 2011 revised guidelines for the use of CCTV systems in publicly accessible places, that is allowed only for the protection of persons and goods. The guidelines define the substantial and procedural conditions (limits of equipment, time limitations, 'privacy zones', notification requirements) for this use to be lawful.

Privacy in public places and security

Despite the fact CCTV is becoming a part of everyday life, it interferes with personality, privacy and data protection rights that – as already mentioned – are embedded also in the Greek Constitution (in Articles 5, 9 and 9A) and the law. According to Greek legal theory and jurisprudence people enjoy also 'privacy in public'. Audio/image data are considered to be personal data, if they refer to identified or even identifiable persons. Both the DPA and courts have accepted that the operation of CCTV systems in public places violates the right to personality of the citizens because it 'puts them under control and unjustifiably restricts their freedom and hinders the free development of their participation in social and political activities.'[13] In particular, it is accepted both by theorists and jurisprudence that CCTV surveillance has the potential to discourage people from exercising their rights to freedom of expression and freedom of association in public places.

On the other side, security is, in general, regarded as a restriction to fundamental rights, despite the divergent views about its nature (Tsiftsoglou, 2011). However, a 'right to security', does not have a distinct, self-existent ground in the Greek Constitution. Additionally, it is interesting to underline that the DPA defines public safety as 'the obligation of the State to take the appropriate measures for the protection and the efficient exercise of civil rights.'[14] The concept of public safety as an obligation to protect rights is grounded on a generic clause of the Greek

Constitution, which introduces the positive obligation of the state and its agents to guarantee the rights of man as an individual and member of society and ensure the unhindered and efficient exercise thereof (Art. 25 (1), Sec. 1 of the Greek Constitution). Regardless of its conception either as the result of the demand on the state to undertake positive actions to protect the rights of life, personality, property or as a public good, security constitutes a limitation of freedom and privacy that is not allowed to affect their core.

A significant share of Greek scholars rejects the existence of a 'self-existent' right to security also because of the fear that such a right could be easily transformed into a 'hyper-right', which, countervailed against the right to privacy and data protection, would result to override them, eventually leading to drastic constraints on freedom. An acknowledgement of a right to security would constitute an additional, new, specific limitation of all rights, beyond and on top of the general limitation for non-infringement of the rights of others (Art. 5 (sec. 1) of the Greek Constitution) (Katrougalos, 2011). The 'invention' of a 'fundamental right to security' would do nothing to resolve the problems of security, but could be only used as an argument to justify ever wider powers of state intervention (Denninger, 2002).

Historical context and privacy perceptions and preferences: vigilance against the state surveillance and institutional distrust

It is difficult to define a dominant perception of privacy and its threats as well as the respective preferences, as Greeks are sensitive to and vigilant against any state monitoring. Until the second half of the 1970s, when democracy was re-established in Greece, modern Greek political and social history was marked by a culture of suspicion and discrimination. The wide use of traditional surveillance mechanisms had far reaching impacts even on citizenship status: the so-called 'Civic- mindedness certificates', based on police records about political convictions of entire families, were officially required until 1974 for any Greek who wanted to work in the public sector, professional permit, passport, driving licence or even access to university education (Samatas, 2014).

Greek citizens, after the Second World War and especially during the Civil War (1946–1949) and the military dictatorship (from 1967 until 1974), experienced some of the most direct and repressive forms of state surveillance (Alivizatos, 1981). They were afraid of any state and police filing,[15] which could potentially classify them and their family in police records, and exclude them from access to public benefits or to face other forms of discrimination or even sanctions. Samatas (2014) argues that especially for the older generation which had experienced the authoritarian political control surveillance, the problem is not watching i.e., the 'real-time monitoring', but the storage of personal data, what the Greeks describe as 'fakeloma' (filing). This is a tendency that can explain the results of the PACT survey which shows that respondents who agree with the statements 'Often security is used as an excuse to impose stricter surveillance and control over the population' and 'Increasing surveillance increases the risk of discrimination' indicate disinclination towards the presence of CCTV cameras (Patil *et al.*, 2015).

Authoritarianism has probably left its mark on the distrustful relations between citizens and state institutions (Sotiropoulos, 2004). In the case of Greece, surveillance seems to have permeated the relationships between the state and its citizens well beyond the end of repressive regimes (Marx, 2014). Due to these historic experiences many Greek citizens have adopted a general 'negative surveillance culture' (Samatas, 2004)**.** In Greece there is a popular mistrust and demonization of personal data collection and processing even for legitimate and generally acceptable purposes, such as public safety, taxation or traffic control. It is remarkable that any attempt of the government to organize a new register (nowadays mostly for taxes or public expenses control) is negatively presented or delegitimized in advance by the media as 'new electronic filing'.

Respondents' attitudes significantly affect their preferences in relation to privacy, security and surveillance. Levels of distrust and trust in public institutions have been identified as relevant parameters with regard to privacy preferences. The correlation between distrust of institutions, attitudes and privacy preferences is documented also in Special Eurobarometer 359 (2011): the country standing out because of the lowest trust levels in all institutions and companies is Greece. In this Eurobarometer survey the Greek population appeared to have the lowest level of trust in most institutions and the highest levels of concerns in most examined categories.

As noted, the majority of respondents in all EU Member States trust certain national public authorities, such as tax authorities and social security authorities. The relevant percentage figures are smallest in Greece (52 per cent), followed by Poland and Romania (both 61 per cent). Also, in the Flash Eurobarometer 225 survey on Data Protection in the European Union, conducted in 2008 (European Commission, 2008), Greece was situated more often than any other country at the lower end of the scale with regard to trust in organizations. Greek respondents were the most likely to argue that personal data protection was low in Greece (71 per cent), although *Greece* had the highest levels of recognition (51 per cent) of the DPA. In general, Greeks accorded relatively little legitimacy to the performance of the parliament, government and the legal system (Katsimi *et al.*, 2013).

As noted by van den Broek *et al*, trust in institutions plays a relevant role, and trust in public institutions correlates positively with acceptance of privacy intrusive measures (van den Broek *et al.*, 2016). In general, the more distrustful (towards business, government and technology) a respondent is, the greater their concern for privacy (Patil *et al.*, 2015). However, we should note that the highest proportion of respondents to the PACT survey with 'high institutional distrust' was not observed in Greece, but in Italy, Spain and France (Patil *et al.*, 2015).

Tolerance towards private videosurveillance and 'function creep'

At the same time, social analysis, surveys and media reports confirm a 'Greek surveillance paradox': while there is mistrust towards even legitimate 'institutional surveillance', which however presupposes trust in the state and public institutions (Lianos, 2003)*,* Greeks are generally less concerned with non-state, private video

surveillance and data collection,[16] although several surveys have also shown that – compared to other European countries – in Greece there is comparatively low interpersonal trust. Greeks on the average do not trust most other people (Katsimi *et al.*, 2013).

As already noted there is a significant increase in the number of CCTV systems operating in Greece, especially by private persons and organizations. People tend to ignore or disregard other forms of non-state surveillance (Samatas, 2013); they seem to tolerate the ever growing use of CCTV systems in banks, hotels, and shopping centres. CCTV use by private organizations becomes 'unremarkable, mundane, normal and consequently may not even be challenged' (Murakami Wood and Webster, 2009). They react to the use of CCTV systems only in cases that they feel directly affected in their privacy or in relation to their right (to personality) in the workplace. It is interesting to note that the majority of the (relatively few) citizens' complaints that the Greek DPA has to deal with, refer to the use of CCTV or web cams in restaurants or by neighbours: people defend their freedom from (optical) interference in their private sphere despite the fact that CCTV monitoring does not take place in private space. At the same time 20 per cent of complaints about the use of CCTV relate to the use of such systems in work environments.[17]

There is a particular attitude which is to be understood in the light of 'privacy paradox'. Individuals who consider privacy as an important value, under other conditions, are known to easily surrender personal data (potentially giving away their privacy) in exchange for some (usually relatively minor) benefit (Grossklags and Acquisti, 2007). Greeks are concerned with the use of CCTV or their tracking via mobile telephone or Internet,[18] yet in both the PACT survey (on Choice of ISPs) and the Eurobarometer survey (2011), there is no major divergence between Greeks and respondents from other EU countries with regard to their concerns about their behaviour being recorded through the Internet when browsing, downloading files, and accessing content online. These results indicate also the significance of context on attitudes and preferences: Potoglou *et al.* (2014) underline that the differentiated findings reflect the nuances in *the* analysis between privacy in a context characterized by physicality, for instance, the travel context, and privacy understood as personal information, as illustrated in the Internet and health care system contexts.

Collecting and aggregation of information by private organizations 'fits well into a society where most things are marketable' (Marx, 2014) and people are inclined to expose their life and activities to social media and leave data traces by every electronic interaction. Moreover, we should not ignore the driving force of technology. Institutional values and principles do acquire and foster their content also through the opinions and expectations which are formulated and formed in society. The availability of innovation products and the promises of technological progress and goods for the well-being of individuals may slightly, but definitely, influence or even change their position on certain core fundamental values and consequently the interpretation thereof. The wide availability of (low cost) CCTV or biometric/face recognition systems, and respectively their increasing use also in

the private sector and by private citizens, change slightly but steadily the social perception of what is acceptable or excessive in relation to security measures.

Another factor that influences the perception of CCTV monitoring conducted by private entities is the degree of awareness and understanding of the legal framework. It seems that most people are unaware, ignore or do not realize that information gained through privately deployed CCTV systems is increasingly placed at the disposal of the state, which tends to result in 'function creep' (Lyon, 2001). This involves systematic (and not only occasional) data sharing between the public and the private sector, such as in the case of communications data retention. The use of material captured by private cameras for law enforcement purposes is quite often reported in the media. However, such reports do not cause any reactions, as such a use seems to be acceptable as it serves the detection of mostly serious crimes (Samatas, 2014).

The technique of folding private organizations into a government's surveillance network creates a system of 'distributed surveillance', allowing the state to overcome the practical limits on its resources (Stanley, 2004). The state's ability to access and assess such vast amounts of data, which was initially collected by private entities entirely for other purposes, constitutes a threat to informational self-determination, which can potentially chill not only political participation but also professional and personal activities (Mitrou, 2010).

The 'Greek crisis' and the trade-off of security and privacy: some concluding remarks

Attitudes are clearly influenced by the interrelation between distrust and privacy concerns, demographic and socio-economic characteristics, such as age, gender and income as well as by general socio-economic factors. With regard to Greece, there are no specific surveys illuminating the impact of economic crisis and its sequential results (unemployment, poverty, lack of cohesion) on perceptions of privacy and data protection as well as on the relation between security and privacy and the people's preferences.

However it is clear that the Greek crisis has far reaching impacts on the level of data protection. The urgency that the crisis creates and the fear of unintended consequences as well as the need to fight corruption and tax evasion have generated the necessary political legitimacy for extending and intensifying the state's ubiquitous surveillance (Tsapogas, 2016), characterized by Samatas as 'austerity surveillance' (Samatas, 2015). In the meantime, lack of confidence in the efficiency and accountability of the state institutions remains high (Samatas, 2015). At the same time, it seems that the regulatory content of core legal principles, such as the principle of proportionality is slightly but clearly changing: taking also 'into consideration the need to prevent terrorist attacks' the Hellenic DPA has approved in November 2015 the (initially rejected as not sufficiently justified) application of the Athens Metro Company to install security cameras inside the trains.

In parallel, public fears about property and violent crime appear to have risen dramatically during this period: public concern about crime has more than

doubled in Greece between 2008 and 2009 (European Commission, 2008; European Commission, 2009). Such fears are also related to concerns about illegal immigration and political violence. Fears have been fuelled also by media reports and crime statistics that have shown a significant growth in thefts, burglaries and robberies over this time span (Xenakis and Cheliotis, 2013), although crime rates or criminal incidents *alone* are not necessarily a good indicator of public fears and concerns or of the quality and experience people have with their community safety (Squires, 2010).

Especially in an environment of economic and social crisis, when uncertainty is rising on multiple levels, the prevention and removal of risks has become a social and political expectation. In such a context of 'stage-set security' (Murakami Wood and Webster, 2009) the presence of CCTV is a symbol of surveillance and state security but also of 'safety'[19] in a society in which almost everything is seen as a potential source of risk and where insecurity dominates. Tolerance and/or acceptance of CCTV mirror risk perceptions and fears and the sense that 'somebody has to look after you'.

In this context the PACT survey results indicate that respondents' preferences relating to security and privacy are much more nuanced than the simplistic inverse relationship between security and privacy that is often assumed (Patil *et al.*, 2015). If Greeks are against the storing of captured data and 'filing', they do not reject real-time monitoring at stations and on public transport. Despite the historically embedded mistrust in the state and the dissimilarities with regard to the preferences expressed by respondents in other countries, the 'Greek paradox' demonstrates in our opinion that the citizens 'simply want both' (van den Broek *et al.*, 2016). They consider both security and privacy as relevant and not mutually excluded. What is expected from regulating authorities is to strike a fair balance and guarantee, by organizational measures such as deletion of data, such a balance between the need for effective security measures and the need to ensure civil liberties.

Notes

1   According to Hellenic DPA Guidelines (Hellenic Data Protection Autority, 2000) and (Hellenic Data Protection Authority, 2011), the deployment of CCTV and the respective data processing have to be notified by the data controller to the DPA. It is significant that notifications of CCTV systems to the Greek DPA in 2005 (105) represent an annual increase of 75 per cent in comparison to 2004 (60), while the number of notifications in 2008 (477) amounted to an increase of approximately 800 per cent. Between 2007 and 2014 more than 350 CCTV deployments have been notified yearly (DPA Annual Report, 2014, p. 38).

2   By 2009, Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, the Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland and UK introduced CCTV systems operating in public space for the purposes of crime prevention (Norris, 2011).

3   N. Alivizatos, (16 December 2007) 'Human Rights in Danger: The Hidden Side of the CCTV Regulation', *Ta Nea* [in Greek]. Also E. Simeonidou-Kastanidou (11 December 2007), 'Cameras in Public Assemblies', *Ta Nea* [in Greek]. Retrieved 11 November 11, 2009, at http://digital.tanea.gr/Default.

4   See the remarks of Fonio with regard to CCTV in Italy (Fonio, 2011).
5   PACT – 'Public Perception of Security and Privacy: Assessing Knowledge; Collecting Evidence, Translating Research into Action', is a Seventh European Framework Programme project that investigated the security and privacy issues in detail. PACT was a three-year project (2012–2015) aimed at understanding the public perception of security and privacy across 27 European Member States. For more information, see www.projectpact.eu.
6   PRISMS – 'Privacy and Security Mirrors' is a Seventh European Framework Programme project that analysed the traditional trade-off model between privacy and security and worked towards a more evidence-based perspective for reconciling privacy and security, trust and concern. PRISMS was a three year project (2012–2015) aiming to provide users with a decision support system that provides them with an insight into the pros and cons of specific security investments compared to a set of alternatives, taking into account a wider societal context. For more information, see http://prismsproject.eu.
7   Special Eurobarometer 359 concerned attitudes on data protection and electronic identity in the European Union and it was conducted by TNS Opinion and Social at the request of Justice, Information Society and Media Joint Research Centre. 26,574 Europeans aged 15 and over were interviewed by the TNS Opinion and Social network. All interviews were conducted face-to-face in people's homes and in the appropriate national languages.
8   The findings of the survey conducted by Public Issue and an analysis thereof have been presented in the newspaper 'Kathimerini' (21 January 2007). Also accessible at www.publicissue.gr/553/cameras/.
9   About the legal provisions and guidelines of the Hellenic DPA on videosurveillance systems see www.dpa.gr/.
10   In fact, the Athens 2004 Olympic 'superpanopticon' was prescribed to include a large-scale surveillance integration security network composed of 29 subsystems integrated into a unified command and control system linking the Greek police, fire-fighters, the Greek coast guard, and the Greek armed forces through 130 fixed and five mobile command centers. It was also to include a surveillance blimp above Athens, underwater sensors guarding Piraeus harbor, hundreds of closed-circuit television (CCTV) cameras, vehicle tracking devices and motion detectors (Samatas, 2007).
11   The academic community, the heads of all Greek lawyers' associations, human rights NGOs, and several mayors have vigorously protested against the perpetuating operation of the Olympic cameras after the games (Samatas, 2008).
12   The text is available in Greek at the Supreme Court's Public Prosecution Office website www.dpa.gr/.
13   Court of the First Instance of Patras Judgment 2765/2005.
14   Hellenic DPA Opinion 1/2009 on use of CCTV systems in public places and Opinion 2/2010 on use of CCTV systems by public authorities and individuals.
15   Discourses and attitudes are shaped by historical and political historical experiences also in other states like Germany where due to the totalitarian Nazi regime of Adolf Hitler there has been a public mistrust of the state's power to surveil its citizens (Norris, 2012) (Hempel and Töpfer, 2004).
16   (van den Broek et al., 2016) point out as third conclusion of PRISMS survey that the type of actor (whether from the public or private sector) which collects and processes personal data is relevant: vignettes of public sector actors receive higher levels of acceptance than vignettes of private sector actors.
17   Greek DPA Annual Report (2011, p. 108ff.), Annual Report (2012, p. 100 ff.), Annual Report (2013, p. 108 ff.), Annual Report (2014, p. 99ff.) (in Greek). References in the text are based also on a discussion with the Head of the Auditors' Department of the DPA.

18 A majority of respondents in 15 Member States led by Greece (65 per cent) say they are concerned about being tracked via mobile phone or mobile (Internet European Commission, Special Eurobarometer 2011, p. 66).
19 It is noteworthy that despite the richness of the Greek language there is only one word ('*asfaleia : without fault*") that indicates both security and safety.

References

Alivizatos, N. (1981) 'The Emergency Regime and Civil Liberties', in J. Iatrides, ed. *Greece in the 1940s. A Nation in Crisis*, Hanover, NH: University Press of New England, 219–228.

Amicelle, A., Bus, J., El-Baba, T., Fuchs, C., Mordini, E., Rebera, A., Robinson, N., Trottier, D., Venier, S., and Wright, S. (2012) *Report on Theoretical Frameworks and Previous Empirical Research*, PACT Project – Deliverable D.1.1.

Anthopoulos, H. (2011) 'The Electronic Surveillance of Public Assemblies: Political Privacy and Public Anonymity in Greece', in A. Akrivopoulou and A. Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practice*, Hershey, NY: IGI Global, 59–69.

van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M. and Rung, S. (2016) 'Privacy and Security – Citizens' Desires for an Equal Footing', in M. Friedewald, J.P. Burgess, J. Čas, R. Bellanova and W. Peissl (eds), *Surveillance, Privacy and Security: Citizens' Perspectives*, Abingdon: Routledge.

Budak, J., Rajh, E. and Recher, R. (2016) 'Citizens' Privacy Concerns: Does National Culture Matter?', in M. Friedewald, J. Čas, R. Bellanova, and W. Peissl (eds), *Surveillance, Privacy and Security: Citizens' Perspectives*, Abingdon: Routledge.

Denninger, E. (2002) 'Freiheit durch Sicherheit? Wie viel Schutz der inneren Sicherheit verlangt und verträgt das deutsche Grundgesetz?', *Kritische Justiz*, 35: 467–475.

European Commission (2008) *Data Protection in the European Union: Citizens' perceptions*, Flash Eurobarometer 225, Brussels: European Commission.

European Commission (2008) *Eurobarometer 69*, Brussels: European Commission.

European Commission (2009) *Eurobarometer 71*, Brussels: European Commission.

European Commission (2011) *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 225, Brussels: European Commission.

Fonio, C. (2011) 'The Silent Growth of Video Surveillance in Italy', *Information Polity – Special issue on Part 1: Revisiting the Surveillance Camera Revolution: Issues of Governance and Public Policy*, 16(4): 379–388.

Grossklags, J. and Acquisti, A. (2007) 'When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information', *Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA*. Available at: www.econinfosec.org/archive/weis2007/papers/66.pdf (accessed 14 November 2016).

Hellenic Data Protection Autority (2000) *Directive on the Use of Video Surveillance Systems* [in Greek], Athens: Hellenic Data Protection Authority.

Hellenic Data Protection Authority (2004) *Decision No. 63/2004* [in Greek], Athens: Hellenic Data Protection Authority.

Hellenic Data Protection Authority (2005) *Decision No. 58.2005* [in Greek], Athens: Hellenic Data Protection Authority.

Hellenic Data Protection Authority (2011) *Directive on the Use of Video Surveillance Systems to Protect Persons and Goods* [in Greek], Athens: Hellenic Data Protection Authority.

Hempel, L. and Töpfer, E. (2004) *CCTV in Europe*, Technical University Berlin. Available at: www.urbaneye.net/results/ue_wp15.pdf (accessed 18 January 2016).

Katrougalos, G. (2011) 'IT and the Tension between Privacy and Security: The Case of Surveillance of the Public Sphere', *US-China Law Review*, 8(1): 579–596.

Katsimi, M., Moutos, T., Pagoulatos, G. and Sotiropoulos, D.A. (2013) *GINI Country Report: Growing Inequalities and their Impacts in Greece*, Amsterdam: Amsterdam Institute for Advanced Labour Studies (AIAS).

Lianos, M. (2003) 'Social Control after Foucault', *Surveillance & Society*, 1(3): 412–430. Available at: www.surveillance-and-society.org/articles1%283%29/AfterFoucault.pdf (accessed 22 March 2016).

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life (Issues in Society)*, Milton Keynes: Open University Press.

Marx, G. (2014) 'Conceptual Matters – The Ordering of Surveillance', in K. Boersma, R. van Brakel, C. Fonio and P. Wagenaar (eds), *Histories of Surveillance in Europe and Beyond*, Abingdon: Routledge, 221–227.

Mitrou, L. (2001) 'The Right to Data Protection: A New Right?', in D. Tsatsos, E. Venizelos and X. Contiades (eds), *The New Constitution: Proceedings of the Conference on the Revised Greek Constitution of 1975/1986/2001*, Athens: Sakkoulas, 83–103.

Mitrou, L. (2010) 'The Impact of Communications Data Retention on Fundamental Rights and Democracy: The Case of the EU Data Retention Directive', *Surveillance and Democracy*, 127–147.

Murakami Wood, D. and Webster, C. W. R. (2009) 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example', *Journal of Contemporary Research*, 5(2): 259–173.

Norris, C. (2011) 'There's No Success like Failure and Failure's No Success at All: Some Critical Reflections on Understanding the Global Growth of CCTV surveillance', in A. Doyle, R. Lippert and D. Lyon (eds), *Eyes Everywhere – The Global Growth of Camera Surveillance*, Abingdon: Routledge.

Norris, C. (2012) 'The Success of Failure – Accounting for the Global Growth of CCTV', in K. Ball, K.D. Haggerty and D. Lyon (eds), *Routledge Handbook of Surveillance Studies*, Abingdon: Routledge.

Panousis, Y. (2010) 'Camera-phobia and Camera-worship. Democratic Insecurity?', in *Aspects of New Surveillance. International and Greek*, Athens: Vivliorama, 211–331.

Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D. and Robinson, N. (2015) *Public Perception of Security and Privacy: Results of the Comprehensive Analysis of PACT's pan-European Survey*, Cambridge: RAND Corporation.

Potoglou, D., Robinson, N., Patil, S., Dunkerley, F., Fox, J., Lu, H. and Patruni, B. (2014) 'Privacy, Security and Surveillance: New Insights into Preferences of European Citizens', in *The 42nd Research Conference on Communication, Information and Internet Policy*, Arlington, TX. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418346 (accessed 14 November 2016).

Samatas, M. (2004) *Surveillance in Greece: From Anticommunist to Consumer Surveillance*, New York: Pella Publishing Company.

Samatas, M. (2007) 'Security and Surveillance in the Athens 2004 Olympics: Some Lessons From a Troubled Story', *International Criminal Justice Review*, 17(3): 220–238.

Samatas, M. (2008) 'From Thought Control to Traffic Control: CCTV Politics of Expansion and Resistance in post-Olympics Greece', *Surveillance and Governance: Crime Control and Beyond*, 10(1): 345–369.

Samatas, M. (2013) Online survey, 'Reservations, Considerations and Scientific Conclusions

on the Students' opinions of the University of Crete', in M. Bottis (ed.), *Privacy and Surveillance: Current Aspects and Future Perspectives*, Athens: Nomiki Bibliothiki, 257–259.

Samatas, M. (2014) 'A Brief History of the Anticommunist Surveillance in Greece and Its Lasting Impact', in K. Boersma, R. Van Brakel, C. Fonio and P. Wagenaar (eds), *Histories of Surveillance in Europe and Beyond*, Abingdon: Routledge, 49–63.

Samatas, M. (2015) 'Austerity Surveillance', in Greece under the Austerity Regime (2010−2014), *Media and Communication*, 3(3): 68–80.

Sotiropoulos, D. (2004) *Democratization, Administrative Reform and the State in Greece, Italy, Portugal and Spain: Is There a 'model' of South European Bureaucracy?,* London: London School of Economics and Political Science.

Squires, P. (2010) *Evaluating CCTV: Lessons from a Surveillance Culture,* Rotterdam: European Forum for Urban Security.

Stanley, J. (2004) *How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*, New York: American Civil Liberties Union.

Tsapogas, D. (2016) 'The Importance of the Sociopolitical Context and Ideology in Explaining Citizens' Attitudes towards Digital Surveillance and Citizenship', in M. Friedewald, J.P. Burgess, J. Čas, R. Bellanova and W. Peissl (eds), *Surveillance, Privacy and Security: Citizens' Perspectives*, Abingdon: Routledge.

Tsiftsoglou, A. (2011) 'Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy', in C. Akrivopoulou and A. Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, Hershey, PA: IGI Global, 93–102.

Webster, W., Töpfer, E. and Klauser, F.R.C. (2011) 'Revisiting the Surveillance Camera Revolution: Issues of Governance and Public Policy. Introduction to Part 1 of the Special Issue', *Information Polity*, 15(1): 297–301.

Xenakis, S. and Cheliotis, L.K. (2013) 'Crime and Economic Downturn: The Complexity of Crime and Crime Politics in Greece since 2009', *British Journal of Criminology*, 53(5): 719–745.

8 Urban security production between the citizen and the state

Matthias Leese and Peter Bescherer

> Urban security presents equally difficult challenges for both security studies and policymakers, since it crosses divides between existing disciplinary boundaries, political institutions and jurisdictions.
>
> (Abrahamsen *et al.*, 2009: 364)

> The problems that a city faces are so manifold, you can't solve them in a singular fashion.[1]
>
> (Interview, 6 January 2015)

Cities are dense spaces where societal friction can be experienced in an unmediated fashion, and urban politics can serve as a powerful magnifying glass for questions of security politics and security practices. Cities have indeed long been conceptualized as epitomes for programs of surveillance and governance through data, for the privatization and hybridization of policing, and for the roll-out of new technologies (e.g., Graham, 2006; Abrahamsen *et al.*, 2009; Coward, 2009; Kitchin *et al.*, 2015), thereby framing the urban as a prime arena for questions of contemporary government. Cities are being monitored by CCTV cameras and sensors, "smart" grids regulate street lighting, and predictive policing algorithms indicate where to dispatch patrol cars. In short: the relation between privacy and security converges in the urban, as the search for data-fueled insights into the social fabric of the city continues and thus potentially keeps uprooting traditional imaginaries of privacy. While scholars have increasingly focused on data-driven modes of governance, particularly with regard to the production of security, we seek to address the fragile constellation of *privacy vs/and/or security* through a focus on urban (in-)securities and the political and social struggles that they entail.

The relation between privacy and security is an ambiguous and unstable one that refuses to be put into clear-cut categories (e.g., Amoore, 2014; de Goede, 2014; Jeandesboz *et al.*, 2012; Leese, 2015; Bellanova, 2014). As both privacy and security are notions that need to be filled with meaning through context and practices, such "moving targets" (Friedewald *et al.*, 2010: 61) are hard to pin down in an abstract fashion. Put differently: in order to make sense of privacy vs/and/or security, empirical research is needed. Concentrating on the security part of the relation between privacy and security, we seek to contribute to an understanding of what

is at stake when it comes to the production of security throughout the urban. We thereby illustrate that (in-)security cannot be easily defined, as it shifts both meaning and means throughout the manifold perspectives that we encounter in the city. Building on 16.5 hours of qualitative interview material with stakeholders from the field of urban security (e.g., police, municipalities, civic organizations) that was collected within the research project VERSS,[2] we empirically retrace contemporary modes of security production and aim to map complex constellations of security *problems*, security *actors*, and security *solutions*.

Special attention is given to modes of (non-)cooperation between public security agencies and civic organizations. We thus address questions such as: Who should have a say, and who should be entitled to take action, in rendering cities secure? Based on which political programs or assessments? To which extent do civic organizations exist dependent or independent of political incentives? And to which extent do they resist and counter; or support and foster urban security politics? In the vein of ongoing political struggle, more recently there have been calls for a re-appropriation of urban space that largely build on the "Right to the City" works of Henri Lefebvre (e.g., Lefebvre, 1996; Dikeç, 2002; Harvey, 2008; Marcuse, 2009; Butler, 2012; Revol, 2014). Among others, such calls have put forward the need to include citizens in security policy-making and security production (Connolly and Steil, 2009), thus opening up a research agenda at the intersections of policing, civic engagement, and securitization. Participatory accounts of urban politics are said to incorporate multiple advantages: (1) the scale of the city is large enough to provide meaningful governmental power, but still small enough to enable participatory impacts; (2) participatory programs foster political legitimacy; and (3) policy makers can incorporate citizens' needs to match political programs and requirements, thus leading to improved efficacy and reduced costs. Against such an affirmative reading, we call to carefully consider concrete contexts of (in-)securities. Citizens' perceptions of insecurity must not necessarily be congruent with experts' assessments, thus requiring us to think about the premises of policy-making and mechanisms of democratic representation more generally – and about how to think about security vis-à-vis privacy more specifically.

Urban (in-)securities

Attempts to pinpoint the relationship between (in-)security and the urban have been manifold – be it that "the city represents the hazardous threshold of crisis, the vulnerable cradle of humanity's future" (Bishop and Phillips, 2013: 222); that "we increasingly live in divided and conflict-prone urban areas" (Harvey, 2008: 32); or that "urban areas are not only the site of extraordinary growth: they are also the locus of intense violence and physical insecurity" (Abrahamsen *et al.*, 2009: 363). However, a common theme that unites most commentators is the emphasis on the urban as a catalyst for all sorts of friction and conflict. On the one hand, this appears to be rather obvious, as of today the majority of the global population in fact lives in cities. The ensuing increase in population density alone is likely to bring incommensurable ideas of lifestyle to the fore. Or, as Butler (2012: 143–144) claims, "the

urban operates as a space of encounter – simultaneously encouraging differences to flourish, but also generating possibilities for collective action through processes of spatial production."

On the other hand, as Abrahamsen *et al*. (2009: 364) note in their introduction to a *Security Dialogue* special issue on urban security, scholars have also highlighted that "the city is an awkward object for analysis." This is due to the fact that there is no such thing as *the* city. Urban infrastructures are not only dynamic and contingent, but also highly dependent on historical, geographical, cultural, economic and spatial contexts that contribute to their constant re-assemblage – as spaces of living and dwelling, but also as objects of government and as arenas where social questions are regularly (re-)negotiated. And yet, as Graham (2004: 3) notes, "it is no longer adequate to theorize cities as local, bounded sites that are separated off from the rest of the world," as particularly international and homeland security politics extend deeply into urban spaces (Marcuse, 2006). Increasingly, "the design of buildings, the management of traffic, the physical planning of cities, migration policy, or the design of social policies for ethnically diverse cities and neighborhoods, are being brought within the widening umbrella of 'national security'" (Graham, 2004: 11), thus arguably catalyzing already existing tensions. A normatively charged perspective on contemporary urbanity might ask: "has the astonishing pace and scale of urbanization over the last hundred years contributed to human well-being?" (Harvey, 2008: 23). Critical commentators would undoubtedly deny that. In fact, recent protest movements and calls for citizen empowerment have been sparked by a perceived neglect of social justice in urban politics. We will further explore those questions and their implications for urban security in the ensuing section.

On an abstract level, security is ontologically characterized by the absence of its materiality – in other words: there is no manifest *in*security as long as no threat materializes. And yet the threats that could possibly bring about such insecurity are always already present in political programs as well as in our imaginations. This means that security is awkwardly stuck in a virtual realm that must never transcend into the real world, or otherwise security politics and security practices would have failed (Massumi, 2007). This logic often leaves threats and fears, quantifications and perceptions as the basis for political action, and "urban governments have become increasingly involved in developing policies to improve the security perception of their inhabitants" (van den Berg *et al.*, 2006: 21). Critical security scholars have in this vein pointed out that insecurity might not always be a problem that government needs to address, but also a powerful instrument *through* which populations can be governed, thereby upholding a level of unease in order to justify political action (Bigo, 2002). As van den Berg *et al.* (2006: 10) frame the problematic of this security paradox with regard to the city: "though gates, policing and surveillance systems, defensive architecture, and neo-traditional urbanism do contribute towards giving people a greater sense of security, they also contribute to accentuating fear by increasing paranoia and distrust among people."

More empirically, the production of security (and particularly the policing of urban space) has become increasingly detached from a presupposed primacy of the

state. There are widespread trends of outsourcing, privatization, or contracting the production of security in multiple ways that are empowered through (neo-)liberal logics and ensuing marketization (Ericson and Haggerty, 1997; Garland, 2001). This has in fact led to new modes of citizen responsiblization that are arguably fostered by political programs that call for active involvement of the population, as "citizen participation must be universally promoted and civil society must play a role at all stages of the policy-making process, from conception, to implementation, to evaluation" (European Forum for Urban Security, 2012: 7). Framed differently: it now appears that citizens are to blame themselves for any state of insecurity that they find themselves in. Along such lines, new forms of citizen or community policing, the incorporation of non-profit organizations, and the contracting of police tasks to private service providers have become rather common (e.g., Eick, 2003; Eick and Briken, 2014; Abt *et al.*, 2014).

   Cities are multi-faceted spaces that are subjected to manifold political, social, and economic transformations. In a sense, the urban thus becomes a site of frictions that must not neatly be put into theoretical categories, but that call for ongoing empirical research to capture their dynamics. If, as Abrahamsen *et al.* (2009: 364–365) note, "cities, perhaps more than most objects of social analysis, tend to generate extremes or (perhaps more pejoratively) to attract hyperbole and gather clichés, and a suitably skeptical eye is needed whenever their insecurity is invoked," then this eye must indeed look at the particular practices that empower, enact, or resist urban government. In this chapter, we look at the specific modes of security 'production' along the continuum between designated public bodies (i.e., the police and municipal authorities) and the population by empirically engaging their modes of cooperation and/or conflict. Before turning to the empirical analysis, the ensuing section will sketch out the social and economic contexts that have more recently painted a rather bleak backdrop, and have sparked citizen involvement throughout the urban.

Neoliberal crises and the re-appropriation of the urban

As Hobsbawm (1973: 221) has pointed out more than 40 years ago, cities are more likely to become a site of riots if they feature a streetcar system, "partly because the raising of fares is a very natural precipitant of trouble, partly because these vehicles, when burned and overturned, can block streets and disrupt traffic very easily." The urban indeed provides a rather unmediated space for multiple forms of political contestation. In this vein, Mayer (2008, 2011) identifies four historical stages of (Western) urban social movements – starting with the crisis of Fordist societies in the late 1960s and the ensuing mass protests against large-scale refurbishment and functional division of urban areas. Protesters back then called for improved infrastructure, enhanced participation in urban planning processes, and more fundamentally for societal change. Activists not only engaged in alternative forms of urban life and communal services, but also sought to bring about political change through the foundation of new parties. Following this first stage, roll-back and roll-out forms of neoliberalism characterize the second and third stage in the

1980s and 1990s. In the wake of welfare cutbacks, urban movements changed in composition and put existential needs such as housing and employment high on the agenda. At the same time, local governments began to recognize the 'creative potential' of grass-root projects and thus started to support citizen initiatives – as long as they would stay within the boundaries of austerity politics and not stir social unrest. Notably, radical groups unwilling to "collaborate," as well as middle-class movements remained outside this new liaison between the state and its citizens, thus making for a fragmentation of civic involvement.

Already existing tensions intensified during the 1990s, when municipalities implemented new strategies for innovation, economic growth, and decentralized governance. City centers were increasingly restructured in order to attract businesses and consumers, while marginalized districts became sites of reintegration politics (e.g., 'Soziale Stadt' in Germany; 'Neighbourhood Renewal Fund' in the UK; 'Politique de la ville' in France), thereby unintentionally further fostering the independence and non-cooperation of certain forms of civic involvement, most notably initiatives by/for the poor and anti-racism organizations. Since the beginning of the 2000s, urbanization has become closely entangled with the booms and bubbles of international markets and finance. Empowered by new – yet risky – financial tools (most notably subprime mortgages), large-scale urban projects were to "absorb the surpluses that capitalism must produce if it was to survive" (Harvey, 2012: 11). The imperatives of short-term profit maximization thereby contributed directly to population polarization and a rise in social inequality (Harvey, 2012: 15). Today, middle classes are shrinking, while the percentage of low-income as well as high-income earners in urban regions rises (Gornig and Goebel, 2013: 64) – and so does the average rental rate and the number of homeless people (Holm, 2014: 15–20). Subsequently, the fragmentation of urban movement has continued, with new coalitions emerging for instance between trade unions, churches, precarious workers, and the anti-globalization movement. At the same time participatory mechanisms have become part of the inventory of urban politics, rendering the occurrence of radical counter-cultures less likely.

With the financial crisis of 2008 at the latest, austerity politics have arrived at the municipal level (Préceteille, 2013: 36). As a "side effect" of this development, civic initiatives, and particularly Right to the City movements, benefited in their struggle against social injustice. Following Lefebvre, the Right to the City is not limited to a legal claim with regard to participation in the *existing* urban configuration, but should rather be seen as a right in the sense of a moral claim that must be *created* through the appropriation of urban space in the first place (Mayer, 2011: 62), thereby engaging in communication, cooperation and confrontation. The Right to the City is conceptualized as a right for the marginalized, for those who are discriminated against, and against the backdrop of recent crises, also for the increasingly affected middle classes. In this vein, it must necessarily challenge existing power relations and is thus bound to clash with many of the participatory mechanisms that are offered by local government. The underlying rationale of such programs is arguably driven by an idealistic notion of well-integrated and harmonic city life, thus fostering a peculiar vision of a "postpolitical city"

(Swyngedouw, 2009). As mentioned earlier, similar tendencies can be witnessed when it comes to urban security. The remainder of this chapter thus empirically engages modes of urban security production between the citizen and the state.

Urban security production

Having sketched out the manifold social, political and economic frictions that run throughout the urban, it has become clear that cities must be analyzed as "places where communities are formed, thus developing protean systems of value and practice, and locations of social unrest, of contested space, where tensions between opposing groups flare up as they fight them out" (Bishop and Phillips, 2014: 128). In other words, urban (security) governance is a delicate task that needs to balance multiple stakes and actors. In the words of Wakefield and Braun (2014: 4), "running through each design, plan, or experiment is not just the same presupposition – that cities are integrated and extended socioecological networks – but also the same problem: how to govern this totality?" And keep in mind that such totality is increasingly characterized by the effects of economic crises, resulting in budget cutbacks not only for security agencies, but also for public institutions. Said one interviewee from a squatting initiative: "We have a local austerity policy, which had, even before the European level was brought into it, dramatic consequences for the city. With regard to cultural life, with regard to public swimming pools that are shut down, admission fees to the zoo, acquisitions for the library, closure of municipal service points" (Interview, 6 January 2015). Depending on the budget situation of the municipality, such austerity in turn creates a backdrop of reinforced neoliberal efforts to re-arrange governance and public service provision through market mechanisms of outsourcing and contracting, most notably also leading to enhanced citizen incorporation in policing and crime prevention (Eick and Briken, 2014) – thus ironically trying to counter economic crisis by means of the same toolbox that caused it in the first place.

In order to conceptually clarify the multiple and blurred stakes of urban security, we shall provide an empirically informed perspective that maps (1) how security problems present themselves, (2) which actors are entitled, competent, and/or willing to solve them, and (3) how such problems are envisioned to be solved.

Security problems

There is crime, of course, and there is violence. There are those many breaches of the law that concern citizens' bodily integrity and personal belongings in an unmediated fashion. But apart from such obvious security problems, many of the security issues that we encountered during field research evolved around the notion of public space – its purpose, its use, and most notably the forms of behavior that would be deemed appropriate within public streets and squares. Naturally, opinions and expectations on such questions tend to diverge according to the heterogeneous nature of urban spaces, and perceived social deviance would then

quickly be turned into a security issue through a filter of subjective insecurity and uneasiness. An apt illustration for such conflicts was provided by a municipality representative who spoke about a skater scene that had occupied a public square, and was described as highly threatening by senior citizens who had to cross said square. As she put it, "that's just two worlds colliding – of course skating is perceived as a problem from one side, and from the other side rather not" (Interview, 16 September 2014) – and yet the conflict was framed under the headline of a security problem.

A commonly encountered urban security issue that also speaks to diffuse social tensions is deviant behavior in public space. Said one interviewee: "Of course we have a drug scene, we have multiple spaces in which people linger in the middle of the day, consuming alcohol of course, and not everyone is happy with that" (Interview, 16 September 2014). And while public authorities were quick to point out that for instance the consumption of alcohol in public space was perfectly within legal boundaries, and therefore there was neither a desire nor an instrument to solve a (security) problem that from their perspective was indeed non-existent, a police officer clearly pointed out that subjectively perceived security problems had to be taken seriously and carefully considered in order to demonstrate responsibility towards the population. We will go more into detail concerning strategies of resolving security problems below. It should however be noted here that the much-discussed divide between "objectified" threats, often defined through the knowledge and authority of security experts and professionals, and the affective layer, in academic takes on security often dismissed as "irrational" reactions within the broader population, appears to be one of the key constituents of a blurry urban security problematic.

Diverging demands and expectations in terms of the use of public space are on the one hand closely linked to subjective insecurities, and on the other hand also to the characteristics of space itself (which in turn arguably links back to the subjective dimension). Different neighborhoods produce very distinct expectations when it comes to security, often connected to imaginaries of law, order, and aesthetics (or the lack thereof). As one police officer put forward: "often these are simply issues that interfere with subjective expectations, especially in quieter districts and neighborhoods. Of course people in the city center are not as susceptible as for example in [District A]" (Interview, 29 October 2014). Apart from such diverging interpretations of the urban, more generally the public, and eventually the willingness to endure friction and contradiction, there are indeed spaces that are agreed upon by many, though not all, as to induce fear and anxiety. Think of a barely lit tunnel, or a dark and rundown alley. In fact, municipal action plans seek to re-design such "places of fear," and thereby to increase the subjective level of security. As said one interviewee from the municipality: "that's what I have to face at work on an everyday basis, that someone tells me: yes, I am afraid of that place. And there are places where that's reasonably comprehensible" (Interview, 16 September 2014).

Security actors

As has been shown, urban security problems are rather complex and indeed hard to locate among the continuum between expert assessments and the legal framework, and the feelings and needs of population subgroups. Just as complex as the question of the nature of security problems is the question of who should be concerned with their solution. Security actors might be broadly divided into professionals (police and other state authorities as well as private security firms) and lay people (civic initiatives such as for instance neighborhood watches, vigilantes, or volunteers). As mentioned earlier, the transformation of policing over the past decades has brought about a multitude of new modes cooperation and co-optation, outsourcing and contracting, the emergence of a new private security market, and more generally a much more managerial scope of police work (e.g., Osborne and Gaebler, 1993; Ericson and Haggerty, 1997; Garland, 2001; Jones and Newburn, 2002; for Germany see notably Wehrheim, 2004; Eick *et al.*, 2007; Wurtzbacher, 2008; Kaufmann, 2013; Abt *et al.*, 2014).

As Abt *et al.* (2014) put forward, contemporary constellations of security actors might best be described as "dynamic arrangements" that emerge and re-emerge in reaction to specific problems. A strong emphasis thereby lies on participatory mechanisms, particularly within the urban. As Connolly and Steil (2009: 6) argue, "the city is the scale large enough for a government to have meaningful power, but still small enough for a democracy in which people can actually affect politics," which allows for an unmediated experience of the success (or failure) of participatory action. Such emphasis has resonated in a positive political framing of participatory accounts of urban security, as for instance put forward by the European Forum for Urban Security (2012: 17) that claims the importance of "shared social responsibility in making decisions related to security, which starts with a collective definition of the term 'security'." Such shared responsibility is not always easily enacted – as Kaufmann (2013: 1021) highlights, there are problems linked to uneven resources in terms of knowledge, time, and general habitus when it comes to cooperation between experts and lay people. Moreover, as mentioned earlier, participation is also characterized by an ambivalent notion of "post-politicality" – raising questions about whether civic involvement can have a meaningful impact, or whether it might be misguided as a means of legitimizing pre-defined political programs.

Empirically, forms of (non-)cooperation could be witnessed by two civic initiatives; one that patrols the neighborhood streets at night in order to take care of youths and mitigate potential conflicts; and one that, managed and coordinated by local police, deploys senior citizens as "security experts" who then enact peer group education among the population, thereby highlighting means and tools of crime prevention. Against the backdrop of scarce resources, representatives from both the initiatives themselves, as well as from the police, admitted that such new organizational forms in a certain way make up for the lack of municipality and police personnel. Said one respondent: "[the municipality staff] can't do that during their working hours. They are working during the day, they can't work at night, too.

They do their duty during the day, they can't do that" (Interview, 15 January 2015). Accordingly, the initiative saw justification to 'claim' the night shift and to provide a security/community service that otherwise would be lacking.

At the same time, all interviewees involved in cooperative citizen-state security production made it perfectly clear that there must be a strict divide between the sovereign powers of the police and the competencies of citizens. Said one police officer: "I don't want to have volunteers out there who give people the impression that they are on some kind of deputy mission" (Interview, 7 January 2015). Notably, this divide was also highlighted by civic initiatives themselves, expressing no desire to be confused with the police in the first place as this would potentially undermine their trusty relationship with their focus group. Said one volunteer: "If, for example, under-aged youths smoke or drink alcohol – we won't report that. We want to build a trustful atmosphere" (Interview, 15 January 2015). Added a "senior citizen security expert," speaking about their experiences with their peer group: "There were definitely circles who wanted nothing to do with the police" (Interview, 7 January 2015).

Security solutions

As has been shown, actor perspectives on security problems are easily as diverging as the frictions of urban space that constitute many security problems in the first place. How then can such complexity that is arguably often rooted in broader social problems be resolved? Notably, a strategy for the solution of security problems, particularly subjective insecurity, that was often put forward during our fieldwork was to strengthen security in a way that is a stunning reminder of the "broken windows" (Kelling and Wilson, 1982) argument, thus emphasizing the nexus of aesthetics, law and order. In the vein of the broken windows paradigm, once the integrity of a given neighborhood would be compromised through, for instance, a broken window or any other form of decay and/or vandalism that would not be repaired in a timely fashion, cascading effects of social disorder would unfold. Said one interviewee from a neighborhood initiative: "Of course I have a great interest that there are no empty pizza boxes, or that people don't dispose of their household waste into public trash bins, and that kids don't just drop everything that they don't need right at the moment. Simply cleanliness and security." (Interview, 7 January 2015). It should however be noted that the link between aesthetics, law, and order remains questionable and has been subject to theoretical, empirical, and normative critique (for a comprehensive account, see Harcourt, 2001).

Another way of addressing security problems, especially the conflicts sketched above that stem from diverging interpretations of public space, was to mitigate insecurity through a practice of recognition. This is true for professionals as well as for civic involvement. As said one respondent from a civic initiative, for them it is of utmost importance to show "that we recognize the youths, that we take them seriously" (Interview, 15 January 2015) – thereby setting their work clearly apart from repressive strategies. A similar approach was in fact claimed by representatives from the authorities. As one police chief framed the matter at hand: "I would start

with taking [citizens] seriously. By that I mean the uttered worries, the uttered uneasiness, take that seriously. That is our self-conception as police in the first place" (Interview, 6 January 2015). The rationale behind such an approach, as he detailed further, was to strengthen trust in the institutional capacity to protect, and to prevent possible radicalization that could be fostered by discontent with the state early on. Thus, in a certain sense, subjective insecurity must be seen as a leitmotif for security production across the urban; and one that must be recognized and acknowledged. Indeed, as a public order office supervisor admitted, "where the need for security, the cry for security is the loudest, that's where we try to be present" (Interview, 16 September 2014).

A third strategy for security solutions, as became clear from our fieldwork, is the enhancement of what might best be described as "social security," and that stands closely connected to contemporary urban protest movements that are grounded in Lefebvre's dictum of the Right to the City. Such enhancement of social security is enacted primarily through means of integration and social work, but also through forms of self-organization. As put forward by a police officer, "for example social work can be related to security. Integration is related to security. Now we have a contact point for Muslims, that was unimaginable ten years ago" (Interview, 29 October 2014). Integration in relation to security is thus conceptualized as a means to mitigate the manifold conflicts about the purpose and use of public space. Such an approach would ultimately resemble community-based conceptions of the urban, as prominently described by Lefebvre. If the Right to the City is one of accessibility, shared space, and participation, the theoretical gap between social problems and security problems would need to be bridged. Said one respondent from a squatting initiative: "There are areas in which I feel naturally safe, because I know that all newsstands, all shops, all snack bars, that basically everyone in the streets – even if they are people who I don't know – takes care of each other" (Interview, 6 January 2015).

To be quite concise here: the rationales behind police work and left-wing activism are rather different and arguably incompatible. Notably, however, they do converge in recognition and the mitigation of urban friction through integration and participation. As stated by one police officer, it is deemed important "that citizens have the ability to participate, to provide their input, that they communicate the problems that they have" (Interview, 29 October 2014) – even if the police would eventually decide that the problem was not a 'real' security problem in the first place, but rather an issue that called for a good long conversation rather than repressive force. At the same time, civic involvement remains subject to interpretive struggles that may result in very distinct judgments about politics and state sovereignty. As said an interviewee from the squatting initiative: "Actually there is no way around political change. And sometimes my impression, or my suspicion, is that such projects as [Social City] are an attempt to obscure fundamental urban problems" (Interview, 6 January 2015).

Conclusions

The aim of this chapter was to empirically map the field of urban security production, with a special focus on where and how to locate forms of civic engagement and participation. As our analysis has shown, the complex and overlapping constellations of security problems, security actors, and security solutions are multi-dimensional and feature many layers. The production of urban security thereby easily escapes narrow definitions of crime and violence, and must rather be located within a broader continuum that includes mobile notions of space and affect. Politically, urban insecurities have been incorporated and re-framed into a positive reading of civic participation, thereby claiming that "security does not seek to alienate citizens from each other but rather to create shared spaces in which the safety of all is ensured" (European Forum for Urban Security, 2012: 8). Such a vision raises questions of whether such shared spaces and common-good security could ever be achieved, given the empirical findings that a good deal of urban (in-)securities stem from conflicts around public space in the first place. Subsequently, should it not rather be acknowledged that not all security problems are resolvable, especially considering the necessary frictions that urbanity creates (and is supposed to create)? As one police officer frankly admitted, "in a city you always have to have to live with beggars, with homeless people, with alcoholics" (Interview, 29 October 2014) – and arguably, this is not a bad thing. The urban characteristics of encounter, conflict, and difference must however not be mistaken for a legitimization of social injustice.

Connecting those findings to larger trajectories of privacy and security, it becomes in fact clear that not only privacy is a moving target, but that the meaning of security – and subsequently the adequate means to achieve it – hinges to a large extent on the applied perspective, thereby also rendering it a contingent variable. Cities are dense social and political spaces where distinct angles on (in-)securities converge, thus laying bare the contested nature of security production. With regard to the relation between privacy and security, we therefore call to proceed with caution. After all, as Valkenburg (2015) claims, perceiving of two abstract concepts through a presupposed "trade-off" runs the danger of painting an overly simplistic picture. In the end, any analysis of privacy vs/and/or security will necessarily have to proceed through empirical contextualization.

In this chapter, we have put a particular emphasis on the role of civic participation in the multiple productions of urban security. There is certainly a political economy surrounding modes of including the population in urban processes, often with a subtext that civic involvement might produce the best results when put under the supervision of public bodies that provide the necessary vision and managerial competence. We pledge for the continuation of a research agenda that carefully scrutinizes how exactly citizens become part of security – and to notably extend this agenda to questions of privacy. As Marcuse (2006: 921) argues, for many urban insecurities "there is no absolute division between legitimate and false responses: there are many borderline cases, and there is certainly a subjective element involved." This is true for privacy as well. We would like to conclude by

highlighting that exactly those borderline cases provide the possibility to get a better grip on the social fabric – both of the city and beyond – as it is precisely those interstices all too often remain hidden in grand claims about power, expertise, and democracy.

Acknowledgments

Notes

1   Interviews have been conducted in German. All quotes have been translated by the authors.
2   Funded by the German Federal Ministry for Education and Research, the project analyzes modes of security production in two German cities (Stuttgart and Wuppertal), thereby exploring implications for distributional justice.

References

Abrahamsen, R., Hubert, D. and Williams, M.C. (2009) 'Guest Editors' Introduction'. *Security Dialogue* 40: 363–372.

Abt, J., Hempel, L., Henckel, D., Pätzold, R. and Wendorf, G. (eds) (2014) *Dynamische Arrangements städtischer Sicherheit: Akteure, Kulturen, Bilder,* Wiesbaden: Springer VS.

Amoore, L. (2014) 'Security and the Claim to Privacy'. *International Political Sociology* 8: 108–112.

Bellanova, R. (2014) 'Data Protection, with Love'. *International Political Sociology* 8: 112–115.

Berg, L. van den, Pol, P.M.J., Mingardo, G. and Speller, C.J.M. (2006) *The Safe City: Safety and Urban Development in European Cities.* Aldershot/Burlington: Ashgate.

Bigo, D. (2002) 'Security and Immigration: Toward a Critique of the Governmentality of Unease'. *Alternatives: Global, Local, Political* 27: 63–92.

Bishop, R. and Phillips, J.W.P. (2013) 'The Urban Problematic'. *Theory, Culture & Society* 30: 221–241.

Bishop, R. and Phillips, J.W.P. (2014) 'The Urban Problematic II'. *Theory, Culture & Society* 31: 121–136.

Butler, C. (2012) *Henri Lefevbre: Spatial Politics, Everyday Life and the Right to the City.* Abingdon: Routledge.

Connolly, J. and Steil, J. (2009) 'Introduction: Finding Justice in the City'. In Marcuse, P., Connolly, J., Novy, J., Olivo, I., Potter, C. and Steil, J. (eds) *Searching for the Just City: Debates in Urban Theory and Practice.* Abingdon: Routledge, 1–16.

Coward, M. (2009) 'Network-Centric Violence, Critical Infrastructure and the Urbanization of Security'. *Security Dialogue* 40: 399–418.

Dikeç, M. (2002) 'Police, Politics, and the Right to the City'. *GeoJournal* 58: 91–8.

Eick, V. (2003) 'New Strategies of Policing the Poor: Berlin's Neo-Liberal Security System'. *Policing and Society* 13: 365–379.

Eick, V. and Briken, K. (eds) (2014) *Urban (In)Security: Policing the Neoliberal Crisis,* Ottawa: Red Quill Books.

Eick, V., Sambale, J. and Töpfer, E. (eds) (2007) *Kontrollierte Urbanität: Zur Neoliberalisierung städtischer Sicherheitspolitik,* Bielefeld: transcript.

Ericson, R.V. and Haggerty, K.D. (1997) *Policing the Risk Society.* Oxford: Clarendon Press.

European Forum for Urban Security (2012) *Security, Democracy and Cities: The Manifesto of Aubervilliers and Saint-Denis.* Paris: European Forum for Urban Security.

Friedewald, M., Wright, D., Gutwirth, S. and Mordini, E. (2010) 'Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework'. *Innovation: The European Journal of Social Science Research* 23: 61–67.

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society.* Oxford: Oxford University Press.

Goede, M. de (2014) 'The Politics of Privacy in the Age of Preemptive Security'. *International Political Sociology* 8: 100–104.

Gornig, M. and Goebel, J. (2013) 'Ökonomischer Strukturwandel und Polarisierungstendenzen in deutschen Stadtregionen'. In Kronauer, M. and Siebel, W. (eds) *Polarisierte Städte: Soziale Ungleichheit als Herausforderung für die Stadtpolitik.* Frankfurt/New York: Campus, 51–68.

Graham, S. (2004) 'Introduction: Cities, Warfare, and States of Emergency'. In Graham, S. (ed.) *Cities, War, and Terrorism: Towards an Urban Geopolitics.* Oxford: Blackwell, 1–25.

Graham, S. (2006) 'Cities and the "War on Terror"'. *International Journal of Urban and Regional Research* 30: 255–276.

Harcourt, B.E. (2001) *Illusion of Order: The False Promise of Broken Windows Policing.* Cambridge, MA: Harvard University Press.

Harvey, D. (2008) 'The Right to the City'. *New Left Review* 53: 23–40.

Harvey, D. (2012) *Rebel Cities: From the Right to the City to the Urban Revolution.* London: Verso.

Hobsbawm, E.J. (1973) 'Cities and Insurrections'. In Hobsbawm, E.J. (ed.) *Revolutionaries: Contemporary Essays.* London: Weidenfeld and Nicolson, 220–233.

Holm, A. (2014) *Mietenwahnsinn: Warum Wohnen immer teurer wird und wer davon profitiert.* Munich: Droemer Knaur.

Jeandesboz, J., Bigo, D. and Frost, M. (2012) 'Discourses and Politics of Security and Surveillance, Privacy and Data Protection'. In Friedewald, M. and Bellanova, R. (eds) *Smart Surveillance: State of the Art. SAPIENT Deliverable D1.1.* Available at: www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf (accessed 29 April 2016).

Jones, T. and Newburn, T. (2002) 'The Transformation of Policing? Understanding Current Trends in Policing Systems'. *British Journal of Criminology* 42: 129–146.

Kaufmann, S. (2013) 'Die Stadt im Zeichen ziviler Sicherheit'. In Heckmann, D. (ed.) *Verfassungsstaatlichkeit im Wandel: Festschrift für Thomas Würtenberger zum 70. Geburtstag.* Berlin: Duncker and Humblot, 1011–1028.

Kelling, G.L. and Wilson, J.Q. (1982) 'Broken Windows: The Police and Neighborhood Safety'. Available at www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/ (accessed 29 April 2016). *The Atlantic.*

Kitchin, R., Lauriault, T.P. and McArdle, G. (2015) 'Knowing and Governing Cities Through Urban Indicators, City Benchmarking and Real-time Dashboards'. *Regional Studies, Regional Science* 2: 6–28.

Leese, M. (2015) 'Privacy and Security – On the Evolution of a European Conflict'. In Gutwirth, S., Leenes, R. and De Hert, P. (eds) *Reforming European Data Protection Law.* Dordrecht: Springer, 271–289.

Lefebvre, H. (1996) *Writings on Cities.* Malden: Blackwell.

Marcuse, P. (2006) 'Security or Safety in Cities? The Threat of Terrorism after 9/11'. *International Journal of Urban and Regional Research* 30: 919–929.

Marcuse, P. (2009) 'From Critical Urban Theory to the Right to the City'. *City: Analysis of Urban Trends, Culture, Theory, Policy, Action* 13: 185–197.

Massumi, B. (2007) 'Potential Politics and the Primacy of Preemption'. *Theory & Event* 10.

Mayer, M. (2008) 'Städtische soziale Bewegungen'. In Roth, R. and Rucht, D. (eds) *Die sozialen Bewegungen in Deutschland seit 1945: Ein Handbuch*. Frankfurt/New York: Campus, 293–318.

Mayer, M. (2011) 'Recht auf die Stadt-Bewegungen in historisch und räumlich vergleichender Perspektive'. In Holm, A. and Gebhardt, D. (eds) *Initiativen für ein Recht auf Stadt: Theorie und Praxis städtischer Aneignung*. Hamburg: VSA, 53–77.

Osborne, D. and Gaebler, T. (1993) *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*. New York: Penguin Books.

Préceteille, E. (2013) 'Die europäische Stadt in Gefahr'. In Kronauer, M. and Siebel, W. (eds) *Polarisierte Städte: Soziale Ungleichheit als Herausforderung für die Stadtpolitik*. Frankfurt/New York: Campus, 27–50.

Revol, C. (2014) 'English-Speaking Reception of "Right to the City": Transpositions and Present Meaning'. In Erdi-Lelandais, G. (ed.) *Understanding the City: Henri Lefebvre and Urban Studies*. Newcastle upon Tyne: Cambridge Scholars, 17–36.

Swyngedouw, E. (2009) 'The Antinomies of the Postpolitical City: In Search of a Democratic Politics of Environmental Production'. *International Journal of Urban and Regional Research* 33: 601–620.

Valkenburg, G. (2015) 'Privacy versus Security: Problems and Possibilities for the Trade-Off Model'. In Gutwirth, S., Leenes, R. and de Hert, P. (eds) *Reforming European Data Protection Law*. Dordrecht/Heidelberg/New York/London: Springer, 253–270.

Wakefield, S. and Braun, B. (2014) 'Governing the Resilient City'. *Environment and Planning D: Society and Space* 32: 4–11.

Wehrheim, J. (2004) 'Städte im Blickpunkt Innerer Sicherheit'. *Aus Politik und Zeitgeschichte*: 21–27.

Wurtzbacher, J. (2008) *Urbane Sicherheit und Partizipation: Stellenwert und Funktion bürgerschaftlicher Beteiligung an kommunaler Kriminalprävention*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Part III

Governance of security and surveillance systems

9 Moving away from the security–privacy trade-off

The use of the test of proportionality in decision support

Bernadette Somody, Máté Dániel Szabó, and Iván Székely

The trade-off model and its critiques

Contrasting security to privacy is one of the well-known manifestation areas of the popular approach according to which competing values and demands in a democratic society, as well as the fundamental rights reflecting them, can only be realized at the expense of each other, by creating a balanced result in a virtual zero-sum game. In other words, realizing such a demand or right prevents people from realizing a competing demand or right, or more precisely, they need to waive the same amount of their demands or rights as much as they expect them to increase on the other side. In a narrower sense this trade-off approach can also be applied in situations where the mere preserving of the existing level of realizability of a certain demand or right – or at least the mitigation of its erosion – presupposes the waiving of a competing right or demand.

Naturally, the legitimization of this trade-off approach always necessitates the defining of an antipole, a competing demand or right. Privacy is one of the most frequently referred such antagonists of security.[1] This approach, however, inherently disregards the complexity of demands, values and legal rules in society together with their interdependencies, and reduces the problem to a single conflict, real or imaginary. Although this intention for simplifying the problems and making them easily comprehensible and acceptable for the public is understandable from the policy-makers' point of view, the temptation for abusing this oversimplified approach can lead to propagating a false image in society according to which in a democratic society every demand or right – in general, the realizing of public goods[2] – has a 'price' in the domain of public goods, which has to be paid by waiving certain demands or rights. This image may suggest a 'reasonable trade-off' between the competing demands or rights but at the same time masks the longer-term consequences, namely that not only the complementing demand or right will be eroding but also a host of associated rights, freedoms and values that the trade-off is designed to protect, including democracy itself.[3]

Loader and Walker (2007) argue that the concept of 'public good' can usefully be applied to the study of security, and can be expanded beyond its narrow

economistic usage in which it refers to non-excludable and non-rivalrous goods from which everyone benefits, such as fresh air or national defence. The concept of public good can also include shared societal goods such as liberty or freedom of expression, but additionally, it is argued, can be expanded further still to capture its broader role as a 'constitutive public good'; that is, a societal good understood as an integral and essential element of society itself.

In the present historical period when the importance of security in general is becoming more and more emphasized in politics, mass communication and public discourse alike, and when rapid technological developments and the associated business interests stimulate the introducing of new technologically mediated security measures, in particular surveillance measures, this trade-off approach can easily serve as an ideology for legitimizing unreasonable restrictions of fundamental rights, including privacy.

Although not contesting the existence and necessity of such trade-off situations, several theoreticians have criticized the exclusivity of this approach in the area of fundamental rights and, consequently, its exclusive application at various levels of decision-making. Charles Raab in his chapter 'From balancing to steering: new directions for data protection' (Raab, 1999) critically analysed the 'balancing paradigm' in privacy-related control mechanisms and observed that 'balancing often constitutes steering towards a preferred privacy outcome' and that '"balancing"' as such is an inadequate normative conception'. He also noted that in practice '"striking a balance" or "getting the balance right" remains a *mantra* rather than a practical philosophy for decision-making in difficult circumstances where fundamental issues are at stake' (p. 69). Others (Wright and De Hert, 2012; Wright and Raab, 2012) developed impact assessment methodologies to be used in situations when decisions have to be made over the introduction of privacy-intrusive and security-enhancing measures, such as increased surveillance. These methodologies aim to clarify the longer-term impacts, the identity of the affected parties, and the social and economic costs of the decision to be made, thus forcing the decision-maker to legitimize the envisioned 'balance' between security and privacy. In Chapter 3 of this volume Vermeersch and De Pauw (2016), from the aspect of public acceptance of new security oriented technologies, experimented with replacing the trade-off approach with 'framing' technologies.

From another angle, everyday practice and common sense may also contest the absolute primacy of the trade-off between privacy and security over other approaches. For example, if the question is whether enhancing the security and safety of homes should be achieved by installing more CCTV cameras in the house or by installing stronger locks on the doors, many would opt for the latter, since this solution increases *both* security and privacy of the people concerned, and there is no need for a trade-off between the two demands. Also instructive is the recent history of body scanners installed at US airports, introduced as a result of a typical trade-off between the enhanced security of travelling and the privacy of individual travellers. Investigations initiated by advocacy groups[4] revealed that the early X-ray devices were ineffective but seriously infringed travellers' dignity and privacy, and caused medical harms, so the trade-off was hardly legitimate. After a series of

lawsuits the scanners have been removed and replaced by less intrusive devices that do not record and transfer naked images of air travellers, still fulfilling their function of detecting weapons and explosives.

In the field of empirical sociology, researchers of the EU-supported international research project PRISMS[5] recently conducted a large scale empirical survey, the first of its kind to sample public opinion in all Member States to determine whether people evaluate the introduction of security technologies in terms of a trade-off. Although it is not the task of the present study to interpret the findings of this survey, the preliminary results already show that the importance of the two values, privacy and security, do not depend on each other at all in people's mind.[6]

Privacy vs. security is not the only field of application of the trade-off model. Since the fundamental values of society are reflected in the legal systems, it was a historical necessity during the course of developing democratic rule-of-law systems to work out methodologies by the use of which it became possible to manage such conflicts within the legal domain, in particular to judge the lawfulness of measures restricting fundamental rights. The present study is using one of the two historically developed such methodologies as the basis of further research.

The trade-off approach has infiltrated the policy level, too, sometimes simply serving the purpose of legitimizing those measures which restrict fundamental rights. Similarly, business entities, which have vested interests in introducing such measures, for example deploying and operating surveillance systems, and in convincing decision-makers to support the use of such systems, often use this argumentation for legitimizing their activities. In a broader sense it is the interest of the whole security industry (with a less polite term, risk industry) to use this argumentation for justifying the harmful side-effects of its activities on privacy, dignity, or equality, when fulfilling real demands for enhancing security. Those analyses, which evaluate the social advantages and harms of such measures, for example Norris (2012), Germain, Dumoulin and Douillet (2013) or Čas *et al.* (2014) often find these measures unreasonable, not only in terms of social costs but also in terms of economic costs (Groombridge, 2008).

The legal approach – the anatomy of the test

In the following we briefly present how democratic legal systems handle conflicting fundamental rights and legitimate interests, and show how the judicial practice seemingly corroborates the illusion of inevitableness of the trade-off. From among the two main methodologies developed in democratic rule-of-law traditions we analyse the European one, the test of proportionality in detail, and show how methodological rigour in using the test can help superseding the trade-off model within the legal domain.[7]

The concept of proportionality was originally developed by the German Federal Constitutional Court, but expanded far beyond Germany, and one can say that it became the post-war paradigm of human rights protection. The doctrine was also adopted by the European Court of Human Rights (ECtHR), since the interpretation of the limitation clauses of Articles 8-11 of the European

Convention of Human Rights (ECHR) were grounded on proportionality. The 'Strasbourg method' includes the identification of the legitimate aim of restrictions, and, under the 'necessary in a democratic society' clause, the examination of the necessity and proportionality of limitations.

Deciding about the lawfulness of the limitation of a fundamental right is also a methodological challenge. Should it be a constitutional or a conventional right, the responsible court – a constitutional court or the ECtHR – can make its decision verifiable, increase its persuasiveness and secure its authority if it strictly follows the steps of the limitation test where only the last step constitutes the actual balancing between the conflicting rights and interests, which involves, by its nature, moral arguments. Prior to that, the human rights courts, thus the ECtHR, too, have to decide, first, whether a fundamental right, protected by the given constitution or the Convention, is concerned in the case, and second, whether the quality of the law restricting the right meets the requirements.

The test of proportionality is not a single test: it consists of four sub-tests, namely the legitimate aim test, the suitability test, the necessity test and, finally, the proportionality test in the narrow sense (Figure 9.1).

During the first sub-test, a purpose can justify the limitation of a fundamental right if it is considered legitimate in society, if it is expresses a value on which the society is founded. In a constitutional democracy, generally speaking, safeguarding
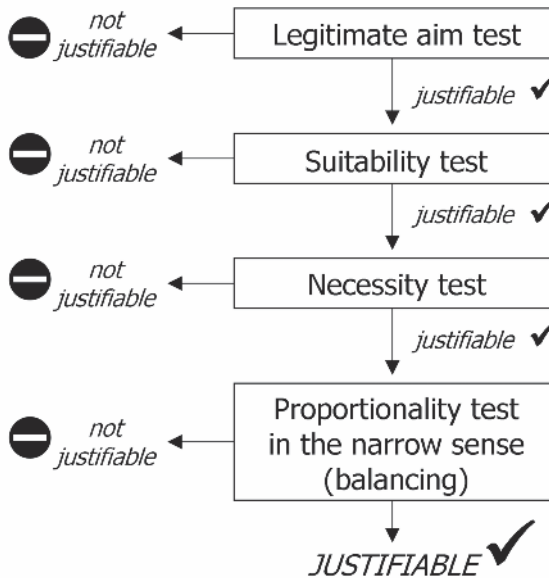
Figure 9.1 The structure of the test of proportionality

human rights and, to a certain extent, satisfying public interests can be taken into account as legitimate purposes. The ECHR contains special limitation clauses listing such legitimate purposes. It should be noted that from the viewpoint of a legal examination, the public interest of security as one of the legitimate aims does not need further justification when it or certain aspects thereof are explicitly named in the relevant limitation clause.

The function of the second sub-test is to determine whether the limitation of the fundamental right concerned – in case if it was found to have a legitimate aim – is suitable for realizing the aim. When deciding about the rational connection between the purpose of the limitation and the limiting measure, research results of other disciplines shall also be relied on. Sociology, criminology, and other disciplines offer scholarly achievements that make the decision on the suitability of the intrusive measure a question of fact. More CCTV cameras, for example – according to the results of criminological research – do not necessary lead to a higher level of security.[8]

In the third sub-test, after having established the legitimacy of the aim and the suitability of the limitation to achieve the given aim, the necessity of the limitation is examined, in other words, whether the limitation applies the *less restrictive means* in order to advance the legitimate aim. For example, justifying the necessity of a measure limiting privacy, non-legal measures also have to be taken into account: such measures, which are less intrusive or do not limit rights at all. Experience shows that there exist privacy-friendly, even non-surveilling, technologies for realizing the same security purposes.

The last sub-test, the proportionality test in the narrow sense, is the real field of (judicial) discretion which requires balancing between two values: on the one hand, the aim of the limitation and, on the other hand, the limited fundamental right. The limitation of a fundamental right is justified if there is a proper relation between the benefit gained by the realization of the aim and the harm caused to the fundamental right.

As we have seen, a series of methodological steps on the basis of these sub-tests should be taken in order to decide whether a limitation imposed on a fundamental right is justified. Even if these structural elements of the test of proportionality are not clearly identifiable in each judicial decision, the strict application of the methodology requires that the conducting of the next sub-test can only be permitted if the case concerned has successfully passed the preceding sub-test.[9]

The privacy/security conflict in the practice of the ECtHR

The test of proportionality is not explicitly recognized by the text of the European Convention on Human Rights. Nevertheless, the European Court of Human Rights interprets the limitation clauses attached to Articles 8–11 of the ECHR in accordance with the concept of proportionality and applies the methodological steps of the test.

The ECtHR – also known as the Strasbourg Court – can reasonably be considered to be the most significant *human rights* forum in Europe since it sets the

minimal standard of the protection of fundamental rights for European states and its case law is decisive also for the European Union and the European Court of Justice interpreting the EU Charter of Fundamental Rights.[10] A number of legal theorists and authors have analysed the ECtHR's case law in general and the application of the proportionality test in particular, presenting the steps of the test in great detail and quoting the most well-known cases extensively. The value added by the present study to this corpus of legal texts is the methodological rigour with which we followed and analysed the steps of the test of proportionality, the great number of cases analysed from this aspect, and the suggestions made in order to find legal solutions to supersede the predominant concept of 'balancing'.

In the following we focus on the Strasbourg Court's case law about privacy, especially the information aspect thereof which provides protection for human personality in connection with the processing of data relating to the person. This protection is guaranteed primarily by Article 8 of the ECHR on the right to respect for private and family life. The essence of the proportionality test here is that the limitation on privacy in the interest of security can be justified if the two values stand in balance. This method of legal interpretation seems to be favourable for the trade-off model according to which the debate between privacy and security is a zero-sum game and people are forced to choose between the two.[11] According to the test of proportionality, courts have to choose between conflicting rights and interests and set up a balance between privacy and security since, as the test of proportionality suggests, the conflict flows from the very fact that both of them cannot be secured at the same time. However, as we noted above, both practical experience and empirical surveys show that there exist means and methods the application of which can strengthen security and privacy at the same time; in addition, people regard security and privacy as separate values, thus they want both. Therefore, after analysing the application of the proportionality test in the practice of the ECtHR, we attempt to answer the question whether the trade-off between privacy and security can be superseded within the framework of the proportionality test.

Information privacy, data protection and the ECtHR's jurisdiction

The right to privacy is one of the human rights of primary importance which protects various aspects of human personality. Decisional privacy guarantees freedom to make decisions about one's body and family. Its continental counterpart, the right to self-determination, covers matters such as termination of pregnancy, sterilization, refusing life-sustaining treatments, consumption of drugs and sexual decision-making. However, several traditional privacy issues do not raise the question of balancing with security interests at all. Surveillance for security purposes concerns expressly the right to *information privacy,* a special segment of privacy securing protection against collection, use and disclosure of a citizen's personal information.[12] Surveillance aimed at enhancing security affects citizens by the fact that these tools and methods involves collection, storage, use and disclosure of their personal information, the exclusion of the access to personal data related to them

or the restriction of the control over their personal information. In order to analyse the 'privacy vs. security' conflict in the framework of the present project, we will focus on cases where the intrusion into citizens' private life is the result of *processing information* relating to them.

We argue that in the ECtHR's practice the protection of information privacy is based on Article 8 of the Convention, which guarantees everyone's rights to respect for their private and family life, their home and their correspondence – despite the fact that this Article does not use the category of personal information or personal data. The ECtHR does not clarify the theoretical relation of the right to privacy and to data protection. This is still an open question, as it can be described with more than one logical relation within the European legal systems, including the jurisprudence of the ECtHR.[13] Since there are existing judgments that interconnect these rights, it is plausible to argue that these rights have an overlapping common segment, however, privacy protection can aim at a different kind of protection than data protection does, and the scope of data protection covers personal information in a distant or indirect relation with the private sphere.

Nevertheless, throughout its jurisprudence, the ECtHR has examined many situations in which the issue of data protection arose, and all these cases were adjudged on the basis of Article 8 of the ECHR. Interferences with the right to personal data protection, including cases concerning protection against the interception of communications,[14] various forms of surveillance[15] and storage of personal data by public authorities[16] may be brought before the Strasbourg Court through the allegation of breach of the rights covered by Article 8. Surveillance and record-keeping of personal data are in close connection with the protection of private life. In some cases, where the Court had to decide whether there was an interference with the applicants' privacy rights – thus, when it examined the applicability of Article 8 – it consequently used the notion of *private life* as a broad term that is not susceptible to exhaustive definition,[17] but it undisputedly covers data protection issues. The Court holds that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8.[18] Article 8 also protects the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[19] It may include activities of a professional or business nature.[20]

According to the Court, there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'.[21] According to the Court, private-life considerations may arise when any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[22] The Court's case law has, on numerous occasions, found that the covert tapping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence. While it is generally the case that the recordings were made for the purpose of using the content of the conversations in

some way, the Court also stated that recordings taken for use as voice samples cannot be regarded as falling outside the scope of the protection afforded by Article 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. In a case where the applicant being charged by the police had to answer formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants.[23]

The broad field of case law interpreting security as the purpose of limitation of privacy covers various situations (for example where, because of detention, refusal of a residence permit or expulsion from a country to another, the applicants were incapacitated to communicate with close relatives, etc.). However, regarding the importance of security-purpose surveillance in limiting the right to privacy, we further narrowed down the scope of the analysis to those cases in which surveillance measures are in interference with information privacy. These cases concern typical conflicts between security and information privacy/data protection, such as interception of private communication, secret surveillance of individuals, registration of citizens in various databases for lustration purposes, or investigation of crimes.

Security as a legitimate aim

One can observe that the possible legitimate aims are exhaustively enumerated in the limitation clause attached to the declaration on the right to respect for private life. According to the second paragraph of Article 8, the interference must pursue national security, public safety or the economic wellbeing of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

On the one hand, we can state that security as the purpose of a limitation can be considered a justified aim. On the other hand, however, only those aspects of security are acceptable *which are explicitly listed* in the cited paragraph. On the basis of the text of Article 8, the ECtHR is entitled to take security into account as national security, public safety or the prevention of disorder or crime. From a descriptive viewpoint it can be stated that security is present in the Strasbourg Court's practice as any of the mentioned categories.

Identifying the legitimate aim and deciding whether or not the limitation imposed on the right to privacy serves this aim are matter of facts and rational argumentation. At least in theoretical terms, these steps of the limitation test do not leave room for the discretion which manifests in the last phase of the test, namely in proportionality *stricto sensu*. It could be a yes or no question of whether or not security (or more precisely, enumerated aspects thereof) stand in conflict with the right to privacy in the given situation.

Being a question of facts and having an *expressis verbis* basis in the text of the Convention, the realization of the public interest of security could be considered as a strict requirement of the proportionality test applied in 'privacy vs. security'

conflicts. In fact, however, the examination of the legitimate aim proves that *this is the weakest component of this methodology.*

When analysing the ECtHR's case law on privacy and security one can identify several components of the right to privacy on the basis of which the scope of this fundamental right can be determined rather precisely. However, we cannot reach a similar result regarding the security-related purposes of limitation. The content of the relevant legitimate aims (national security, etc.) expressly listed in Article 8 is not expounded in the Court's practice. We cannot find abstract definitions or explanations in the decisions from which the notion of different aspects of security, or security in general, can be built up. The lack of defined contours of these categories is also proved by the fact that, in general, the Court does not refer to a single purpose of the limitation which can assumedly be selected as the relevant aspect of security in the case. The ECtHR often lists two or three security-related categories from Article 8(2), without defining the specific relevance of the different purposes.

The most frequently used formula by the Court simply enumerates *in one sentence a set of legitimate aims* that may be taken into account, for example *'the interests of national security or the economic well-being of the country or, just as equally, for the prevention of disorder or crime'*.[24] In other cases, the legitimate aims are *not even specified* in the judgment, the Court only declares that the '*restrictions pursued* one or more *of the legitimate aims enumerated in Article 8 § 2.*'[25] The eventuality of the referred legitimate aims is best proven when *the wording of the judgment indicates exemplification*, for example when the Court states that '*In the Court's view, it is not open to doubt that the monitoring of the applicant's correspondence pursued the legitimate aims of,* inter alia*, protecting 'national security' and/or preventing 'disorder or crime' referred to in Article 8 § 2'*.[26]

Analysing the cases where security-related purposes justified the limitation, one can find only a few sentences about the relevant legitimate aim where the ECtHR is satisfied with the mere indication of the purpose. In general, the Court does not make an attempt to define the conception of the referred legitimate aims and avoids any kind of reasoning on how and why the intervention by the state is serving the referred legitimate aim.

The lack of argumentation is represented by the wording used by the Court in paragraphs of judgments assessing the existence of one or more relevant legitimate aims of the intervention, such as '*the Court finds it established*'[27] or '*[t]he Court is prepared to accept*'[28] what the Government refers to, or when, according to the Court, the purpose pursued '*is not open to doubt*'.[29] The same occurs when '*the Court accepts the assertion by the Government*'.[30] The lack of a reverse statement of the applicant may be enough for the establishment of the legitimate aim: '*the applicant did not appear to deny that the impugned restrictions were imposed in pursuit of legitimate aims*'.[31] Furthermore, when none of the parties refers to or denies the establishment of a legitimate aim, the Court itself may assist them to do so: '*While the applicant contested the existence of a legitimate aim, the Government did not expressly refer to any legitimate aim pursued in this case. The Court, for its part, is ready to accept that the impugned measure pursued the legitimate aims of safeguarding national security and preventing disorder*'.[32]

The probability or possibility of the establishment of a legitimate aim may be enough to satisfy the Court: for instance, the intervention '*could have been in the interests*' of the relevant purposes, or '*the Court therefore concludes that the interference pursued a legitimate aim…*'.[33]

This leads us to the conclusion that, according to the Court's view, the reference to the security-related legitimate purpose of the restriction on privacy basically falls within the competence of the Government, which competence is untouched by the ECHR and is not subject to reconsideration by the ECtHR, resulting in that Strasbourg organs have very rarely found a violation of Convention rights by reference to the legitimate aim standard.[34,35]

Necessity and proportionality of the limitation of privacy

As we argued above, the ECtHR is rather reluctant to revise the governments' references to the different interests of security. Consequently the emphasis gets to the latter components of the test of proportionality. However, in these phases of the test the general tendency of the Court's argumentation is similar: it focuses the scrutiny on the 'necessary in a democratic society' standard.[36] This also means that the justification of a limitation on privacy is mostly a matter of balancing. The protection of privacy against the states' interests depends on the Court's discretion, which is manifested in comparing the weight of the interest of security with privacy.

We have to add here to the methodology of the test of proportionality that the ECtHR has developed, among others, the notion of the 'margin of appreciation'. This doctrine provides some sort of latitude to the national governments in certain cases, namely in lack of a European agreement, which is taken into consideration by the Strasbourg Court when it decides on the justification of a limitation and the proportionate balance. In respect of the limitation on privacy in the interest of security, this concept is of high importance, in these cases the ECtHR acknowledges the Member States' wide margin of appreciation.

In one of the most referred judgments about the justification of surveillance for security purposes, the Court summarized the relevant methodological steps of the legal evaluation, namely the assessment of necessity, proportionality and the consideration of the margin of appreciation, as follows: 'The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued […]. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life'.[37]

Superseding the trade-off model within the test

Although the steps and the structure of the test of proportionality are well-known in legal literature and judicial practice alike, few have studied the possibility of

categorizing the phases of the test from another aspect, namely, whether the respective sub-test is based primarily on factual or moral considerations. If we compare the structural composition of the test with the cases analysed above and the ECtHR's practice in general, we will find that the first three sub-tests are based on factual elements, and only the last sub-test involves moral considerations, that is, the actual balancing that may be based on a trade-off approach (Figure 9.2).

Judicial practice in which the sub-tests are merged or not sufficiently separated, and in which the first three sub-tests are concluded in a nonspecific manner, may result in making the whole procedure subject to moral balancing, and this is a methodological reason for the seeming inevitableness of the trade-off. The first thesis of the present study is therefore that the better separation of the factual and moral phases in the test of proportionality and a shift in the weight of factual and moral elements of the test to the advantage of the factual ones, coupled with an enhanced methodological rigour, can lead to more substantiated judicial decisions in the security vs. privacy conflicts and reduce the application area of the trade-off model.

In the Strasbourg case law several other principles and factors can be identified which are to be taken into consideration when evaluating the 'privacy vs. security' conflict within the framework of the proportionality test. Therefore, we can formulate some auxiliary theses that may further specify and facilitate the application of the proportionality test to the specific conflict between surveillance and information privacy by national courts or other responsible authorities. One such auxiliary thesis is that Article 8(2) is to be interpreted narrowly. Being exceptions
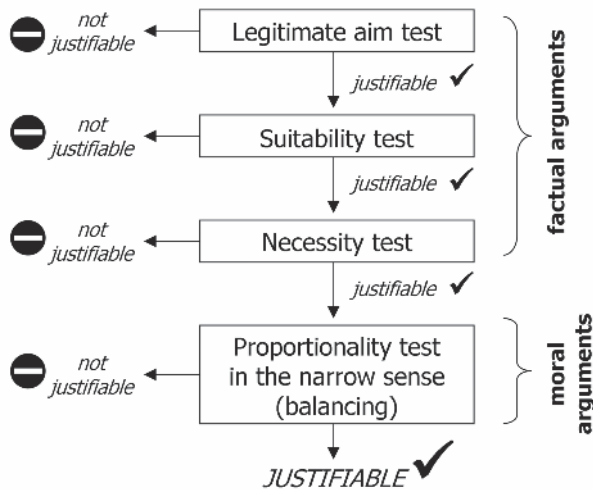
Figure 9.2 Factual and moral arguments in the test of proportionality

to the right to respect for private life, permissible limitations, such as the possibility of surveillance, have to be subject to a rigorous scrutiny. This general principle is acknowledged by the ECtHR: '[p]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions'.[38]

Today, surveillance is realized mainly through various surveillance technologies,[39] consequently – as a second auxiliary thesis – it needs to be emphasized that the peculiarities of the surveillance technology used in the case under judgment are to be investigated. This may seem as a trivial requirement; however, the structured analysis of the peculiarities of technologies is relevant equally when the necessity and when the proportionality of the interference is adjudged. The use of an intrusive surveillance technology is considered to be necessary only if less intrusive methods of surveillance were considered ineffective. As for the proportionality in the narrow sense, the balance between the interest of security and the right to privacy can also be influenced by the characteristics of the technological means or the use thereof. Several questions can be raised, such as whether the technology used is interconnected with other technologies, who has access to the collected data, or when and for how long the surveillance technology have been operating.[40]

Third, it also needs to be emphasized that the significance of security reasons may depend on the 'historical' context. The Court often states that nowadays democratic societies find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result recognized by the Court that the state must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court therefore accepts that some surveillance measures, under exceptional conditions, are necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[41] The intensity of the threat of terrorism changes over the years, and the Court is aware of that: it accepts the context of threat of terror because of actual terror events as a reason for the adoption of intrusive measures by the legislation, but it also warns that the maintaining or the reinforcement of such measures over the years may not be justified for longer periods of time.[42] Passage of time may also blur the significance of personal data collected and therefore weakens the connection between the storage of the personal data and its legitimate aim, security. Continued storage may not be supported by the original reasons that may become irrelevant and insufficient after a longer period of time.[43]

Finally, it should be noted that in order to establish the balance between security served by surveillance measures and information privacy, certain procedural guarantees also have to be taken into consideration. These safeguards include the effective domestic judicial proceedings; the Court examines whether the domestic proceedings were attended by sufficient procedural guarantees. The Court emphasizes that even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and rele-

vant evidence, if need be with appropriate procedural limitations on the use of classified information. The individual must be able to challenge the executive's assertion that national security is at stake. Failing such safeguards, the state authorities would be able to encroach arbitrarily on rights protected by the Convention.[44]

The application of the test in decision support

Security/privacy trade-off is an established approach in judicial practice, but it is also popular in decision-making situations where privacy-restricting measures are introduced in the interests of greater security. This approach is regarded as natural not only by those communicators and PR professionals whose task is to 'sell' and make socially acceptable the security measures originating from business, policy or other interests, but also by the decision-makers who can legitimate for themselves, too, the measures to be introduced.

The above analysis and the resulting theses have shown that by the use of the necessary methodological rigour it is possible to move away from the primacy of the trade-off model even within the legal domain. In the next phase of our study we examined whether the methodology of the test of proportionality can be exported to the field of decision support, more precisely, to decisional situations regarding the introducing of surveillance measures which may infringe people's privacy.

Naturally, there exist significant differences between the two application domains: the test had originally been developed for the vertical relationship between the state and the citizens, whereas in the decision-making environment the test will serve as a decision support tool for the decision-maker itself, or will be relating to the relationship between the decision-maker and the supervisory authorities, or will help defend the decision in a political or social debate. A further difference is that it is not the task of the courts to suggest solutions for improving the acceptability of a privacy-restricting surveillance measure, or to call the decision-maker's attention to possible win-win type solutions; however, the decision-maker should expressly be encouraged to apply such solutions.

These differences made it necessary to modify certain steps in the test, their order and weight and to increase their detailedness, while keeping the fundamental elements of the test and the separation of factual and moral arguments.

The list below contains the questions the decision-maker needs to answer before making its decision on the introducing (maintaining, or expanding) surveillance measures that may infringe people's privacy. It should be noted that there exist decision support tools in this area, developed in recent years, which offer question lists, thus inducing stakeholders to ask questions from themselves and from the decision-maker alike.[45] Such a tool can *support* the decision-making process, indeed, but leaves it to the discretion of the stakeholders concerned which questions they want to ask and what weight they give to the respective answers. In contrast, our suggested methodology obliges its users to follow the questions step by step, and to proceed to the next question only if the previous one has been answered successfully – according to the logic of the test of proportionality, otherwise the decision will not be legitimate.

The list of questions

The user has to read all of the questions below and answer them to the best of his knowledge. If the user does not have enough information for the proper answering of the question concerned, he has to acquire the missing information before answering the question and continuing the procedure. Depending on the content of the answer, the user may proceed to the next question, or has to modify the planned measure, or – if the modification is not feasible – should desist from the implementation of the planned surveillance measure. The entire procedure is summarized in Figure 9.3.

1.1 Does the planned application of surveillance have implications on people's privacy?
It must be presumed that any kind of the application of surveillance technologies has such implications, however, there may be exemptions. The question is whether the surveillance in question can be qualified as such an exemption.

1.2 If the surveillance does not have privacy implications at present, will it likely have such an implication in the future?
It is possible that a CCTV system monitoring traffic uses low resolution cameras at present that do not allow the identification of individuals, however, when new, high resolution cameras will be installed, pedestrians and car drivers will become directly identifiable.

2.1 Does the surveillance in question have a legal ground? Could you identify the relevant legal ground?
Usually laws do not provide an explicit entitlement or prohibition on establishing a surveillance system. Instead, the application of one of the general legal grounds (e.g. informed consent of the subjects affected) is required.

2.2 Could you interpret the legal ground in a strict way? Could the strict interpretation result that the identified legal ground does not serve as a suitable basis?
For example, informed consent cannot be considered as a valid legal ground if it is not freely given (e.g. an employee's consent to the installation of a CCTV system at his workplace). In case of an explicit entitlement its scope has to be considered and interpreted narrowly (e.g. the specific legal ground for the surveillance of employees is not applicable for that of students).

2.3 Does the surveillance in question break an explicit legal prohibition?
Explicit legal provisions may inhibit surveillance in situations where the subject may have a reasonable expectation of privacy (e.g. in changing-rooms).

3 Could you identify the purpose of surveillance in question as precisely as possible?
The mere fact that surveillance systems are widespread and seem to be

useful for various purposes is not satisfactory here. The purpose should be specific as much as possible (e.g. recording potential thefts and identifying the perpetrators).

4.1 Could you identify the security risks that the surveillance is supposed to react against?

Similarly to the question of the purpose of surveillance, the concrete security risk should be identified precisely (e.g. vandalism, robbery, employees' idleness).

4.2 Is the surveillance in question capable of decreasing these security risks?

The fact that the surveillance system is suitable for decreasing the risks specified in the previous point should be verified, which means that it should be proven by sociological, criminological, psychological etc. evidence.

5.1 Can the purpose served by surveillance (identified in Question 3) be achieved without surveillance?

The decision-maker has to consider various alternatives to surveillance. Alternatives not having privacy implications (e.g. physical protection of property) should be preferred.

5.2 If the purpose can be served without surveillance, would it involve further implications on rights or interests other than privacy?

When considering alternative measures, possible consequences on legitimate rights and interests should be taken into account (e.g. physical protection of property can cause damages to the objects of property). The interference with a legitimate right or interest also requires answering a list of questions similar to this algorithm.

5.3 Could you identify the characteristics of the surveillance technology planned to be applied?

For example, what kind of personal or sensitive data are collected? Who will access to the data collected? Where, when and for how long will the surveillance means be applied?

5.4 Considering the characteristics identified in Question 5.3 one by one, can the purpose served by surveillance (identified in Question 3) be achieved by surveillance that intrude into privacy to a lesser extent?

For example, remote monitoring does not require a CCTV system storing the recordings.

6.1 Do the individuals affected by the surveillance in question have the possibility to exert control over their surveillance?

Individuals may have rights to influence the surveillance affecting them, i.e. to obtain information about and to challenge data relating to them. If individuals have some ability to have their data erased, rectified, completed or amended, it provides them with more practical protections.

6.2 Could you identify these possibilities of the individuals?

For example, are they informed proactively? Are they given further information about the details? Are they allowed to object to the surveillance in general or to certain parts of it, etc.
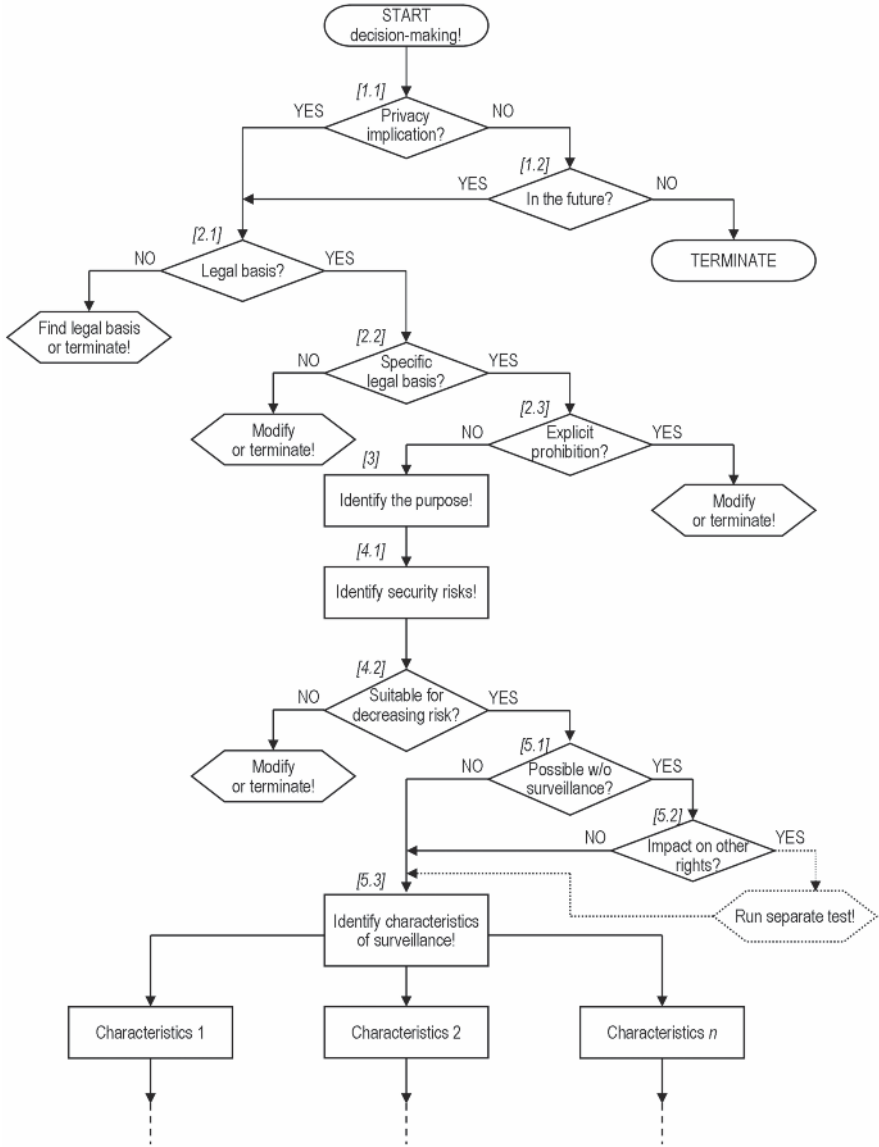
Figure 9.3a The steps of surveillance–related decision-making inspired by the test of proportionality (Part 1)
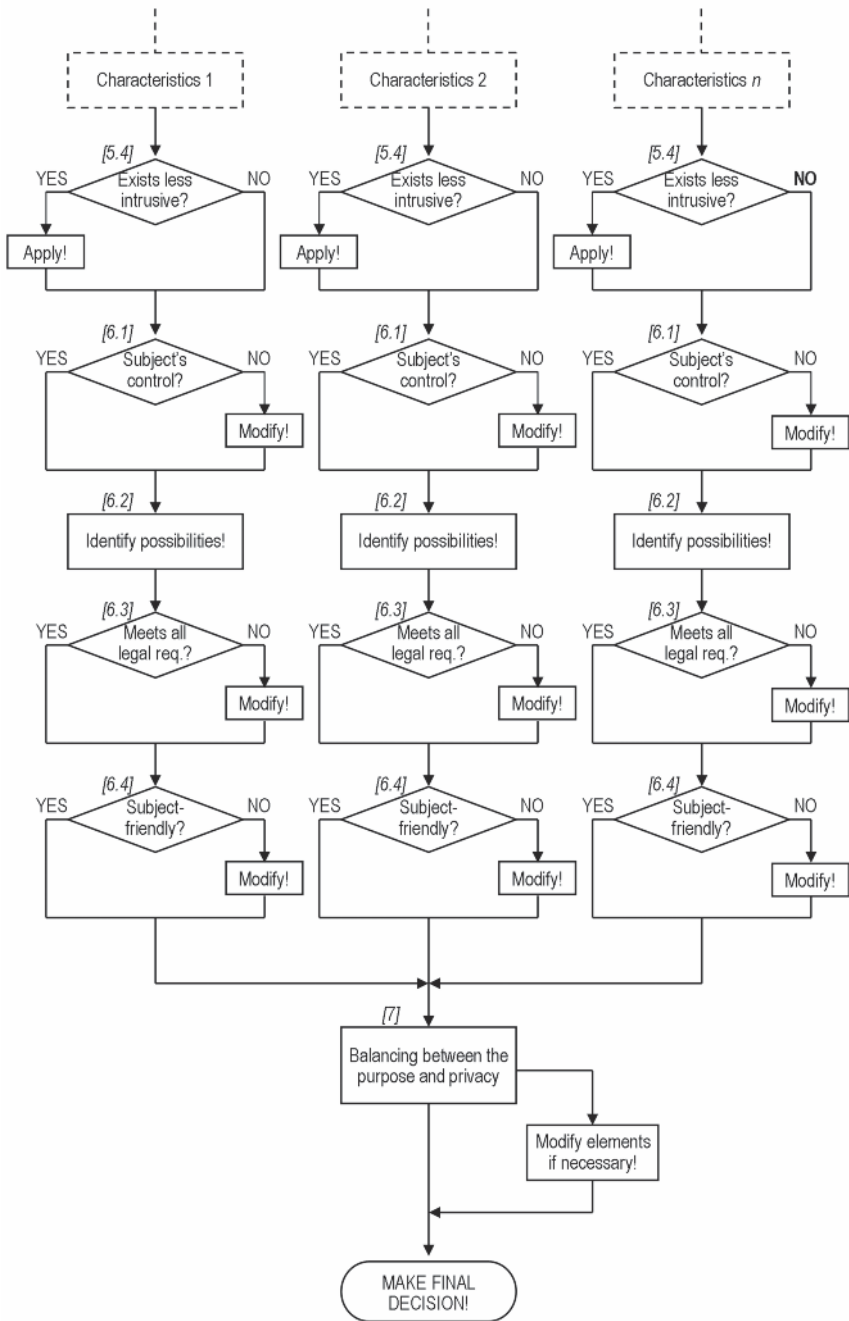
Figure 9.3b The steps of surveillance–related decision–making inspired by the test of
proportionality (Part 2)

6.3 Do these possibilities meet all the requirements prescribed by law?
     Certain rights of data subjects can be expressly regulated by legal provisions. For example, an opportunity shall be provided where the data subjects may personally view the recordings made and stored of their personal data, at the data controller's official premises, and make statement about the manner in which they wish to exercise their rights. The operator of a CCTV system has to obey this regulation.

6.4 Besides fulfilling the legal requirements, are the above mentioned measures (Questions 6.1–6.2) carried out in a 'data subject friendly' way?
     Legal provisions usually leave some latitude for the implementation, i.e. the concrete manner of the fulfilment of obligations.

7   This is the ultimate balancing between the purpose identified in Question 3 and the privacy rights.

Summary of the decision support procedure

The above detailed flowchart reflects the logic of the above list of questions, completed with branching points, tasks, loops and termination points (Figure 9.3).

Conclusion

We have seen that the use of the test of proportionality is not merely an issue of legal dogmatics but it is highly relevant in judicial practice. According to our first thesis, by laying more emphasis on the first three phases of the test, the factual subtests, and by applying the necessary methodological rigour, the scope of balancing can be significantly reduced, and the primacy of the trade-off approach superseded. These effects can be further improved by taking our auxiliary suggestions into consideration.

   We have also shown that this methodology, which had originally been developed for the relationship between the state and the citizens, can successfully be transposed into a different environment, namely the decision support procedures relating to the implementation of surveillance measures, which potentially infringe people's privacy. This new environment made it necessary to modify the order and relative weight of the steps in the test and to include detailed questions relating to the characteristics of the planned surveillance measures and their potential privacy implications. Nevertheless, we preserved the fundamental elements of the test of proportionality and the separation of factual and moral arguments. We formulated these methodological steps in the form of questions to be asked by the decision-maker himself. The whole procedure has been illustrated by a detailed flowchart.

   In conclusion, our suggestions, if implemented, make it possible to move away from the security–privacy trade-off both in judicial practice and decision-making environments.

Notes

1 'Balancing privacy and security' results in more than 24 million Google hits in general search, and about 10.000 hits for the exact string.
2 We understand the concept of 'public goods' beyond its narrow economistic usage and include shared societal goods which are essential elements of society itself, see Loader and Walker (2007) or Raab, Jones and Székely (2015).
3 Raab, Jones and Székely (2015) analysed in detail the double-facedness of surveillance in the context of resilience in society.
4 The campaign was led by the Electronic Privacy Information Center (EPIC) and supported by a host of other NGOs, including religious organizations, see http://epic.org/privacy/airtravel/backscatter/
5 Privacy and Security Mirrors, www.prismsproject.eu The project declared as one of its main research ambitions to critically analyse the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security. The present study is the outcome of a spin-off research originally started in PRISMS.
6 See the study of van den Broek *et al.* (2016) in Chapter 1 of this volume.
7 In the US conflicting fundamental rights are typically handled with the methodology of balancing between the rights, while the European approach is the use of the test of proportionality. The two end in analytically similar results and perform similar functions, and, leastwise, the final subtest of proportionality, i.e. proportionality in the strict sense, is analogous to the American balancing. The principal difference between the two methodologies is that the European approach, before arriving to the step of the ultimate balancing, follows a more analytical structure. For more details see Cohen-Eliya and Porat (2010).
8 There are a number of studies that have found security purpose CCTV systems to be ineffective. For a collection of these studies see: www.no-cctv.org.uk/caseagainst/reports.asp.
9 From the most current jurisprudence see Barak (2012).
10 It has to be noted that in one of its recent judgments on a privacy vs. security issue the European Court of Justice applied the test of proportionality in a very detailed and dogmatically rigorous manner. See judgment in joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others of 8 April 2014, on the invalidity of the Data Retention Directive.
11 Robert Alexy illustrates the balancing between the two conflicting principles with an indifference curve as it is used in economics (Alexy, 2010, 102–105).
12 Several well-known definitions or typologies of privacy attempt to grasp the essence of privacy as information privacy: the right to control knowledge about oneself (Fried, 1968, p. 475), the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others (Westin, 1967, p. 7), or, from among the recent studies, the 'seven types of privacy' (Finn *et al.*, 2013) also include information-centric elements, such as privacy of communication and privacy of data and image. On the distinction among different aspects of privacy and defining information privacy, see Solove *et al.* (2006).
13 On the relationship between privacy and data protection in contemporary European law, see Kokott and Sobotta (2013), or González Fuster (2014). See also González Fuster's study in Chapter 10 of this volume.
14 For example *Malone v. the United Kingdom*, no. 8691/79, 2 August 1984, *Copland v. the United Kingdom*, no. 62617/00, 3 April 2007.
15 For example *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, *Uzun v. Germany*, no. 35623/05, 2 September 2010.
16 For example *Leander v. Sweden* no. 9248/81, 26 March 1987, *S and Marper v. the United Kingdom*, no. 30562/04, 4 December 2008.

17 See, for example, *Glor v. Switzerland*, no. 13444/04, § 52, ECHR 2009; *Tysi c v. Poland*, no. 5410/03, § 107, ECHR 2007-I; *Hadri-Vionnet v. Switzerland*, no. 55525/00, 14 February 2008, § 51; *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III; and *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, § 66, ECHR 2008.

18 See, for example, *B. v. France*, 25 March 1992, Series A no. 232-C, § 63; *Burghartz v. Switzerland*, 22 February 1994, Series A no. 280-B, § 24; *Dudgeon v. the United Kingdom*, 22 October 1981, Series A no. 45, § 41; and *Laskey, Jaggard and Brown v. the United Kingdom*, 19 February 1997, *Reports* 1997-1, § 36.

19 See, for example Case of *Burgartz v. Switzerland,* no. 16213/90, opinion of the Commission, p. 37, § 47, and *Friedl v. Austria*, 31 January 1995, Series A no. 305-B, opinion of the Commission, § 45.

20 See *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B, pp. 33–34, § 29, and *Halford v. the United Kingdom,* no. 20605/92, 25 June 1997, § 44.

21 See *von Hannover v. Germany (No. 2),* nos. 40660/08 and 60641/08, § 95.

22 See *Rotaru v. Romania*, no. 28341/95, §§ 43–44, ECHR 2000-V, *P.G. and J.H. v. the United Kingdom* no. 44787/98, 25 September 2001, § 59.

23 *P.G. and J.H. v. the United Kingdom*, § 59.

24 Example from case *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, no. 13178/03, 12 October 2006, § 79.

25 See for example *Nada v. Switzerland*, no. 10593/08, 12 September 2012, § 174.

26 *Erdem v. Germany*, no. 38321/9, 5 July 2001, § 60.

27 *Nada v. Switzerland*, § 174.

28 *Liu v. Russia (No. 2),* no. 29157/09, 26 July 2011, § 80.

29 *Erdem v. Germany*, § 60.

30 *Drakšas v. Lithuania*, no. 36662/04, 31 July 2012, § 58.

31 *Nada v. Switzerland*, § 174.

32 Example from *Ciubotaru v. Moldova*, no. 27138/04, 27 April 2010, § 55.

33 Example from case *Mubilanzila Mayeka and Kaniki Mitunga v. Belgium*, § 79.

34 The same is true in general, regardless of the connection of purposes with security (van Dijk *et al.*, 2006, p. 340).

35 It deserves noting, however, that when dealing with privacy violations by the state through (mass) surveillance, the Court is willing to relax its focus on individual rights and interests. In some cases the Court is willing to accept claims based not on actual and concrete harm but on hypothetical harm or 'reasonable likelihood' (e.g. in *Malone v. the United Kingdom*). In other cases the Court recognizes the 'chilling effect' or the future harm as the basis for a claim (see for example *Marckx v. Belgium*). In certain cases the Court is even willing to accept *in abstracto* claims, despite the general inadmissibility of claims regarding the legality and legitimacy of laws and policies (see *Liberty and others v. the United Kingdom*). See van der Sloot (2016).

36 Van Dijk *et al.* (2006) p. 335.

37 *Leander v. Sweden*, no. 9248/81, 26 March 1987, §§ 58–59.

38 E.g. *Klass and Others v. Germany,* § 42.

39 In the field of security such technologies are called surveillance-oriented security technologies (SOST). Naturally, there exist a range of security technologies, which are not surveillance-oriented.

40 *Uzun v. Germany,* §§ 78–80.

41 *Klass and Others v. Germany*.

42 *Nada v. Switzerland*, § 186. The judgment refers to the years of the fear of terror after 9/11.

43 *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, 6 June 2006, § 90.

44 *Liu v. Russia (No. 2)*. Procedural guarantees were the most significant element of the decision in cases *Klass and Others v. Germany* and *Leander v. Sweden*.

45 See for example the Handbook on Increasing Resilience in a Surveillance Society, developed by the IRISS consortium, available at http://irissproject.eu/?page_id=9

References

Alexy, R. (2010) *A Theory of Constitutional Rights.* Oxford: Oxford University Press.

Barak, A. (2012) *Proportionality. Constitutional Rights and their Limitations.* Cambridge: Cambridge University Press.

Broek, T. van den, Ooms, M., Friedewald, M., van Lieshout, M. and Rung, S. (2016) 'Privacy and security – citizens' desires for an equal footing'. In: Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., and Peissl, W. eds. *Surveillance, Privacy and Security.* Abindgon; New York: Routledge, 15–35.

Čas, J., Strauß, S., Amicelle, A., Ball, K., Hallinan, D., Friedewald, M. and Székely, I. (2014) 'Social and economic costs of surveillance'. In: Wright, D. and Kreissl, R. eds. *Surveillance in Europe.* Abingdon; New York: Routledge, 211–258.

Cohen-Eliya, M. and Porat, I. (2010) 'American balancing and German proportionality: The historical origins', *International Journal of Constitutional Law,* 8(2): 263–286.

Dijk, P. van, van Hoof, F., van Rijn, A. and Zwaak, L. eds. (2006) *Theory and Practice of the European Convention on Human Rights.* Antwerp; Oxford: Intersentia.

Finn, R.L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy'. In Gutwirth, S., Leenes, R., de Hert, P. and Poullet, Y. eds. *European Data Protection: Coming of Age.* Dordrecht: Springer Science+Business Media B.V., 3–32.

Fried, C. (1968) 'Privacy', *Yale Law Journal,* 77: 475–493.

Germain, S., Dumoulin, L. and Douillet, A.-C. (2013) 'A prosperous "business": The success of CCTV through the eyes of international literature', *Surveillance and Society,* 11(1/2): 134–147.

González Fuster, G. (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* New York; Dordrecht: Springer.

Groombridge, N. (2008) 'Stars of CCTV? How the Home Office wasted millions – a radical "Treasury/Audit Commission" view', *Surveillance and Society,* 5(1): 73–80.

IRISS Consortium (2014) 'Handbook on increasing resilience in a surveillance society: key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public'. IRISS project, EC Grant Agreement No. 285593, available at http://irissproject.eu/?page_id=9 (accessed November 3, 2016).

Kokott, J. and Sobotta, C. (2013) 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law,* 3(4): 222–228.

Loader, I. and Walker, N. (2007) *Civilizing Security.* Cambridge: Cambridge University Press.

Norris, C. (2012) 'The success of failure. Accounting for the global growth of CCTV'. In Ball, K., Haggerty. K.D. and Lyon, D. eds. *Routledge Handbook of Surveillance Studies.* London and New York: Routledge, 251–258.

Raab, C. (1999) 'From balancing to steering: new directions for data protection'. In Bennett, C.J. and Grant, R. eds. *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, 68–93.

Raab, C., Jones, R. and Székely, I. (2015) 'Surveillance and resilience in theory and practice', *Media and Communication,* 3(2): 21–41.

Sloot, B. van de (2016) 'Is the human rights framework still fit for the Big Data era? A discussion of the ECtHR's case law on privacy violations arising from surveillance activities'. In Gutwirth, S., Leenes, R. and De Hert, P. eds. *Data Protection on the Move.* Dordrecht: Springer, 411–436.

Solove, D.J., Rotenberg, M. and Schwartz, P.M. (2006) *Privacy, Information and Technology.* New York: Aspen Publishers.

Vermeersch, H. and De Pauw, E. (2016) 'The acceptance of new security oriented tech-
    nologies, a "framing" experiment'. In: Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R.,
    and Peissl, W. eds. *Surveillance, Privacy and Security*. Abindgon; New York: Routledge,
    52–70.

Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum.

Wright, D. and De Hert, P. eds. (2012) *Privacy Impact Assessment*. Dordrecht: Springer.

Wright, D. and Raab, C. (2012) 'Constructing a surveillance impact assessment', *Computer
    Law & Security Review,* 28(6): 613–626.

10 The legal significance of individual choices about privacy and personal data protection[1]

Gloria González Fuster and Serge Gutwirth

Introduction

This chapter looks into the security/privacy relationship through a legal prism. It is not about the *legal acceptability* of security measures, but rather about their legality. Policy makers in the European Union (EU) taking security-related decisions are obliged to ensure all adopted measures are compliant with fundamental rights requirements. It is true that they might also, additionally, be interested in questioning whether (some) individuals might perceive such decisions as impacting fundamental rights negatively or not.[2] These are however two different issues, and should not be conflated: one regards compliance with fundamental rights, while the other is about *perceptions of compliance*. Whereas respect for fundamental rights is unquestionably a legal issue, perceptions of compliance might be described as a societal consideration, potentially addressed from an economic perspective in terms of a possible negative impact on the commercialisation of technological products.[3]

This chapter investigates how legal compliance, as determined by judges and courts, proceeds to take into account individual choices referring to privacy and personal data protection in relation to security.[4] In other words, it is concerned with how legal decisions are taken using or ignoring individual choices related to privacy and personal data protection. As such, it does not seek to directly investigate whether decision makers might take into account these individual preferences when defining related security, technology or research policies,[5] or even when legislating.[6] The chapter will nonetheless refer to how positive law sometimes appears to integrate the consideration of individual choices.

Individual choices can manifest themselves independently – as a single, personal choice – or in conjunction with other individual preferences. In the latter case, a sum of individual choices can take the shape of a perceived public opinion, or at least of a certain public opinion, that is, representing the opinion of a certain public. This contribution takes into consideration these two possibilities, giving particular attention to situations in which the endorsement of the choices of some individuals might appear to be in conflict with the choices of other individuals.

From a conceptual view, individual choices may be regarded as both reflecting and informing individual preferences. In relation to the right to respect for private life and personal data protection, individual choices and preferences might be

pictured as globally subsumed under the term 'privacy concerns'. These 'privacy concerns' include attitudinal aspects, related to what people perceive, feel and think; cognitive aspects, related to what people know and the information they are provided with; and practical or behavioural aspects, related to what people do, particularly in the cases where choice is actually effectively in their hands (Oliver-Lalana and Muñoz Soro, 2013).[7] All these dimensions are of course interrelated, and influence each other, but might also be seemingly discordant. Individual actions and decisions related to privacy and personal data protection are always multidimensional, and sometimes inconsistent and contradictory (Muñoz Soro and Oliver-Lalana, 2012: 41). In fact, from that perspective, it would be more appropriate to speak of 'dividuals'.

An example where ignorance of the issues at stake seems to directly affect practical decisions taken by individuals on privacy-related issues can be found in the context of fingerprinting of migrants in application of EU law. The European Commission has observed that in some cases migrants who should be fingerprinted in accordance with applicable laws do not receive a clear explanation of this fact and of the legal consequences linked to their possible refusal from the competent authorities. As a result, some of the uninformed migrants decide to refuse being fingerprinted without knowing that, where they have not yet applied for asylum, their refusal could be treated as an indication that they are likely to abscond, and become an argument used to justify their detention (European Commission, 2014: 4).

The chapter first examines the principles guiding the relation between fundamental rights and individual choices. This is followed by a study of the significance of individual choices for the adjudication of the right to respect for private life, and for the adjudication and regulation of the right to personal data protection. Finally, some of the key tensions of the integration of individual choices in EU personal data protection law are discussed.

General principles of fundamental rights protection

In the EU, the relationship between security, privacy and personal data protection is most critically played out at the level of fundamental rights (González Fuster *et al.*, 2014). It is thus necessary to open up this reflection on the legal significance of individual choices in the area by looking into the very notion of fundamental rights.

Rights of all

Fundamental and human rights aim to protect everybody – all natural persons. They are recognised as such because they are considered to be rights of the highest value, to which all individuals are entitled. In the system of the Council of Europe, this idea is documented by the fact that the European Convention on Human Rights (ECHR) systematically refers to 'everyone' (even individuals who are not citizens of the States party to the Convention) as the subject of the rights

established by its provisions: for example, Article 8 of the ECHR, on the right to respect for private and family life, states that '[e]veryone *has the right to respect for his private and family life, his home and his correspondence'*. Article 34 of the ECHR, mirroring this approach, sets out that 'any person' might file an application before the European Court of Human Rights (ECtHR) claiming to be the victim of a violation of the rights it sets forth. Similarly, the Charter of Fundamental Rights of the EU asserts in its Article 7 that *everyone* has the right to respect for his or her private and family life, home and communications, while its Article 8(1) establishes that *everyone* has the right to the protection of personal data concerning him or her.

The fact that everybody is entitled to the enjoyment of fundamental rights directly implies that those rights are not exclusively destined to protect the majority of individuals, but also any members of possible minorities, both in numerical and cultural terms. Those whose choices are in conflict with the choices of the majority cannot be deprived of protection. On the contrary, typically it will be precisely those whose personal choices differ from the choices of the majority who will be most likely to seek protection in terms of their fundamental rights and freedoms. Fundamental rights protect individuals against John Stuart Mill's proverbial 'tyranny of the majority'. The majority may actually be regarded as 'naturally preserved' by the very social strength of its own normality; 'normal persons', by their condition of being normalised, enjoy a sort of shelter that people living marginal lives, dissidents and minorities in general simply lack (Díez-Picazo, 2013: 57). Freedom of expression would not make much sense if it only protected expressions of common ideas.

Translated into the specific area of privacy and personal data protection this notably entails that the right to privacy and to personal data protection must aim to protect everybody as opposed to just people with normal or average 'privacy concerns'. In reality, it is probably those with singular and extraordinary 'privacy concerns' that will be in particular need of legal protection, and it is also for them that the mentioned rights should be effectively implemented.

Rights protected with special safeguards

Fundamental and human rights are typically given an especially high status in European legal orders, which aims to preserve them from some of the oscillations of the will of the majority as represented and enacted by the legislator. This special rank is also derived from the human rights obligations originating in the ratification of international treaties and agreements, such as the ECHR. In the EU, Member States sometimes condition the adoption of norms restricting the exercise of fundamental rights and freedoms to special legislative requirements, and can provide for reinforced judicial control whenever fundamental rights are at stake. This can imply, for instance, that legal norms formally backed up by the legislator might however be declared null and void by the judiciary due to a violation of constitutionally protected rights and freedoms.

This shielding of fundamental rights and freedoms from the will of the majority through judicial review is grounded in an acknowledgement of the fact that the

rights of minorities are often violated with the majority's explicit or implicit approval. The shielding must also however be linked to another basic feature of fundamental rights, which is their dual dimension as being regarded by law as valuable both subjectively and objectively (Díez-Picazo, 2013: 55). Fundamental rights have a subjective dimension insofar as they aim to protect concrete individuals, but they also have an objective dimension in the sense that they represent foundational elements of constitutional democratic states. Owing to this objective dimension, they must be protected and promoted by public authorities regardless of the particular preferences of few (or many) individuals.

Limited possibilities of waiver

Another attribute derived from the basic premise according to which fundamental and human rights are recognised as being of the greatest importance for the legal order establishing them is that, in principle, individuals cannot relinquish them. It would be paradoxical for any legal order to place at its summit a selected set of rights and freedoms, envisioned as subjectively and objectively essential, and then to confer to individuals the possibility to renounce to them on the basis of personal choices. Establishing a general possibility to relinquish fundamental and human rights could be understood as an indication of accepting to give away a series of guarantees that are claimed to be essential. Renouncing fundamental and human rights, or even to some specific rights or freedoms, shall thus in general be regarded as legally inadmissible. Individuals cannot, for instance, decide to renounce their personal freedom and accept slavery, or to give up their freedom of expression and condemn themselves to eternal silence (Díez-Picazo, 2013: 137).

   This does not mean, however, that individuals are obliged to exercise their fundamental rights and freedoms in all cases and under all circumstances. As a matter of fact, a duty to exercise these rights and freedoms can never be imposed: individuals may always choose to refrain from reacting to a violation of any of their rights. The prohibition of a global waiver of fundamental rights coexists with the recognition of individual freedom, and thus law attempts to strike a balance between the autonomy of the individual and the State's obligation to protect fundamental rights (for a discussion of the issue of waiver in these terms, see: De Schutter, 2014).

   As a result of the prohibition of general waiver of rights, any exercise of a fundamental right must be considered legitimate and valid regardless of any possible previous commitment stating that a right would not be used (Díez-Picazo, 2013: 139). Individuals must remain free to decide to exercise their rights, and thus any general statement in an opposite sense is to be treated as legally inconsequential. What could happen, nonetheless, is that by first announcing that the intention to renounce exercising a right and later deciding to exercise it, individuals generate negative consequences for a third, and thus such a decision could, in certain cases, be subject to compensation.

   Another important limitation of the waiver of fundamental rights is that it is never possible to relinquish exercise in favour of the State. Public authorities cannot impose, support or accept a waiver of this kind, which would go against one

of the basic functions of fundamental rights in general, that is, to limit the power of public authorities and through 'horizontal effect', of other actors (Díez-Picazo, 2013: 138). This is particularly pertinent in relation to the right to respect for private life, commonly envisaged as located at the very heart of individual freedom and aiming to ensure individuals are free from arbitrary interference by a public authority (or by others). The right's classical conception as devising an abstract space that the State cannot penetrate would be in full contradiction with granting to such State the possibility to put any kind of pressure on individuals to surrender this protection.

Individual choices in the adjudication of privacy

Moving to the issue of how individual choices operate specifically in the adjudication of the right to respect for private life, we shall now focus on the case law of the ECtHR on Article 8 of the ECHR – in search of insights to illuminate the importance of individual choices for defining the relationship between security, privacy and personal data protection.

The ECtHR's case law is of special interest due to the Strasbourg's Court's emphasis on the need to interpret the Convention in a dynamic way, also taking into account changes in social attitudes (Harris *et al.*, 2014: 8). The ECtHR famously stressed in 1978 that the European Convention is 'a living instrument' that 'must be interpreted in the light of present-day conditions'.[8] The Court, for instance, inferred that Article 8 of the ECHR encompasses an obligation not to discriminate against children born out of wedlock after observing that laws in the great majority of Member States of the Council Europe had evolved and were evolving in such a direction.[9]

Individual perceptions and the scope of private life

One of the ways in which individual choices can play a role in the adjudication related to the right to respect for private life is by affecting the construction of the notion of 'private life', which has never been defined or thoroughly circumscribed by the ECtHR (Harris *et al.*, 2014: 525). Delimiting the contours of 'private life' is decisive to determine the scope of Article 8 of the ECHR.

Generally speaking, law can approach the delimitation of this notion in two distinct ways, either by granting a wide discretion to individuals to decide what they wish to keep protected under such a term, or rather by following material criteria determining whether something should be protected or not regardless of the particular wishes of the individual affected (Díez-Picazo, 2013: 281). In the first perspective, something should be viewed as private where that is the wish of those concerned; in the second, something should be protected as private can and should be delimited on the basis of objective factors irrelevant of individual wishes. Following the first perspective can be problematic both in the cases where individuals do not wish to have any protection at all (despite the objective dimension of the right), and in situations where they desire extensive protection.

The ECtHR has generally considered that what needs to be protected under the right to respect for private life cannot vary completely from one person to another merely depending on their personal wishes, and that there is a certain minimum to be necessarily protected to ensure individuals' dignity and quality of life. The Court has stressed that 'private life' must be understood as a broad term, encompassing a zone of interaction with others, even in a public context[10] and it has put forward a number of elements to be taken into account to determine if a person's private life is affected when people are outside their home or private premises, such as the systematic or permanent record of information about individuals.[11]

The Strasbourg Court has repeatedly detached itself from the so-called 'expectations of privacy' doctrine. This doctrine, imported from the United States (US), conditions the existence of a violation of somebody's privacy to the requirement that the individual affected was actually legitimately expecting to enjoy privacy protection. The Court has observed that, in order to determine whether a measure constitutes an interference with the right to respect for private life, a person's reasonable expectations as to privacy may be a significant, but not necessarily conclusive, factor.[12] The ECtHR, therefore, does not condition the recognition of an interference with the right to respect for private life to the fact that the individual had actually any concrete expectations of privacy. The Court, nonetheless, sometimes takes into account whether actions such as the publication of recorded material occurs in a manner or degree that goes beyond what was normally foreseeable; if that is the case, this may be considered as an important element to regard the action as falling under the scope of the right to respect for private life.[13]

All in all, it can be deduced that there is no need to prove the existence of a general expectation of privacy in a concrete circumstance to actually be granted the right to obtain privacy protection. Nevertheless, individuals' expectations in terms of anticipated limited use of personal information may be a significant factor in determining whether there has been an interference with their fundamental rights. The Court, therefore, appears to grant only a limited significance to individual preference in such matters, preferring to rely on objective to criteria to determine the possible existence of interferences with the right to respect for private life under Article 8 of the ECHR.

Also in relation to other rights set out by the ECHR, the Strasbourg Court has been reluctant to grant any major relevance to societal views for the determination of the scope of the right protected. For instance, in 1978 the Strasbourg Court observed that the fact that birching of young persons had many advantages according to the local public opinion of the Isle of Man was irrelevant to the question whether such birching constituted inhuman and degrading treatment.[14]

Can public perceptions legitimise interferences?

A different issue is whether some public perceptions or choices may play a role in the legitimisation of interferences with the rights of the ECHR, and concretely with the right to respect for private life of its Article 8. This right is indeed one of those enshrined in the ECHR that might be legitimately limited in certain

circumstances and in accordance with certain requirements. When considering applications of individuals who claim their rights under Article 8 of the ECHR have been violated, the Strasbourg Court first examines whether the applicant's rights have been affected, and, if the existence of an interference is indeed established, it then turns to the question of whether the restriction can be regarded as permissible.

To be permissible, restrictions of the rights contained in Article 8 of the ECHR must be 'necessary in a democratic society' for achieving one of the aims listed in the Article's second paragraph.[15] The ECtHR has held that the requirement of being 'necessary in a democratic society' does not mean that measures constituting interferences must be 'absolutely necessary' or 'indispensable', but it has equally underlined that it is not enough for measures to be merely 'useful' or 'desirable'.[16] In the Court's view, for an interference to be 'necessary in a democratic society' it must correspond to a 'pressing social need'. The requirement of amounting to a 'pressing social need', however, does not imply that interferences must be approved be the majority of society. Two important judgments throw light on the role granted to public perceptions for the possible justification of interferences with the rights protected under Article 8 of the ECHR.

The first, *Dudgeon v UK,* dates from 1981 and was about the criminalisation of male homosexual acts in Northern Ireland.[17] In this case, the ECtHR pointed out that this prohibition concerned a most intimate aspect of private life, and, therefore, could only be justified for particularly serious reasons. The Strasbourg Court argued that some forms of legislation could be regarded as 'necessary' to protect particular societal groups and 'the moral ethos of society as a whole', but added that any measures needed nevertheless to remain within the bounds of what might be regarded as strictly necessary to accomplish the aims pursued.[18] The Court noted that it was 'relevant', in order to assess compliance with the requirements of Article 8(2) of the ECHR on the legitimacy of interferences, to examine 'the moral climate in Northern Ireland in sexual matters', which encompassed 'a genuine and sincere conviction shared by a large number of responsible members of the Northern Irish community that a change in the law would be seriously damaging to the moral fabric of society'.[19] These elements, although relevant, were nevertheless not sufficient according to the Court to justify the maintenance in force of the impugned legislation insofar as it had the general effect of criminalising private homosexual relations between adult males capable of valid consent.[20] Indeed, they did not amount by themselves to a proof that there was a *'pressing social need'* to regard such male homosexual acts as criminal offences.[21] In this context, the Court also noted that the 'democratic society' to which alludes the requirement of being 'necessary in a democratic society' bears as hallmarks tolerance and broadmindedness.[22]

In the second judgment, *Smith and Grady v UK*, of 1999, the ECtHR addressed the investigation into and subsequent discharge of personnel from the armed forces on the basis of their homosexuality.[23] Here, the Court notably made explicit that the measures at stake could not be justified on the basis of social negative attitudes towards homosexuals. In its defence, the UK government had put forward a report allegedly expressing the general views of the personnel on the issue, but the Court

described such a report as documenting negative attitudes of heterosexual person-nel towards those of homosexual orientation which 'ranged from stereotypical expressions of hostility […] to vague expressions of unease about the presence of homosexual colleagues'.[24] The Court added that, to the extent that these negative attitudes expressed 'a predisposed bias', they could not be considered to amount to sufficient justification for the interferences with the applicants' 'any more than similar negative attitudes towards those of a different race, origin or colour'.[25] Doing so, the ECtHR unambiguously declared it simply irrelevant for the justifi-cation of interferences with Convention rights these categories of negative attitudes.

Individual choices and European personal data protection

Entering into the discussion of the relationship between personal data protection and individual choices, (construed as encompassing individual attitudes, knowledge and practices) there are a few general observations that can be advanced. First of all, it must be noted that the EU legislator often appears to rely on a vision of individ-uals as 'data subjects', that is, as subjects of the right to personal data protection, that are poorly informed and prone to take wrong decisions (see notably: González Fuster, 2014b). This vision is sometimes illustrated by the image of individuals that are confused up to the point of ignoring that the services that they use, and that they imagine to be free services, are as a matter of fact services that they are actually paying for, not with money but through the provision of their own personal data.

This viewpoint contrasts but coexists with a second perspective, according to which data subjects must nevertheless be considered as being in a position allow-ing them to decide freely on whether they should consent or not to certain personal data processing practices, at least in some circumstances. This idea is firmly entrenched in EU personal data protection, through the notion of consent.

The role of consent

Under current EU personal data protection rules, individual consent can operate as one of the grounds rendering personal data processing activities lawful.[26] The provision of the Charter of Fundamental Rights of the EU on the right to personal data protection, Article 8, explicitly refers to consent by establishing that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[27] The explicit reference to consent made in this provision actually concedes to this ground a symbolically privileged position among all other possible legitimate grounds for personal data processing detailed in EU secondary law.

Consent may however operate as a legitimate basis for personal data processing only in some circumstances, as for it to be valid data subjects must have been given a genuine and free choice and be subsequently able to refuse or withdraw consent without detriment. Despite this limitation, through the notion of consent EU personal data protection law appears to grant great relevance to individual choice.

If the major exception to the validity of consent is indeed that it shall not be valid when individuals have no real choice, this could be seen as implying that whenever they do have a choice, their choice should be taken into account.

The literature has discussed widely whether consent, as it functions in everyday situations, actually reflects the true choices of individuals or is performing independently or against such choices (Oliver-Lalana and Muñoz Soro, 2013: 160).[28] It must be stressed that in order to be valid, consent must be informed, which means that data subjects should have been appropriately informed about the specific purposes of the data processing operations to which they are consenting. Nevertheless, it is questionable whether in light of the general misinformed condition of data subjects (as discussed above), and despite the absence of any real time information provided, they could still be regarded as being informed enough as to provide fully informed consent.

The widespread use of consent as a legitimising basis for personal data processing activities and its known problems may lead one to think that, instead of allowing the expression and enforcing of individual choices, it rather ends up covering a waiver to any real possibility of effective control. This has notably led the doctrine to refer to consent as a myth (Oliver-Lalana and Muñoz Soro:167; see also Gutwirth, 2012). Despite these criticisms, the legislative package for the review of EU personal data protection law introduced in 2012 by the European Commission (2012a, 2012b and 2012c) confirmed and reinforced the prominence of consent, supported by EU institutions as contributing to the 'empowerment' of data subjects (Oliver-Lalana and Muñoz Soro, 2013: 164).

The case law of the Court of Justice of the EU (CJEU) offers some insights on the significance of individual choices in EU personal data protection law, and in particular in relation to consent. Particularly relevant is the *Deutsche Telekom* judgment,[29] of 2011, concerning the obligation placed on an undertaking assigning telephone numbers to pass to other undertakings data in its possession relating to the subscribers of third-party undertakings. In this ruling, the Luxembourg Court examined a provision of Directive 2002/58/EC[30] giving to subscribers of telecommunication services the opportunity to determine whether their personal data shall be included in public directories.[31] The Court declared that this provision did not grant to subscribers a selective right to decide in favour of certain providers: by consenting to have their data being published in a directory with a specific purpose, individuals lose standing to object to the publication of the same data in another, similar directory.[32] *Deutsche Telekom* is revealing as it appears to grant to individual choices a real impact, but an impact nevertheless limited in scope. Individuals might accept or refuse a processing of personal data (in that specific case, the publication of personal data in a directory), but cannot decide who shall be responsible for such processing (they cannot accept the processing only on the condition that it takes place under the control of a certain company, and oppose it if it is carried out by another).

Other judgments of the CJEU provide only glimpses of the role that consent is supposed to play in EU personal data protection law. A particularly puzzling example is the ruling in *Volker und Markus Schecke and Eifert*, of 2010.[33] In this case, the

Luxembourg Court dismissed the possibility that the processing of personal data at stake (namely, the online publication of beneficiaries of EU funds) was grounded on consent, noting that it was based instead on an obligation imposed by law, law which nevertheless constituted an interference with the EU fundamental right to personal data protection that had to comply with the limitations imposed by the horizontal provisions of the EU Charter.[34] What is striking, however, is that in this ruling the Court appeared to treat consent as a possible way not only to legitimise personal data processing as such, but rather as a means to actually set aside the possibility that an interference with the EU fundamental right to the protection of personal data ex Article 8 of the EU Charter had taken place at all.[35] This could be read as implying, *a contrario*, that whenever data subjects have consented to a particular data processing operation, the operation cannot be regarded as an interference with their fundamental right to personal data processing[36] – which would be highly problematic.

Choosing between individual choices and the public interest

There is however still another noteworthy judgment of the CJEU on the legal significance of individual choices for EU personal data protection. The ruling *Google Spain*, of 2014,[37] concerns the possible tensions between a particular individual choice and the potential interest of the public in opposing such choice. The CJEU addressed indeed the issue of whether data subjects have a right to request that any list of results displayed following a search made on the basis of their name does not display some information relating to them that is inadequate, irrelevant or no longer relevant. The Court asserted that data subjects have indeed such a right, in the light of Articles 7 and 8 of the EU Charter, and underlined that as a general rule this right overrides the right of the general public in having access to that information when carrying out a search using the data subject's name.[38]

This dominant role granted to the individual choice to have some information removed from a list of results in front of the potential public preference to have the information preserved is, nevertheless, not asserted with a general character, but rather as a presumption that might be contested and possibly invalidated. The Luxembourg Court observes in this sense that the overriding of the right of the general public in having access to the information upon the search on the data subject's name can in some cases not take place, if special conditions apply. That would be the case, the Court notes, if it appeared that for particular reasons, such as the role played by the data subject in public life, the interference with their fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[39]

The views of data subjects in data protection impact assessments

Another way in which EU personal data protection law will in the future integrate a consideration of individual choice is through 'data protection impact assessments'. The General Data Protection Regulation adopted by the European Parliament and

the Council in April 2016[40] foresees establishing the obligation to carry out 'data protection impact assessments' in certain circumstances. As a general rule, an assessment shall be carried out whenever 'a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'.[41] In the context of this assessment, and '[w]here appropriate', the data controller 'shall seek the views of data subjects or their representatives on the intended processing'.[42]

Concluding thoughts

This chapter has shown that, legally speaking, the significance of individual choice for defining the relation between security, privacy and personal data protection has multiple facets. Globally speaking, law appears to be ready to fully support personal choices, even choices that go against the choices of other individuals, however numerous or persuasive these might be. It will, for example, decide to ignore some societal opinions that are perceived as going against the basic principles of inclusiveness of democratic societies. Law can also, nonetheless, pursue the protection of individuals also against their own individual choices, and for this purpose reduce or limit the relevance of their own preferences.

Against this complex background, the role granted to consent by EU personal data protection law is noteworthy for its ambiguousness. This ambiguity can manifest itself in concrete individual decisions, where single acts of consent might appear to go against some established knowledge on the limitations on the waiver of (human) rights. More remarkably, the widespread use and misuse of consent as a ground to process personal data in the EU can also have global consequences for instance via the active use of online social media. In such instances the fact that many individuals appear to 'consent' to some popular data processing practices, is taken as evidence of their preferences or lack of 'privacy concerns'. In a similar vein, policy makers appear to have an increased interest in attempting to appraise the economic value of personal data in the eyes of data subjects, in the understanding that such examination could provide relevant orientations for future policy decision in this area.

In face of these developments, it is crucial to go back to the idea of the multidimensionality of privacy concerns, and to rethink how the limitations imposed by law on the significance of individual choice can be appropriately integrated. As noted, attitudes, knowledge and practices related to privacy and personal data protection cannot be envisaged as independent aspects, because they affect each other. From this viewpoint, one should not focus on trying to assess or calculate individuals' 'personal' preferences in relation to the use of personal data concerning them, or to merely take note of how lightly people appear to consent to certain data processing practices, but rather investigate the factors that determine these preferences and practices, and the relations between them.[43] In other words, instead of acting as if there were some pre-existing personal choices that happen to operate among the current legal landscape for privacy and personal data protection, it

might be necessary to inquire how the current legal landscape shapes attitudes and decisions, and, finally, discuss which kind of preferences and choices it should encourage or discourage (Rouvroy, 2008: 17). The exact legal significance of these choices will afterwards, in any case, shift (back) to the hands of courts and judges.

Notes

1   This chapter is based on a deliverable (5.3) written in the framework of the Privacy and Security Mirrors (PRISMS) research project. For more information, see http://prismsproject.eu/.
2   The importance of this concern is notably developed in: (European Commission, 2012a). See for instance p. 11 referring to public fear provoked by some security measures, or p. 28 stating that security technologies are often perceived as an intrusion of the personal sphere.
3   In this sense, ibid. p. 28.
4   'Law' as primarily understood here is what judges and courts do whenever they rule, rather than legislation. On the specificity of law, see e.g: (Gutwirth, 2015) and (González Fuster and Gutwirth, 2014).
5   On the relation between public debate and technological research, for instance, see (Von Schomberg, 2011: 13).
6   On the use of public opinion shifts to support decisions by policy makers, see, for instance (Dimitris Potoglou *et al.*, 2010).
7   On the limits of gathering knowledge on these dimensions, see for instance: (Szoka, 2009).
8   *Tyrer v UK*, Judgment of the Court (Chamber), of 25 April 1978, § 31.
9   *Marckx v. Belgium*, Judgment of the Court (Plenary) of 13 June 1979, § 61.
10   See, for instance, *Uzun v Germany,* judgment of the Court (Fifth Section) of 2 September 2010, § 43 and case law cited thereof.
11   *P.G. and J.H. v. the UK*, judgment of the Court (Third Section) of 25 September 2001, § 57.
12   Idem.
13   *Uzun,* § 48.
14   *Tyrer,* § 38.
15   That is, national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Art. 8(2) of the ECHR).
16   See notably *Handyside v the UK,* Judgment of the Court (Plenary) of 7 December 1976, § 48.
17   *Dudgeon v UK*, Judgment of the Court (Plenary) of 22 October 1981.
18   *Dudgeon,* § 49.
19   Ibid., § 57.
20   *Dudgeon,* § 61.
21   Ibid., § 60.
22   Ibid., § 53.
23   *Smith and Grady v UK,* Judgment of the Court (Third Section) of 27 September 1999.
24   Ibid., § 97.
25   Idem.
26   This is the general function of consent of EU personal data protection law. It also plays other roles, notably as a means to render lawful the processing of sensitive data, generally prohibited (for this purpose, consent shall be explicit), and consent can also render lawful data transfers to third countries that would be otherwise not allowed.
27   Art. 8(2) of the Charter of Fundamental Rights.
28   On consent in EU personal data protection, see also: (Kosta, 2013).

29 Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland*, Judgment of the Court (Third Chamber) of 5 May 2011.
30 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201, 31/07/2002, pp. 7–47.
31 Art. 12(2) of Directive 2002/58/EC.
32 Deutsche Telekom, § 62.
33 Joined Cases C-92/09 and C-93/09, Judgment of the Court (Grand Chamber) of 9 November 2010, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 2010 I-11063.
34 See notably § 62 and 63.
35 See § 61 and § 64.
36 On the weaknesses of existing CJEU case law on the right to personal data protection, see notably (González Fuster, 2014a).
37 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Judgment of the Court (Grand Chamber) of 13 May 2014.
38 Google Spain, § 97.
39 Idem.
40 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119, 4.5.2016, pp. 1–88.
41 Art. 35(1) of the General Data Protection Regulation. See also 35(3) for specific cases.
42 Art. 35(9) of the General Data Protection Regulation.
43 In this sense: (Rouvroy, 2008: 16).

Bibliography

De Schutter, O. (2014) *International Human Rights Law*, 2nd edition, Cambridge: Cambridge University Press.

Díez-Picazo, L. M. (2013) *Sistema de derechos fundamentales*, Madrid: Thomson Reuters.

European Commission (2012a) *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, COM(2012) 9 final, Brussels, 25 January 2012.

European Commission (2012b) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels 25 January 2012.

European Commission (2012c) *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM(2012) 10 final, 25 January 2012, Brussels.

European Commission (2012d) *Commission Staff Working Paper: Security Industrial Policy, Security Industrial Policy Accompanying the Document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Security Industrial Policy Action Plan for an Innovative and Competitive Security Industry* (COM(2012) 417 Final), SWD(2012) 233 Final, Brussels, 26 July 2012.

European Commission (2014) *Report from the Commission to the European Parliament and the*

Council: Fifth Bi-Annual Report on the Functioning of the Schengen Area 1 November 2013–30 April 2014, COM(2014) 292 final, Brussels, 26 May 2014.

González Fuster, G. (2014a) 'Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection', *Birkbeck Law Review*, 2(2): 263–278.

González Fuster, G. (2014b) 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *IDP Revista de Internet, Derecho y Política*, 19: 92–104.

González Fuster, G. and Gutwirth S. (2014) 'Ethics, Law and Privacy: Disentangling Law from Ethics in Privacy Discourse', *Proceedings of the 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, 23–24 May 2014, Chicago, 1–6.

González Fuster, G., Gurtwirth, S., Somody, B., and Székely, I. (2014) *Consolidated legal report on the relationship between security, privacy and personal data protection in EU law*, PRISMS Deliverable 5.2. Online. Available at: http://prismsproject.eu/wp-content/uploads/2015/02/PRISMS-D5-2-Consolidated-legal-report.pdf (accessed 20 December 2016).

Gutwirth, S. (2012) *Short statement about the role of consent in the European Data Protection Directive*, available at: http://works.bepress.com/serge_gutwirth/80/ (accessed 3 November 2016).

Gutwirth, S. (2015) 'Providing the Missing Link: Law after Latour's Passage', in McGee, K. ed. *Latour and the passage of law*, Edinburgh: Edinburgh University Press.

Harris, D., O'Boyle, M., Bates, E., and Buckley, C., eds. (2014) *Law of the European Convention on Human Rights*, 3rd edition, Oxford: Oxford University Press.

Kosta, E. (2013) *Consent in European Data Protection Law*, The Hague: Martinus Nijhoff.

Lec, S. J. (1974) *My li nieuczesane* (Unkempt Thoughts), Kraków: Wydawnictwo Literackie.

Muñoz Soro, J. F. and Oliver-Lalana, D. (2012) *Derecho y cultura de protección de datos: un estudio sobre la privacidad en Aragón*, Madrid: Dykinson.

Oliver-Lalana, D. and Muñoz Soro, J. F. (2013) 'El mito del consentimiento y el fracaso del modelo individualista de protección de datos', in Valero Torrijos, J. (ed.) *La protección de los datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Cizur Menor: Aranzadi, 153–196.

Potoglou, D., Robinson, N., Kim, C.W., Burge, P., and Warnes, R.(2010) '"Quantifying Individuals" Trade-Offs between Privacy, Liberty and Security: The Case of Rail Travel in UK', *Transportation Research* Part A 44, 169–181.

Rouvroy, A. (2008) 'Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?', augmented version of a chapter published in Stéphanie Lacour (ed.), *La sécurité de l'individu numérisé: réflexions prospectives et international*, Paris: L'Harmattan, 249–278, available at: http://works.bepress.com/antoinette_rouvroy/5 (accessed 3 November 2016).

Szoka, B. (2009) 'Privacy Polls v. Real-World Trade-Offs', *Progress Snapshot*, 5(10), Washington, DC: Progress & Freedom Foundation. Online. Available at www.pff.org/issues-pubs/ps/2009/pdf/ps5.10-privacy-polls-tradeoffs.pdf (accessed 14 November 2016).

Von Schomberg, R. (2011) 'Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields', in: *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields: A Report from the European Commission Services*, Directorate General for Research and Innovation, European Commission, 7–16.

11 The manifold significance of citizens' legal recommendations on privacy, security and surveillance[1]

Maria Grazia Porcedda

Introduction

Academia has grown increasingly sceptical of the trade-off between security and 'privacy rights', but citizens are rarely asked about their views on the matter, a grave omission in the face of the resurgence of terrorist attacks in 2015–2016 and the ensuing temptation to resort to restrictive policies. The SurPRISE project (acronym of SURveillance, PRIvacy and SEcurity), of which this chapter is an expression, consulted citizens on privacy rights, security and surveillance by means of a deliberative methodology. Around 2000 citizens from Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom were invited to explain if and under what circumstances they would be prepared to accept policies and the use of technologies that intrude into their 'privacy'[2] for the sake of increased security, thus effecting surveillance. Moreover, citizens were asked to suggest possible solutions to what they saw as the most pressing issues concerning security, privacy and surveillance. 145 out of 250 recommendations contain a *legal message*.

This chapter focuses on the *legal solutions* proposed by citizens, with two objectives. The first is to disseminate citizens' views. The second is to reflect on citizens' active and fruitful engagement to draw lessons for both research and policy-making. As for research, the events demonstrate that participatory events may benefit empirical research in security-related legal matters, and offer some methodological insight. With regard to policy, while citizens were not consulted directly about current initiatives, their contributions could be an *indirect* litmus test for proposed measures, suggesting that the European Union (hereafter EU) could consult citizens on matters pertaining to the Area of Freedom, Security and Justice (hereafter AFSJ), especially in the light of the importance given by secondary law to citizens' perceptions in relation to security expenditure. Relatedly, embedding deliberative democracy in the decision-making process could give concrete meaning to the Lisbon Treaty's innovations on participation.

The chapter develops as follows. In the first half of the chapter I explain the methodology used to organize the participatory events, and then I present the legal recommendations formulated by European citizens therein. The second half of the

chapter is devoted to the lessons drawn from citizens' direct involvement. After having reflected on the significance of citizens' approach for the trade-off model and the law, I compare citizens' messages with the results of the SurPRISE project, and then move onto discussing the lessons for research and policy-making. I conclude by noting that the enthusiastic drafting of recommendations also suggests that direct consultation may prove useful in the face of problematic choices.

Citizens' legal recommendations on privacy, security and surveillance

After having provided a brief description of the SurPRISE events' methodology, I present the recommendations formulated by citizens in the participatory events as a response to their strongest concerns.

The SurPRISE events' methodology, in brief

Based on scholarly work framing the issues (Kreissl *et al.* 2013; Pavone *et al.* 2013),[3] the SurPRISE project events investigated citizens' understanding and concerns regarding the relationship between security and privacy, analysed through the lenses of different surveillance-orientated security technologies (surveillance technologies for short), which provided concrete examples for discussion. Two sets of interrelated events were conducted: the citizen summits, and the citizen meetings.[4]

The SurPRISE citizen summits were 12 large-scale participatory events involving 1,780 citizens in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom from January to March 2014. The summits were based on a mixed approach combining interactive quantitative and qualitative elements, as well as level-setting tools to enable discussions on a relatively equal footing. Prior to attending the summit, participants received an information brochure, while during the events, a short film was presented for each of the two surveillance technologies discussed.

Quantitative data was gathered through a 106-item survey; citizens answered the questions via keypads linked to an electronic polling system, while the results were projected onto a screen immediately after the polling. As for the qualitative element, participants were divided into groups of 6–8 people and sat at roughly 250 tables facilitated by a moderator, who had been trained for the summit.

In practice, the six-hour long events consisted of three sessions. The first two sessions featured pre-defined questions concerning a specific surveillance technology chosen from deep packet inspection (DPI), smart CCTV or smartphone location tracking (SLT), complemented by discussion rounds relating to each technology. In the last session, participants developed suggestions and recommendations to policy makers at national as well as European level (Strauß 2015).

The SurPRISE citizen meetings were small-scale events involving 190 people in a subset of the countries taking part in the project, namely Denmark, Hungary, Italy, Norway and Spain in June 2014. The meetings aimed at validating the citizen summits' outcomes, as well as further investigating open-ended issues either left

unanswered, or even raised, by the citizen summits. Due to smaller numbers, the events relied more heavily on qualitative methodologies that allowed a more in-depth understanding of citizens' perceptions, attitudes, demands and claims.

Similarly to the large-scale events, participants received an information brochure and sat at tables (26 altogether[5]), where discussions were led by experienced moderators. Citizen meetings used a web-based research tool which was not used in large-scale events, the 'SurPRISE Decision Support System'. Accordingly, note-takers could write down in real time the main points of discussion as well as citizens' recommendations and messages, which were shown on a monitor, thus involving the citizens more. The event lasted three hours and was divided into two sessions. The first round featured technology-neutral discussions about four intro-ductory topics. Subsequently, each table discussed a different surveillance technology (DPI, Smart CCTV, SLT, drones and biometrics) and formulated recommendations (Barland *et al.* 2014; Szénay 2014).

Citizens' acceptance of specific surveillance technologies, as well as the purchase of the trade-off model which results from quantitative data, is discussed in detail in Chapters 4 and 14 of this volume. This chapter presents citizens' views as conveyed through the recommendations made at the citizen summits and meetings (small and large-scale events), which must be seen as complementary events. Occasionally, qualitative elements derived from the reports of table discus-sions are used to add nuance to suggestions contained in the recommendations. In Annex 1 I explain in greater detail the process of elaborating and coding the recommendations.

Citizens' recommendations: law as a solution to real concerns

The recommendations formulated in the course of both citizen summits and meetings offer solutions to concerns expressed by participating citizens (Strauß 2015; Szénay 2014). In this respect, the participatory events unveiled a complex landscape.

Participants distinguish personal safety from national security, a concept difficult to grasp, and are baffled by online security (seen as a Wild West where computer science wisdom is rarely applied). While not necessarily aware that surveillance technologies are used for crime prevention and investigation, they are supportive of such use, so long as it is performed by law enforcement agencies only, which they tend to trust. Participants, in fact, worry more about data processing by commercial actors, whether or not for security purposes, due to their drive for profit. Even if they support surveillance technology-based data processing for public and national security purposes (with varying degrees of intensity depending on the specific surveillance technology), they fear abuses, mostly because of the opaqueness of law enforcement agencies' use of surveillance technologies and uncertainty as to existing legal safeguards, oversight mechanisms and appeal proce-dure against adverse decisions. Participants fear a totalitarian drift, although many avow that they use technology carelessly for convenience. They worry about the stealthy and indiscriminate collection and transfer of personal data, often more in

relation to the future. They fear that surveillance technologies are replacing, rather than supporting, human action, and feel they have no voice in the decision as to how surveillance technologies are used to protect a society (the application, not the technology, is seen as problematic, as is overreliance on it).

Participants understand that surveillance technologies affect privacy, seen as a right that the vast majority cherish, both at the individual and collective level. Citizens think of privacy as an evolving concept, and use terms to describe it that match the legal definitions of the two rights it engenders in the EU: intimacy, the private sphere, seclusion, family, home, personal data (Szénay 2014; Barland *et al.* 2014). Citizens believe that there is a core that should not be intruded upon, and which corresponds to a broad legal definition of sensitive data, as well as data of children and exposed people. Citizens clearly link the enjoyment of privacy to a healthy democracy. They fear that the power of control intrinsic in privacy is fading away, due to fast-paced technological evolution, unmatched by the law, which leaves too many grey areas. The existing law is seen as inadequate because it is not enforced properly, and because of its limited territorial scope: unlike data, it stops at national borders. Concerns are worsened by the opaqueness of data processing activities, naivety of users, and the general ignorance of the law and legal safeguards.

The national reports show variations in the type of legal action recommended, in line with the different cultural traditions of the countries represented in this study, but the same principles are expressed all over Europe, and it is such common requests that are addressed in this chapter, as well as discussed in the Annex (see also Chapters 2 and 12 in this volume). Citizens' legal recommendations can be grouped in six clusters, which are discussed below based on their frequency (for more details and the significance of frequency, see Annex 1).

Better applicable law

Improving applicable law was the first piece of advice for citizens, mentioned 101 times in the law-orientated recommendations (roughly in 40 per cent of total suggestions). Being aware that applicable law, unlike data, stops at the border, participants expressed the need for regulation that follows data in transit, applicable abroad. In this vein, they strongly recommended the adoption of an international treaty establishing minimum standards on privacy and surveillance technologies, as well as the conclusion of an agreement with the US to enforce strong laws on US-based companies. Consequently, data transfers to jurisdictions that do not respect rights should be prohibited. Citizens insisted that the law should apply all over the EU harmoniously, and that it should also address law enforcement.

Specific legal solutions include the adoption of clear legal bases for the use of surveillance technologies, and creating a public registry on data controllers using such technologies. The law should also ensure the embedding of a switch-off button for surveillance options, incentivise the routine use of easy secure storage, and the use of encryption for all services processing personal data. Some warned, however, against law hindering research and innovation.

Transparency and participation

The second most desired request (mentioned in half of the legal recommendations, and in 30 per cent of total suggestions) consists of *transparency*, seen as composed of information, education and accountability.

According to citizens, *information* should be provided by public institutions, such as government, the Ministry of Home Affairs, the police, the Data Protection Authorities (DPAs), municipalities, but also the EU and hospitals. To ensure the widest possible reach, information should be delivered in an intelligible manner not only through established media, like TV and newspapers, but also via new media, viz. the Internet, leaflets, public institutions' websites and YouTube. Some citizens recommended disseminating regulation among the public through comics (akin to the Spanish Constitution).

When asked about the kind of information they wish to obtain,[6] citizens asked for access to a range of information enabling them to understand how surveillance technologies affect themselves and society as a whole, so as to avoid (unwarranted) surveillance. Accordingly, on the one hand they expressed the need to be better aware of their rights, be acquainted with the gist of the applicable law, and identify the pressure groups and lobbies influencing regulation. On the other hand, they called for more clarity in the daily processing of personal data, in particular to be able to understand the purposes of data processing and what information is recorded, e.g. by hospitals but also by the apps/services they use, who manages surveillance technology, and how.

To develop the necessary awareness citizens recommended *continuous education*, both for adults and children. Participants suggested developing specific curricula in school (e.g. as part of science or civic education) complemented by courses organized by municipalities for adults. Technologies that could be used for surveillance, moreover, should be sold with user guides that include warnings on the effects on privacy, and suggestions on how to use them wisely.

Some saw transparency as a precondition for *participation*. Citizens felt their voice should be heard when it comes to the use of surveillance technologies, for instance to decide which surveillance technologies will be used. Relatedly, citizens at different events expressed appreciation for the deliberative method, and suggested promoting participatory events as a methodology capable of involving laypersons.

Law enforcement

Citizens' third most common message – contained in 40 per cent of the legal recommendations and expressed by a quarter of the tables – focused on specific provisions for law enforcement. Thus, according to participants the law must foresee sanctions for agents' misuse and abuse of data collection, possibly helped by the introduction of whistle-blowing schemes. But citizens' approach went beyond criminal justice; their suggestions aimed at improving the working environment of law enforcement agents, as well as accountability, with a view to make the best use out of surveillance technologies while minimizing abuse.

For instance, some participants suggested that misuse and corruption may be tied to the low status and salary of agents, thus arguing for an increase in remuneration, and generally to treat the profession with greater respect. As for accountability, citizens vouched for a clever use of stick and carrot, by publicly acknowledging and rewarding good deeds, while publicizing misuses, abuses, and the ensuing sanctions. In the same vein, authorities should publish periodic reports on the use of surveillance technologies, the data processed, and the related outcomes, as well as making known the units responsible for using surveillance technologies, and the names of those in charge. There was a fairly strong request for keeping *commercial actors* out of the maintenance of security, and disclosing and scrutinizing public–private partnerships for the pursuit of security.

The bottom line, for participants, was that adverse consequences could be reduced only if surveillance technologies *support rather than supplant human action*. Thus, agents should undergo ethical training and only authorized personnel should handle data distilled from surveillance technologies. Surveillance technologies should not be used for fishing expeditions, but only to gather details on an (otherwise) identified suspect. Citizens recommended that surveillance technologies be used for the investigation of crimes, to pursue *concrete* national security issues, and help those in need, but any other use should be banned. Accordingly, participants reject the idea that their personal communications be 'tracked' for a vague concept of national security: mass surveillance must be prohibited.

Fringes of participants were equally split on the ideas that, since our society is not under threat,[7] surveillance technologies should not be routinely used; that surveillance technologies are only used for good purposes and we should let the police do their jobs; and finally, that we already live in a police state, so nothing can be done.

Watching the watchers: an oversight agency

Since accountability is the key to trust, participants were asked to *watch the watchers*. In 40 per cent of law-orientated recommendations and at a quarter of the tables, citizens requested the creation of an *agency overseeing the use of surveillance technologies* (or even a dedicated tribunal arbitrating privacy and technology matters). Such an agency should be completely independent of political power. Citizens' suggestions as to what body could perform such functions, and what composition it could have, interestingly reflect national experiences.

Possible bodies include DPAs, an ethics board, and a specialized technological ombudsman. Members could be elected by the public, sit in the parliament with a composition representing all parties, or be composed of a president, DPA experts and technical experts. Most citizens suggested placing such authority either at the international (e.g. UN) level, or the EU level. Only a minority proposed to create a national authority. Such a body should be able to receive information from the public.

Citizens demanded that *technologies be assessed* before use. The results of the assessment should be made public, through as many media as possible, in clear and accessible language. Consequently, an ineffective surveillance technology should be

dropped, while a very intrusive one should be suitably justified. Table discussions revealed that citizens support the idea of financing research on the effects of surveillance technologies, and making the results available to the general public.

Surveillance-orientated security technologies, tech vendors and developers, and the Internet

Several recommendations (30 per cent of legal recommendations, roughly a fifth of the total) concerned the *surveillance technologies* discussed, and mainly focused on DPI as the most controversial technology (see Annex 1). Citizens recommended obliging *tech vendors and developers* to mention privacy risks in the users' manual. Some citizens called for the use of open-source code by developers, while others recommended promoting anonymization whenever data are only needed in the aggregate, and obfuscation when it may be necessary to go back to the identity of the person. Some, with reference to drones, recommended building a registry of the drones in use. Others suggested either prohibiting the sale of data, or treating it as a commodity, and then make it profitable for the data subject. Finally, some groups of citizens suggested that the answer lies in technology, and lamented the lack of alternative products on the market.

Citizens recommend making the terms of use on the *Internet* clear and simple for the layperson, and hard to change. For instance, a pop-up could inform users at login if the policy has changed, and privacy-respecting websites and apps could be signalled by quality labels and certification.

Privacy as a right and real consent

Roughly a fifth of citizens were explicit about 'privacy' being a right. Based on their real life experience, they expressed the wish to have real *control* over their data, and of giving substance to their consent. Some citizens proposed, if feasible in a secure way, to create a dashboard or 'my page', password-protected, cloud-based, where all personal data held by the public administration are gathered. Many insisted that the request for informed consent, preliminary to data processing, is done in a clear, unequivocal way. They should be notified when data have been transferred to a third party, or have been accessed. A few recommendations were geared at strengthening the protection of *sensitive data* (widely seen as a core of 'privacy'), whose secure deletion, especially online, should be guaranteed.

In relation to cameras, their installation in residential areas for security purposes should be subject to the consent of residents. To enforce their wish of not being tracked, some proposed setting up a 'do–not call' registry for surveillance technology. Finally, some citizens recommended enabling collective action/lawsuits against abuses.

The manifold significance of citizens' views

Citizens' rich and deep recommendations testify to the complexity of the topic and allow drawing reflections on the trade-off model and their overall relevance, as well as lessons for research and policy. I discuss each of these points in turn.

What the recommendations say: the trade-off model, and beyond

On the one hand, citizens' views complement the quantitative results on the trade-off model, and offer a deeper understanding of their perceptions. The majority of citizens do not believe that privacy and security are irreconcilable, and they challenge the fact that security is obtained at the sacrifice of privacy. Quantitative data show that approximately 30 per cent of citizens think in trade-off terms, deciding to give up privacy for increased security in return (see Chapter 14, this volume). Recommendations seem to suggest that convenience and the lack of information, rather than indifference toward privacy, often determine people's behaviour. Citizens articulate different views: either the relation between privacy and security has to be negotiated on a case-by-case basis, or appropriate legal solutions need to be found to avoid the clash. Citizens entrust the state (and companies) with the role of educator as to the consequences tied to the processing of their personal data.

To be sure, legal solutions are sustainable (and usable) only if accompanied by a careful reflection on societal factors and technological responses. A glance beyond legal recommendations unveils that technology is seen as a powerful tool to address insecurity, but in the long-term threats can only be tackled by addressing wider societal issues.

On the other hand, when read in the negative, the recommendations hint at citizens' lack of awareness of avenues of specific regulation and administrative oversight. Citizens mentioned neither the national data protection code nor the role played by the national DPAs in protecting personal data processing, especially in the private sector. Moreover, they never alluded to existing European authorities, such as Europol and the European Data Protection Supervisor. Some of the authorities mentioned have competence in those areas where participants felt there was a need to intervene (e.g. the private sector).

Rather than invalidating citizens' perceptions, such reading in the negative should spur important reflections as to whether relevant authorities do take sufficient care in publicizing and making available existing legal remedies. Indeed, citizens themselves expressed a need to scale up information on existing safeguards offered by the law, and the protection provided by the institutions in charge of implementing existing regulations.

Citizens' recommendations vis-à-vis the SurPRISE project's scholarship

Strikingly, many citizens' recommendations converge with the SurPRISE project research outcomes, which point at law and oversight, together with technology assessment and alternatives, toward 'balanced risk assessment' (Kreissl *et al.* 2013). In detail, the legal solution proposed lies in a 'core-periphery approach', based on the inviolability of the essence of any fundamental right, seen as a better alternative to an abstract ex-post balancing. The core/periphery model is to be integrated within a rigorous test for permissible limitations, entailing an early assessment of the proposed solution/technology to a security problem, thus combining compliance with rights to privacy and the needs of law enforcement agencies when conducting an

investigation. Such convergence is illustrated, for instance, by the overlap between citizens' main points and the project recommendations with a legal import contained in Deliverable 3.4 (Kreissl *et al.* 2013). Citizens' request for a mixed oversight body over surveillance technologies matches the project's suggestion of involving data protection agencies, technology experts and civil society organizations to carry out an early assessment of surveillance technologies (Kreissl *et al.* 2013).

But convergence goes beyond the result of the SurPRISE project (and similar projects). It is striking to observe that citizens' recommendations also overlap with those issued, e.g., by the European Group on Ethics in Science and New Technologies (hereafter EGE) (European Group on Ethics in Science and New Technologies 2014) and the European Parliament resolution on the US NSA surveillance programme (2014).

The above-mentioned conclusions could lead to two objections, namely that 'citizens' recommendations are valuable only because of their (partial) convergence with the project's results', and that 'the project guided citizens' answers'. I address each in turn.

First, due to the breadth of concerns expressed by participants, recommendations were wider in scope than the ones identified in the SurPRISE project's research. To this effect, the project's final recommendations incorporate citizens' demands that did not feature in the project research (SurPRISE Consortium 2015). This is the case of requests concerning the role of commercial actors, the enforcement of data protection tenets such as consent and control, and the need to reform the law. The argument mentioned to address the first objection could also be valid for the second one. Moreover, during the events citizens were asked to evaluate the questionnaire, information material and videos. Whenever participants expressed criticism, there was an even split between those who saw a tilt towards privacy and towards security (Christiani Skov and Lygum 2014). When citizens' views stemmed from direct questions, this is clearly indicated in the text.

Such convergence adds credit to literature that highlights the value of participatory events (Klüver *et al.*, 2000): complex issues can be submitted to citizens, and consultations can be conducive to refined results, even if participants are not experts. What it takes is an independent, well-balanced design and the commitment of reasonable resources.

Two important conclusions can be drawn. The first is a lesson for research, namely that there can, and must be, greater integration between law and empirical research, with some caveats on methodology. The second is for policy-making: participants' recommendations could be seen as providing an indirect litmus test for current policy initiatives, and the time is ripe to embed participation in policy-making. I discuss each in turn in the next two sections.

Lesson for research: greater integration between law and empirical research, especially in the AFSJ

Law was the most prominent element of recommendations (see Annex 1), and even when citizens addressed technical issues, they still referred to the law. The

experience from participatory events showed that it was not only possible to ask legal questions, but rather that it was inevitable. This is self-explanatory, if one reflects on the fact that European societies are built on the principle of the rule of law. The ensuing reflection, which stems from direct experience within the SurPRISE project, is that there can, and should, be, greater integration between law and empirical research of the deliberative type. Such integration requires bidirectional efforts and carries with it methodological requirements: first, legal research should strive to turn its language into one that can be understood by citizens; second, research design must include legal issues from the start.

As for the lawyer's approach, evidence-based thinking has spurred increasing attention to empirical legal research/studies, which is helping to understand the broad impact of law on society (Cane and Kritzer 2010). Deliberative methods allow understanding the down-to-earth effects of law on the layperson, including regulatory failures, and should therefore be of direct concern for the legal researcher. For this to work, suitable language must be adopted. Citizens involved in the SurPRISE deliberative events found it difficult to answer the most abstract questions concerning the desired level of safeguards in place (in relation to judicial review, data protection and ex-post checks of conformity). These questions proved inaccessible, leading project partners to understand that they should have provided an additional degree of explanation, and possibly the use of colour coding (example below):

> What kind of safeguards do you expect to be in place when security agencies use SOSTs (Surveillance-orientated security technologies)?' Options: judicial authorization by a public court with all parties presented; judicial authorization without hearing the affected parties; and administrative authorization without judicial control.

With regard to empirical design, the SurPRISE project fell initially short of exploring legal issues in quantitative terms. The large-scale events featured a minority of questions which enquired into aspects related to law, namely concern about the erosion of privacy understood as a right, various facets of privacy, and one question on the adequacy of existing applicable law vis-à-vis the risks of surveillance. Debating legal matters was seen as more appropriate for table discussions (qualitative information), where they could surface spontaneously.

The fact that the adoption of suitable legislation was the most common recommendation proposed by citizens across Europe, as well as several puzzling answers to the questionnaire (Barland *et al.* 2014; Szénay 2014), persuaded the SurPRISE project partners to finding ways of exploring the relevance of legal matters for citizens. The small-scale event was designed to include matters of law addressed with a mixed qualitative and quantitative approach. Citizens were asked to explain what are the biggest threats to them (as a proxy to the meaning of security); instances where surveillance is necessary and appropriate; their awareness as to what information is collected about them; their awareness of applicable law; the relevance of controlling one's information; the meaning of privacy to them (example below), and the existence of an inviolable area of privacy, if any:

How would you formulate in one or two words or in one sentence what privacy means for you? When should privacy be protected against surveillance and why is it important for you?

All such questions, supported by table discussions, allowed framing citizens' understanding to a greater degree of detail. The use of structured qualitative methods allows for the comparison of results from different events, through the use of coding (see *infra*, Annex 1). The experience of the SurPRISE projects calls for greater boldness in approaching citizens, with a view to enriching the area of empirical legal research.

The lesson for policy-making: a litmus test for current policy initiatives

While participants were not consulted directly about current policy initiatives, some of their contributions strikingly meet policy proposals. Keeping in mind that the proposed connection is ideal, not real, recommendations could be said to provide an indirect litmus test for some current policy initiatives. In what follows, I first show such links through a pick-and-mix selection of examples, and then I reason on how participatory research could support policy-making in the AFSJ.

Citizens' recommendations seem to buttress several innovations contained in the General *Data Protection Regulation* (European Parliament and Council 2016). To give but a few examples: the suggestion to have harmonized legislation across Europe is along the lines of the adoption of a Regulation; the request to have clear information policies and real control of one's data may indirectly support the innovations contained in sections 2 to 4 of Chapter II of the Regulation, as well as Article 7 read in the light of recitals 42 and 43 (which specify conditions for freely given consent).[8] Accordingly, the request of prior assessment could be met by impact assessments (Article 35), and the need to have stronger oversight supports the introduction of a data protection board. Moreover, the rejection of automated decisions, the request to issue dissuasive sanctions, and to enable collective lawsuits seem to indirectly support the innovations contained in articles 22, 83 and 80 respectively.

Similarly, citizens' insistence on appropriate laws to tackle misuse and abuse, as well as increasing the accountability of data processing by law enforcement agents (indirectly) endorses the adoption of a *Data Protection Directive* in the field of law enforcement (European Parliament and Council 2016).

Multiple requests concerned protecting data when in transit, and particularly when transferred to the jurisdiction where most online service providers are located, namely the United States. Such a request is along the lines of the overhaul of the *Safe Harbour agreement*[9] following the invalidation of the adequacy decision 2000/520 (Court of Justice of the European Union 2015). Moreover, it has a strong import for the negotiation of international agreements, such as the Framework agreement on data protection in the field of police and judicial cooperation (*Umbrella Agreement*) with the United States of America.[10]

Citizens' requests for financing research on technologies used for surveillance purposes and their impact on fundamental rights and civil society could be seen as supporting the investment in the *Horizon 2020 programme.*

Several recommendations focused on improving technology online and offline. This could be seen as indirectly supporting the adoption of a *privacy by design standard* for the future (European Commission 2012), as well as the setting up of working groups, such as the Internet Privacy Engineering Network, whose objective is to propose workable solutions that make the most of technology while respecting privacy.

The fact that citizens could discuss complex policy issues, and could express perceptions and propose solutions that happened to be in line with initiatives of the legislator, suggests that citizens can be involved in policy-making in the home affairs area. My claim is that the time is ripe to do so, for two reasons.

First, crime prevention, pursuant to Article 2(2) of Council Decision 2009/902/JHA, includes measures that 'reduce or otherwise contribute to reducing … citizens' feeling of insecurity'. The same proviso mentions the work of researchers; the SurPRISE project shows the great contribution of deliberative participatory methods to this point.

Second, and crucially, the Lisbon Treaty contains imperative innovations that try to reduce the democratic deficit, which include articles 10 and 11 TEU, 15(3), 24, 227 and 228 TFEU (Rosas and Armati 2010; Craig 2013). According to Craig, the European Court of Justice (hereafter ECJ) will have a hard time in interpreting such provisions as restrictively as it did in the past (Craig 2013), thus hopefully giving more weight to that principle of democracy which 'forms part of European [Union] law and was expressly enshrined [in the Treaties] as one of the foundations' of the EU (Court of Justice of the European Union 2007: §41). Citizens' belief that transparency is a precondition for participation seems to have been acknowledged by the Court. Indeed Articles 1 and 10 TEU, and Article 15 TFEU enshrine the principle of transparency, which 'enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system' (Court of Justice of the European Union 2010: §68). The ECJ reaffirmed the statement in *Client Earth and Pan Europe v EFSA* (Court of Justice of the European Union 2015: § 56). On the other hand, Rosas and Armati (2010) rightly point to Article 10 (3) as a basis for deliberative democracy: 'Every citizen shall have the right to participate in the democratic life of the Union. Decisions shall be taken as openly and as closely as possible to the citizen.' Political parties 'contribute to', rather than supplant, 'expressing the views of citizens' (art. 10(4)). Active engagement in the administration of public affairs would concretize material justice, which results from the European decision-maker taking into proper account and addressing the legally protected interests of public and private parties, as well as the right to good administration (Art. 41 of the Charter of Fundamental Rights of the European Union).

Deliberative democracy could complement traditional consultation procedures (Rosas and Armati 2010). Obviously it would have to be understood as empirical

legal research carried out with academic rigour and to limit potential shortcomings (Elster 1998; Ochoa 2008), e.g. on the issue of framing (see Chapter 3, this volume). It could be performed in all Member States in the shape of consensus conferences (Klüver *et al.* 2000) or as one-off participatory events, like SurPRISE's. The methodology could be used in the phase of impact assessment, to accompany mid-term review, or prior to adopting long-term strategies. Such an approach seems the minimum if the AFSJ is truly to be offered by the Union to its *citizens* (art. 3 TEU).

Conclusion: embed participation in decision-making

With this chapter I pursued two objectives. First, I made known the legal solutions proposed by participants in the SurPRISE events to tackle the complex interrelation between surveillance, security and privacy. Contextually, I showed that citizens reject indiscriminate surveillance, and believe there should not necessarily be a trade-off between security and privacy if appropriate legal safeguards and oversight are in place. According to citizens, technology can be a meaningful answer, but only in the short term, whereas in the long term the root causes of insecurity must be addressed.

Second, I reflected on the value of citizens' legal recommendations and the striking similarity they bear to SurPRISE projects' scholarship (which rejected the trade-off), experts' advice provided by similar projects, the EGE group, and the European Parliament. Instead of downgrading the value of citizens' input, I believe such convergence should buttress the feasibility of submitting complex issues to the attention of citizens, with two important lessons.

The first is that deliberative methods should espouse legal empirical research to investigate matters within the AFSJ, mindful of the methodological lessons learnt, for instance, within SurPRISE.

The second is that, while citizens were not consulted on current policy initiatives, their advice could be seen as providing an indirect and ideal litmus test for such initiatives. This insight leads to a deeper conclusion, namely that AFSJ-related policies in the EU could actually be tested by citizens through participatory methodology. At the events, many citizens expressed the feeling that participatory events increase awareness and involve citizens, and suggested repeating them.

There is more to participation than renovating (or, perhaps, in the case of the EU, building) the façade of democracy. Participation, in fact, is an expression of the rule of law, which ultimately protects dignity and a 'positive freedom: active engagement in the administration of public affairs, the freedom to participate actively and argumentatively in the way one is governed' (Mendes 2013: 25).

The Lisbon Treaty already contains rules favouring participation; it is a matter of acting upon them. Rooting participation in the process of decision-making, for instance in the form of participatory events assessing such different legally protected interests, would substantiate the rule of law, the right to good administration and, in the case at hand, at a particularly tough conjuncture for the European Union, avoid costly political decisions that have no support among the public, such as trading privacy for security.

Annex 1: coding of the recommendations

The 250 tables or thereabouts at the SurPRISE large-scale events generated approximately 250 recommendations, 145 of which focused on legal matters (the remaining 100 concerned the macro-areas of 'social', 'technology', and 'awareness'). The small-scale events led to 130 expressions of consensus formulated by 26 tables. Consequently, it was necessary to code the recommendations, whose raw version, translated into English, can be found in the Appendix of each national report on the project's website.

The table below shows the result of the coding performed on the legal recommendations, which worked as follows. All recommendations referring to law were scrutinized, and the main topic(s) they contained (listed in italics in the table) noted down. Note that several recommendations were complex and contained more than one topic. The ensuing list of topics was used to cluster recommendations. The central column in the table below contains additional nuances relating to a main topic, thus conveying a more detailed message.

The frequency of recommendations referring to certain topics is mentioned in brackets (next to the topic),[11] as they can be of relevance for the reader. For a similar reason, the topics have been ordered on the basis of their frequency. The frequency refers to the number of times that, throughout Europe, a specific topic was mentioned at a table, which grouped on average seven participants (1,780/around 250 tables). Note, however, that frequency has limited import on the relevance of qualitative information (Cane and Kritzer 2010).

Once I compiled the first table, I compared recommendations gathered through the small-scale events. Under the 'small-scale' column, the dummy variable Y (yes) means that the small-scale events produced a recommendation akin to that listed in the table. 'DNM' means 'did not mention', and indicates that there was no discussion about that specific point; I believe this is more appropriate than using 'N', standing for 'no', as this would possibly convey the wrong message of the point having been rejected. Whenever consensuses provide nuances, these are reported in the column.

Ultimately the content of the recommendations was summarized into the text reported in section 2.

Topic	Detailed message	Small-scale
Adoption of regulation (101 out of 145 legal, 250 total)		
	On surveillance technologies, privacy and data processing	Y surveillance technologies should be regulated from the start
Unspecified	Collection of data, control of use, deletion, proportionality: sometimes generic law, other times 'charter', other ethics code; metadata; strict, clear/simple, up-to-date, forward-looking; effective enforcement. Public registry of data controllers, application of law to data in transit abroad, involvement of companies in raising awareness; harmonization of laws/commercial purposes; should not hinder research/innovation	DNM
International	Strong international treaty (data transfers being a global problem); or treaty establishing minimum standards (awareness of complications). EU-US agreement	Y: to close the gap between EU and US
EU	Harmonization of rules; rules on surveillance technologies; avoid transfers of data where rights are not respected	Y: completely harmonized/Y but room for national differences should be allowed
National	The state must adopt suitable laws/update current	DNM
Transparency (73 out of 145 legal, 250 total)		
Transparency		Y
Education/ information/ awareness	Information campaigns; add to school curriculum; municipal course; surveillance technologies' user guides should include warnings on the effects on privacy; how to protect oneself	Y
Publication of information/ data gathered	Publication of reports concerning processing and other info	Y
Identity of who processes data/ accountability		Y
Policies concerning law enforcement (62 out of 145 legal, 250 total)		
	Fight abuses (prevention, appropriate access, proactive approach, necessary use)	Y, invest on the moral values of LEAs. Maybe include whistle–blowers norms

Topic	Detailed message	Small-scale
	Liability/strict penalties/sanctions (criminal law)	Y
	Switch–off button for surveillance options – limitation of surveillance	Y
	Surveillance technologies used only when suspects have been identified by other investigative means	DNM
	Purpose limitation – deletion – proportionality (purpose limitation, authorization of courts/ checks and balances)	Y: surveillance technologies used only for specified purposes, with checks and balances
	No automated decisions	DNM
	Secure storage	DNM
	Surveillance technologies as a tool to support police (e.g. using technologies in rural areas, while increasing police presence in residential places)	DNM
Independent authority (60 out of 145 legal, 250 total)		
	Assess technology prior of adoption, oversight of technologies, of authorities using data, handling data	DNM
National (Data protection) authority/ethics committee/ monitoring board/ technological ombudsman	Stronger; ethics committee; civil or judicial; made of experts, having regulatory powers; a body made of the president, DPA expert and legal expert; inspection of foreign technology; publicly elected, and able to receive information; could have an MP from each party, to avoid spoils system/guarantee independence; judges, lawyers, IT specialists, sociologists/philosophers; popular representatives	DNM
European authority	One suggestion was to issue licences for CCTV cameras (is there a public registry?); sanctioning powers	DNM
International DPA	United Nations and International Telecommunications Union	DNM
Tribunal for privacy matters	National or international (arbitration)	DNM
Surveillance-orientated security technology-specific (44 out of 145 legal, 250 total)		
Generic	Some provided recommendations on how to improve the technical features of technologies	Only for targeted individuals and specified purposes/ as long as effective

Topic	Detailed message	Small-scale
DPI (24)	Used only by government for national security	Y: for all technologies, as a precondition of trust
	Clear legal basis (worldwide)	Y
	Under supervision	DNM
	Legal limitations (e.g. only if the person is proved to be a suspect)	Y: OK only if used on everyone
	Should be banned	DNM
SLT (12)	Users must know when they are localized/data passed to third parties	DNM
	Only by government for security/rescue	DNM
	Clear legal basis	DNM
	Under supervision	DNM
	Switch–off button	DNM
	Legal limitations (secure storage, data of minors)	DNM
	OK use by commercial parties, but prohibit resale of data	DNM
CCTV (7)	Public spaces only – clearly signposted – consent of residents (but not in parks)	DNM
	Clear legal basis and limitations	DNM
	Filter data from cameras	DNM
	High resolution of images	DNM
	Smart CCTV is useless	DNM
		DNM
	Provision of services should be based on data sharing/selling with clear economic value	DNM
Unclear (1)	'Ticket' for the smartphone	DNM
Privacy-related rights (39 out of 145 legal, 250 total)		
Privacy as a right (16)		
	Must be protected /(explicitly) Right to be forgotten/ensuring that data online is deleted for good Privacy of communications (to be guaranteed)	Sensitive data must be protected more stringently
Data subjects' rights (23)		
	Access to one's data	Y

Topic	Detailed message	Small-scale
	Self–determination of data	Y
	Consent (in general, when using surveillance technologies, when buying technology, when visiting websites or using apps)/make the request for consent clear	Y
	Notification of access	Y
	Limit the collection of sensitive data	Y
	Enable collective action against abuses	DNM
Policy (25 out of 145 legal, 250 total)		
Policies on commercial use of data (20)		
	Prohibition of commercial uses/processing of data	Limit the use by private companies
	Increase offer/alternatives for consumers	DNM
	Force commercial parties to use open–source code	DNM
Policies relating to the online environment (5)		
	Terms of use: clear/hard to change	DNM
	Quality label/certification for websites and apps	Use of encryption
	Law on the use of the Web	DNM
Miscellanea (11 out of 145 legal, 250 total)		
	The notion of 'supervising the supervisors/who controls whom'	Y: watch the watchers and minimize chances of corruption (e.g. good salaries)
	Politicians won't constrain themselves	DNM
	Ensure that regulation does not hinder innovation	DNM
Alternatives (12 out of 145 legal, 250 total)		
	Develop alternatives (for security, investigations)	Y, also because we do not live under constant danger/human control
	Training those that process data/use surveillance technologies	Y, always, only authorized personnel can use surveillance technologies

Topic	Detailed message	Small-scale
Politics (6 out of 145 legal, 250 total)		
	Independence from USA – extra EU companies	DNM
	Balance between security and privacy; security and transparency	DNM
Participation (4 out of 145 legal, 250 total)		
	Participation of citizens	Y, in deciding when surveillance technologies should be used
	Constant policing, the problem cannot be solved	Y, technology and regulation should be discussed with public

Notes

1 I wish to express my gratitude to Martyn Egan and Marta Szénay for their helpful comments and revisions on the current and previous drafts of this chapter. All views expressed remain mine.

2 This chapter uses the expression 'privacy' as a monolithic term, in keeping with the use made within the SurPRISE project. However, my preferred expression is 'privacy rights', due to the double nature of privacy in the European Union, where it is embodied by two rights, namely the rights to private and family life and the protection of personal data. For a thorough reflection on the matter, see M.G. Porcedda (forthcoming). 'The recrudescence of "security v. privacy" and the value of "privacy rights" in the European Union', in E. Orrù, MG. Porcedda and S. Volkmann, (eds) *New Theoretical Perspectives on Surveillance and Control: Beyond the Privacy versus Security Debate*, Baden Baden: Nomos Verlag.

3 All deliverables, including events-related country reports, can be found at: http://surprise-project.eu/dissemination/research-results/ (accessed 15 February 2016).

4 The information material and videos, available in all project partners' languages, can be downloaded from http://surprise-project.eu/dissemination/information-material-from-the-participatory-events/ (accessed 15 February 2016).

5 All countries had five tables, except Italy, where there were six tables, due to the unexpectedly low drop-out rate (smart CCTV was discussed therein).

6 Following the many recommendations delivered at the large-scale events asking for better information, we asked participants in the small-scale events to explain what kind of information they would wish to know.

7 The events were carried out in the first half of 2014, and France was not involved in the research.

8 Accordingly, consent cannot be considered freely given if 'the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment' (recital 42) and 'should not provide a valid legal ground for processing if there exist clear imbalances between data controller and data subjects' (recital 43). This last caveat, originally placed in Article 7 of the Regulation, has been deleted from the final version of that article, hence losing its force. The practical consequences of both caveats will

depend on the willingness of the ECJ to give them sufficient weight when interpreting consent and the obligations of the data controller.

9 On the Privacy Shield see http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm (accessed 9 May 2016).
10 On the Umbrella Agreement see http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm (accessed 9 May 2016).
11 The latter has not been reported in the table for the sake of brevity. Likewise, I have not included in this version detail concerning the countries where each recommendation/nuance appeared.

References

Barland, M., Nilsen, J.S., Pavone, V., Porcedda, M.G., Santiago, E., Szénay, M. and Talo, T. (2014) *Report on Decision Support Testing*. SurPRISE Deliberable 7.1. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 15 February 2015).

Cane, P. and Kritzer, M. (eds) 'Surveillance Technology'. M. (2010) *The Oxford Handbook of Empirical Legal Research,* Oxford: Oxford University Press.

Christiani Skov, E. and Lygum, A. K. S. (2014) *Evaluation of the Citizen Summits*. SurPRISE Deliverable 5.4. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

Court of Justice of the European Union, *Judgment in Maximillian Schrems v Data Protection Commissioner,* C-362/14, EU:C:2015:650.

Court of Justice of the European Union, *Judgment in Client Earth and Pesticide Action Network Europe v. European Food Safety Authority and European Commission*, C-615/13 P, EU:C:2015:489.

Court of Justice of the European Union, *Judgment in Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, Joined cases C-92/09 and C-93/09, EU: C:2010:662.

Court of Justice of the European Union, *Judgment in European Commission v. Federal Republic of Germany*, C-518/07, EU:C:2010:125.

Craig, P. (2013) *The Lisbon Treaty, Revised Edition: Law, Politics, and Treaty Reform,* Oxford: Oxford University Press.

Elster, J. (1998) *Deliberative Democracy*, Cambridge: Cambridge University Press.

European Commission (2012) *Security Industrial Policy. Action Plan for an Innovative and Competitive Security Industry.* COM(2012) 417 final, Brussels.

European Commission (2013) *On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. COM(2013) 847 final. Brussels, Belgium.

European Group on Ethics in Science and New Technologies (2014) *Ethics of Security and Surveillance Technologies*. EGE Opinion n° 28. Available at: http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/ (accessed 15 February 2016).

European Parliament (2014) *Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*, Brussels. Online. Available at: www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230 (accessed 15 February 2016).

European Parliament and Council (2016) 'Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Sata, and Repealing Directive 95/46/EC', *OJ L* 119, 4.5.2016, 1–88.

European Parliament and Council (2016) 'Directive (EU) 2016/680 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA', *OJ L* 119, 4.5.2016, 89–131.

Klüver, L., Nentwich, M., Peissl, Torgersen, H., Gloede, F., Hennen, L., Eijndhoven, J. V., Est, R. V., Joss, S., Bellucci, S. and Bütschi, D. (2000) *European Participatory Technology Assessment. Participatory Methods in Technology Assessment and Technology Decision-making.* Online. Available at: http://cordis.europa.eu/docs/publications/7078/70781441-6_en.pdf (accessed 15 February 2016).

Kreissl, R., Berglez, R., Porcedda, M. G., Scheinin, M., Schlehahn, E. and Vermeulen, M. (2013) *Synthesis Paper on Comprehensive Security Enhancing Policy Options.* SurPRISE Deliverable 3.4. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

Mendes, J. (2013) 'Rule of Law and Participation: A Normative Analysis of Internationalised Rulemaking as Composite Procedure', *Jean Monnet Working Paper Series.* New York: New York University School of Law.

Ochoa, C. (2008) 'The Relationship of Participatory Democracy to Participatory Law Formation', *Indianda Journal of Global Legal Studies,* 15: 1.

Pavone, V., Eposti, S. D. and Santiago, E. (2013) *SurPRISE project Deliverable 2.2. Draft Report on Key Factors.* Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

Porcedda, M.G. (forthcoming) ''The recrudescence of 'security v. privacy' and the value of 'privacy rights' in the European Union'' in Orrù, E., Porcedda, M.G. and Volkmann, S. (eds) *New Theoretical Perspectives on Surveillance and Control: Beyond the Privacy versus Security Debate*, Nomos Verlag: Baden Baden.

Porcedda, M. G., Vermeulen, M. and Scheinin, M. (2013) *Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy.* SurPRISE Project Deliverable 3.2. Florence: European University Institute. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

Rosas, A. and Armati, L. (2010) *EU Constitutional Law – An Introduction,* Oxford and Portland, OR: Hart Publishing.

Strauß, S. (2015) *Citizen Summits on Privacy, Security and Surveillance: Synthesis Report.* SurPRISE Deliverable 6.10. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

SurPRISE Consortium, Čas J. (ed.) (2015) *Policy Paper and Manual.* SurPRISE Deliverable 6.13. Online. Available at: http://surprise-project.eu/dissemination/ research-results/ http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

Szénay, M. R. (2014) *Comparative Report – Citizen Meetings.* SurPRISE Deliverable 7.2. Online. Available at: http://surprise-project.eu/dissemination/research-results/ (accessed 14 November 2016).

12 The importance of social and political context in explaining citizens' attitudes towards electronic surveillance and political participation[1]

Dimitris Tsapogas

Introduction

Snowden's revelations intensified both the mainstream and alternative media coverage of stories around contemporary surveillance practices. Such stories play a significant role in modifying citizens' level of awareness, understanding and perceptions around privacy, data protection, security, and surveillance (Coleman and Sim 2000; Doyle 2003; Nellis 2007). One of the main concerns here is that surveillance may influence negatively important societal values, as individual freedom, autonomy, privacy, solidarity, equality, trust, and the rule of law. These values are of paramount importance for the support of key democratic processes, such as the creation of associations, political interests, constructive and alternative ideas and the raising of criticism (Habermas 1989 [1962]; Solove 2007; Mitrou 2008; Haggerty and Samatas 2010). Yet, a rather small number of studies have tried so far to understand the relationship between surveillance perceptions and political participation and the small amount of literature that is available on the subject contains sometimes opposing and mixed views.

By drawing on a mixed-method approach, this study collected both quantitative and qualitative data through a survey on the one hand, and a series of semi-structured interviews and focus groups on the other, with experts, academics, members of the police cybercrime unit, IT security corporate executives, activists, university students, and citizens with different positioning on the political spectrum. Greece was used as a case study and all empirical data was acquired from respondents who lived there in late 2013.

This chapter suggests the proposition that existing research has neglected important contextual aspects that are important in analysing and explaining citizens' attitudes and behaviour in the context of (electronic) surveillance and political participation. In order to help the reader to have a better understanding of the data and analysis, the chapter starts with a contextual and historical background of Greece's surveillance history and presence, as well as citizens' attitudes to it. This is followed by an overview of the main literature review. Then, it presents the research methods used for the collection of empirical data, as well as the main

insights gained by the analysis. The chapter concludes with a discussion of the main findings, research limitations, and suggestions for future research.

Political and economic surveillance in Greece

Greece has been a prominent example of a country with a long surveillance legacy, which has been exercised as a mechanism of sociopolitical control (Samatas 2004). According to Samatas (2005), Greece's postwar history can be categorized in four distinct surveillance periods. The first is the post-civil war repressive anti-communist surveillance, which started after 1945 and continued until the end of the military dictatorship in 1974. During this period, the police, military, and security agencies were exercising surveillance by using a network of informers dispersed throughout the country. Every individual and their family had a record that was called a dossier (φάκελος (*fakelos*) in Greek) that contained information about their 'national loyalty', as well as about their ideological and political preferences (Samatas 1986). The second period began after the end of the Greek military dictatorship in 1974, when parliamentary democracy was restored and the Greek Communist Party (KKE) was legalized (Samatas 2005). Surveillance during these years continued to be intense, although more discreet, and was focused on the newly formed left-wing parties that were opposing right-wing state positioning. The period lasted until 1981 when the Panhellenic Socialist Movement (PASOK) came to power. From 1981 and until 1996, PASOK was in power (1981–1989 and 1994–1998), with the exception of the period 1989 to 1993 when the New Democracy political party came to power, 'populist' and 'Machiavellian' surveillance was exercised (Samatas 2005: 184). During this period, the two main parties that alternated in power were organizing their own wire-tapping networks. The fourth and final period started in 1996 until today, when 'new surveillance' practices were put into place. During that period Greece entered the European Monetary Union and signed the Schengen Treaty. The 'new' Greek surveillance is characterized by Samatas (2005: 185) as 'a galaxy of electronic surveillance systems deployed by the state, supra states, public and private institutions and individuals'. It is exercised 'with or without individual consent, for legitimate and illegitimate purposes, including security, profit'.

A well-known example of political surveillance in Greece from the latter surveillance period is the so-called Greek Olympic phone tapping scandal that took place in 2004 (Samatas 2010). This concerns the monitoring of the mobile phones of the Greek prime minister, the government, and top military and security officials, a case that has not yet been resolved until today. What is exceptional with this case is that although, traditionally, the Greek state has been the main source of surveillance – usually against the opposition and political activists – this was the first time when the Greek state and its top officials were the target of surveillance (Samatas 2010). Spy software was installed at the telecommunications infrastructure of Vodafone Greece (one of the largest mobile telephony providers in Greece) that 'allowed calls from and to the tapped numbers to be monitored and recorded by other cell phones' (Samatas 2010: 214). It is still unclear whether

Vodafone and/or Ericsson (the latter was responsible for Vodafone's technical infrastructure) were aware of the tapping. What is known is that, two days after the discovery of the spy software and one day before Vodafone informed the Greek government, one software engineer was found dead, allegedly by suicide. The magnitude of these revelations became the main topic of discussion in the Greek press at that time and continued to be discussed sporadically until today. The political and psychological consequences for the broader public were included in various surveys and opinion polls and as Samatas stresses: 'If a prime minister, his top ministers and officials, and telecom corporation like Vodafone or Ericsson could not protect the privacy of their cellular-phone communications, it is not surprising that ordinary people feel almost defenceless against comparable breaches' (2010: 223).

Furthermore, in more recent years and in particular since 2008, Greek society has been experiencing an unprecedented economic, social, political, and humanitarian crisis.[2] During this period that was characterized by uncertainty, depression, and high levels of distrust in public and political institutions and actors, very frequently one could find stories in the media about the state's ubiquitous financial surveillance, that targeted any organization, corporation or citizen that might have been involved in any sort of financial misconduct such as tax evasion. Following state surveillance, arrests of citizens were presented in a dramaturgical way in the mainstream media, along with blatant details of how the Greek Financial Crime Unit (SDOE) managed to arrest the suspected tax evaders, after they had been put under surveillance. The high urgency that the crisis created and the fear of unintended consequences, such as the country's bankruptcy, generated the necessary political legitimacy for the increase of surveillance.

Another type of state surveillance that was also frequently communicated via the media during this era concerns surveillance of political elites or activists, mainly from the far-left and the far-right of the political spectrum, usually on the grounds of their possible relation to terrorist groups and/or organized crime. A recent example is that of surveillance of members of the main opposition,[3] as well as civil society organizations and activists who participated in the anti-gold mining movement and protests, which have been taking place in the gold-mining area of Skouries in northern Greece (Apostolakis 2013; Ravanos 2013). A better-known case that was heavily discussed in the Greek mediated public sphere, as well as in the parliament, is the electronic surveillance of the members of the far-right political party – including parliamentarians – by the Greek National Intelligence Service (NIS) and the so-called Special Suppressive Counter-Terrorism Unit (EKAM). In this case, the government was forced to publicly announce that a warrant from a judge had been issued and the members of the Golden Dawn party had been officially under surveillance, after the public outcry that followed the assassination of an anti-fascist activist in Athens by members of this party. Soon after the assassination, the Greek government stated that important clues had been found, which connected members of the Golden Dawn with the assassination but also with other criminal activities. The disturbing aspect of this case was brought to public attention by an MP of the ruling party at that time:

'How is it possible that the tapping of the NIS has recorded incriminating conversations of Golden Dawn MPs before the murder took place in Athens?' (Katrougalos 2013). As Katrougalos (2013) exemplified, the above aspect means that 'the National Intelligence Service is conducting unconstitutional, mass, pre-emptive, surveillance, comparable to the ones [surveillance practices] that Snowden revealed in the US'.

Greece's legacy in state surveillance was reflected in public opinion surveys around issues of data protection and privacy. In the Special Eurobarometer 359 (2011) that explored national attitudes on data protection and electronic identity in the European Union, the Greek population appeared to have the lowest level of trust in most institutions and the highest levels of concerns in most examined categories. In particular, 83 per cent of them stated that the government asks for more and more personal information, which was the highest figure among all countries, while 77 per cent considered the disclosing of personal information a big issue. Regarding concerns about tracking via mobile phone or mobile Internet, Greek respondents had once again the highest concerns, with 65 per cent of the population holding this opinion. Very importantly, Greece was the only country where more than half of the respondents appeared to be concerned that their behaviour was being recorded in a public space (54 per cent). Interviewees from Czech Republic (72 per cent), Germany (69 per cent), Greece (68 per cent) and Latvia (67 per cent) said that they felt uncomfortable with Internet profiling. Greece also stands out with the lowest percentage (14 per cent) of interviewees that trust phone companies, mobile phone companies, and Internet service providers, followed by Germany (20 per cent). Overall, Greeks appeared to have the lowest level of trust in all institutions and companies compared to their EU counterparts.

In the Flash Eurobarometer 225 survey on Data Protection in the European Union, conducted in 2008, Greece was situated more frequently than any other country at the lower end of the scale regarding trust in organizations. Greek respondents were most likely to argue that personal data protection was low in their country (71 per cent) and at the same time most likely to say that they are worried about leaving personal information on the Internet (82 per cent). Furthermore, Greeks appeared to have the lowest level (37 per cent) of trust in the police in the appropriate handling of personal data. Importantly for the scope of this research, the vast majority of the Greek population (92 per cent) said that transmitting personal data was not sufficiently secure, which was, unsurprisingly, the highest percentage among all countries.

The relation between (electronic) surveillance and participation

Despite the radical increase of state sponsored surveillance, especially since the terrorist attacks of 9/11, Cunningham and Noakes (2008: 176) argue that 'political surveillance, infiltration, counter-intelligence, and the work of agents provocateurs, remain a neglected category of sociological research', apart from some notable exceptions. What is more, the two authors indicate that the current literature regarding the effects of known or secret forms of social control on social

movements focuses mainly at the organizations' level but does not provide insights on the experience of surveillance by political activists.

In his classic article 'Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant', Gary Marx (1974: 408), emphasized the tremendous negative impact that 'undercover agents' can have 'the life of a social movement'. Marx (1974: 428) suggested that sometimes a revelation about the existence of covert surveillance among political activists can actually 'help perpetuate a protest group by offering the kinds of resources and moral support that are often in short supply'. Still, as Marx (1974: 428) explains, the potential negative implications are much more alarming. The discovery of police surveillance within a political organization or just even the idea about such possibility, 'may lead to feelings of demoralization, helplessness, cynicism and immobilizing paranoia, and can serve to disintegrate a movement'.

Following the important work of Marx in the 1970s on the dynamics of repression, Bert Klandermans and Dirk Oegema (1987) presented empirical support from research on mobilization and participation. The authors investigated the effort of Dutch peace activists to mobilize individuals to attend a forthcoming protest and found out that, while 74 per cent of the local population agreed with the rationale of the demonstration, only the one-sixth actually intended to attend. From this one-sixth, only the three-fifths did eventually go. The most usual factors for non-attendance were due to the way citizens perceived the event, and in particular, those who did not eventually attend it believed that there were certain costs and/or risks. For example, those who feared that there was a possibility of violence or that there would be policing of the protest, appeared to be less likely to attend. Cunningham and Noakes (2008) point out the importance of the insight provided by this particular research. Political activists or ordinary citizens that belong to the mainstream political process, did both calculate in the same way the potential costs and benefits before they came to a conclusion of participation or non-participation. Cunningham and Noakes (2008) argue that although such literature on the direct and measurable costs of covert social control is important, still, for the full understanding of the effects of covert social control, one must take into account 'the psychological and relational costs of repression', that is the 'indirect costs imposed by covert forms of social control on the personal emotions of social movement participants and the collective emotions of social movement organizations' (Cunningham and Noakes 2008: 186).

Samuel Best and Brian Krueger tried to connect the emotions about government surveillance perceptions and political participation. In one of their works, 'Government Monitoring and Political Participation in the United States: The Distinct Roles of Anger and Anxiety', the two authors proposed a theoretical model where anger and anxiety about state surveillance influence political engagement positively and negatively respectively. Based on a random sampling that collected more than 1,000 responses, they tested a number of hypotheses that would potentially contribute to the understanding of association between government monitoring and political participation. The key dependent variable in their model was political participation, as measured by combining different participation

activities into a participation category. The main independent variables were the emotions of anxiety and anger over the possibility of U.S. government surveillance.

On the one hand, Best and Krueger hypothesized that there will be positive relationship between anger and political participation. On the other, they expected that anxiety will be negatively associated with participation, an assertion that had not been tested in previous studies until that time. The results showed that when state surveillance generates higher levels of anger in an individual, this leads to higher levels of political participation. In contrast, when an individual develops higher levels of anxiety due to surveillance, political participation is chilled. Interestingly, anger and positive engagement prevail in the findings. Both authors argue that this can be possibly understood as a cycle. When a citizen participates politically, this generates expectations for government surveillance, which in turn provokes higher levels of anger. In contrast, the more individuals participate, the more desensitized they become about potential concerns, and thus less anxious about potential government surveillance. Best and Krueger conclude that the relationship between government surveillance and political participation cannot be explained solely by emotions about government surveillance and that future research should test the hypothesis that will take into account different variables in relation to this model.

In addition, Smith *et al.* (2011: 1005 and 1007) conducted and published in 2011 an extensive interdisciplinary review of privacy-related research outputs with a sample of 320 articles and 128 books and chapters. By reflecting on their findings, the authors argue that academic scholarship on the field has not yet exploited the theoretical advancements that have been developed in normative and descriptive studies. Therefore, as they conclude, future research could gain great value from:

> [R]igorous empirically descriptive studies that either trace processes associated with, or test implied assertions […] Although some possibilities for surveys do exist, the most helpful studies will likely be grounded in direct observation of the group members and their interactions. This suggests a long-term research agenda that will rely heavily on access to group settings in a variety of domains. It will be almost impossible to examine these processes without direct observation or participation.

Following the contextual and historical background and literature review, this chapter intends to discuss the answers to the following questions: i) What are participants' attitudes towards state surveillance? and ii) What is the role of ideology, if any? and iii) Which themes occurred most often in the context of electronic surveillance and political participation?

Methodology

Owing to the complexity of the central problem, a mixed-method research framework has been designed and operationalized. This included the collection of both

quantitative and qualitative data, through a national survey on the one hand and a series of semi-structured qualitative interviews and focus groups on the other. All data discussed here was collected between July and December 2013. The survey and the focus groups/interviews were independently designed in a way that incorporated different quantitative and qualitative perspectives in each one.

As Wolff and colleagues (1993: 119) point out: 'the particular strengths and limitations inherent in different methods might suit them ideally to complement one another in a unified research design'. This approach, namely the 'simultaneous' conduct of both methods that have been designed, is known as triangulation, with which the researcher increases the possibilities for 'improved accuracy' of the research findings, as well as a 'fuller picture' of the explored issues (Denscombe 2010: 348).

In particular, following the exhaustive literature review on the explored themes of privacy, surveillance and political participation, two sets of informal focus groups with university students were conducted, as well as a number of informal, unstructured interviews with university students, activists, and experts. The survey questionnaire was informed by and/or based on a number of pre-existing related studies, namely those of Best and Krueger (2011), and Dinev and colleagues (2008), the fifth round of the European Social Survey (2010), the Pew Research Center's 'Civic Engagement in the Digital Age' survey of 2013, the Special Eurobarometer 359 (2011), and the Flash Eurobarometer 225 (2008). I assessed the non-response bias by confirming that respondents' demographics of this sample are compatible with current Internet offline and online populations, as reported in the fifth round of the European Social Survey, as well as in the two Eurobarometer surveys.

After developing the survey questionnaire in English, two expert reviews were conducted in Vienna. After its improvement, the questionnaire was translated to Greek and a pilot survey was conducted with 30 Greek respondents to test the interview length. The pilot sample was as high as the 3.6 per cent of the final survey sample size (N=799). After the assessment of the pilot survey results, further minor modifications of the questionnaire were deployed, mainly regarding wording and structure. The survey used two modes for collecting data. Initially, 300 printed questionnaires were administered to a broad sample of individuals in Athens. The survey was offered to a broad range of individuals in companies, public organizations, shops and neighbourhoods. The respondents returned a completed survey at the indicated collection points or by using a prepaid envelope. Out of the total questionnaires administered, 145 were collected. Meanwhile, the second survey mode, an online questionnaire, was set up by the use of online survey software. Invitations to survey participation were sent out as emails to Greek universities, to various mainstream and alternative media, online websites and forums across the whole political spectrum, as well as to a large number of groups on Facebook, which again, belonged to the whole political spectrum. Participation in the survey was anonymous.

After the survey, a series of semi-structured interviews with five experts and four focus group discussions with 38 participants with different positions on the political spectrum took place (Table 12.1). In particular, the focus groups were

Table 12.1 Basic demographics of interviews and focus group research

Participants	Number (Total: 43)	Date	Location
Interviews – Experts			
Investigative journalist	1	2013	Athens
Professor of law	1	2013	Athens
Professor of computer science	1	2013	Athens
Former cybercrime unit officer	1	2013	Athens
IT Security corporate executive	1	2013	Athens
Focus groups			
Far–left wing activists	8	2013	Athens
Left–wing activists	8	2012	Athens
Apolitical (ordinary) citizens	10	2013	Athens
University students (mixed)	12	2013	Crete

conducted individually with the following categories: far-left, left, as well as with apolitical citizens and university students. The focus group research extended the depth of understanding gained by the survey and explored how these different political (and apolitical) groups cope with electronic surveillance in the context of political participation.

Main results

Although a convenience sampling technique was deployed for the survey, the demographic distribution of the 799 respondents indicates a fairly diverse sample of individuals. In particular, male respondents represent 70 per cent of the sample, with females occupying 30 per cent. The respondents appear to be highly educated, with 37 per cent of them stating that they had a bachelor's degree, 20 per cent a master's degree, 6 per cent a PhD, while 21 per cent had graduated from high school. Regarding employment, 32 per cent of the respondents were working in the private sector, 23 per cent self-employed, 14 per cent working for the public sector, 12 per cent unemployed, 6 per cent higher education students, while 2 per cent were pensioners. Regarding the main addresses of the respondents, 60 per cent of them indicated that they lived in the Attica region (the wider geographical area surrounding Athens that has a population of around 4 million, out of the country's total 11 million). From the rest of the respondents, 19 per cent had their main address in North Greece, 13 per cent in Central Greece and 8 per cent from the islands.

As Figure 12.1 shows, the vast majority of the sample, namely 92.1 per cent, accessed the Internet every day, 4.9 per cent a few times a week, 1.1 per cent once a week, 0.5 per cent every two to three weeks and 1.4 per cent less than once month. Out of them, 57.4 per cent used a desktop computer to access the Internet, 71 per cent a laptop, 46.3 per cent a smartphone and 18.5 per cent a tablet.

**About how often do you use the internet or email –
whether at home or at work – for your personal use?**
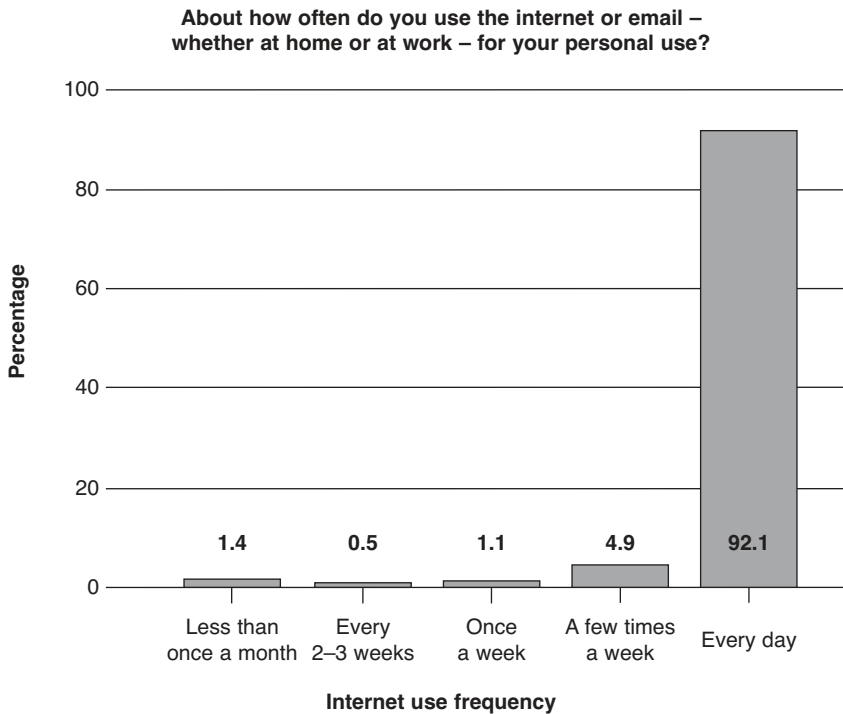
Figure 12.1 Internet usage frequency

   Among the activities they performed online, sending/receiving emails was the most common (87 per cent) while 86 per cent stated that they read or downloaded online news, newspapers or news magazine. Eighty-five per cent found information about goods and services and 67 per cent used social networking sites (Figure 12.2).
   As Figure 12.3 reveals, the respondents of the survey are distributed across the whole political spectrum. In addition, their distribution is comparable to a large extent to distribution of support for political parties in Greece at the time of data collection, the third and fourth quarters of 2013.

Concerns about state surveillance and the importance of personal ideology

Survey data reveal an important level of concern among the Greek participants regarding electronic state surveillance. In particular, as Figure 12.4 reveals, 43 per cent of the respondents were quite or very much concerned about the ability of Greek state authorities to monitor Internet activities, such as the email and the social networking sites. It is notable here that concerns about other categories of

Which of the following activities do you use the internet for?
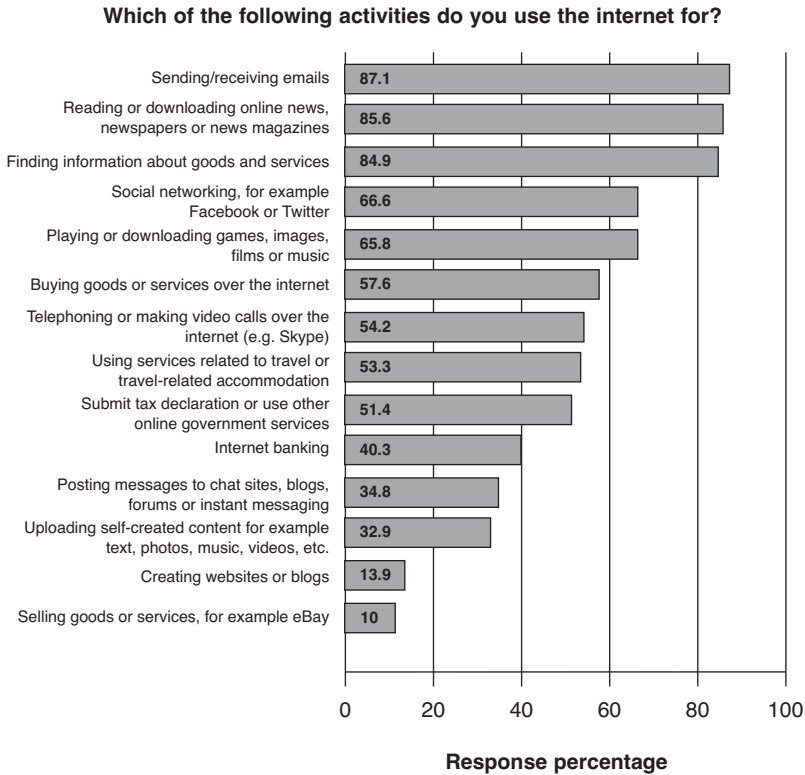
Figure 12.2 Activities on the Internet

surveillance were also tested (namely landline, mobile and CCTV surveillance) with the results being similar. Therefore, I discuss here only the concerns about Internet activities. So what is the effect of political positioning on the Internet surveillance concerns?

Here we can see four different groups of replies (Figure 12.5). The far-left and left have been grouped together. Equally, the centre-left, centre and centre-right have been also grouped together and equally, the right and far-right. Lastly, those who did not wish to place themselves upon the spectrum or did not want to answer were also grouped together. As we can observe, the vast majority of the far-left and left stated that they are quite or very concerned about Internet surveillance, while in all other groups, the majorities were not at all concerned or were a little concerned.

Apart from the Internet, mobile, landline and CCTV surveillance concerns, there was a fifth sub-question that tested concerns regarding foreign, transnational surveillance. Interestingly enough, the response patterns change here fundamentally (Figure 12.6), as almost half of the study's respondents (49 per cent) were very much concerned that foreign, transnational authorities also had the above abilities

Where would you position yourself on the political spectrum?

Far left	Left	Centre left	Centre	Centre right	Right	Far right	Nowhere	Don't know/ Don't want to answer
5.5	14.6	11	9.8	8	7.5	8.1	25.3	10.1
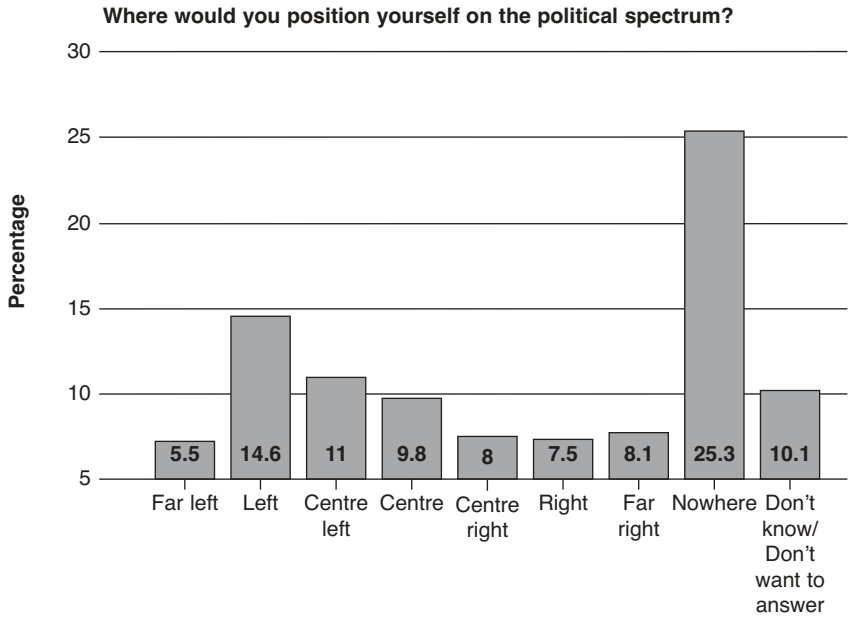
Figure 12.3 Self-positioning of respondents on the political spectrum

Are you concerned about the ability the state authorities have to monitor internet activities (e.g. email, social networking sites etc.)?

Not at all	A little	Quite	Very much
20.3	36.9	26.1	16.7

N=792 (excluded Don't Know responses and missing values)
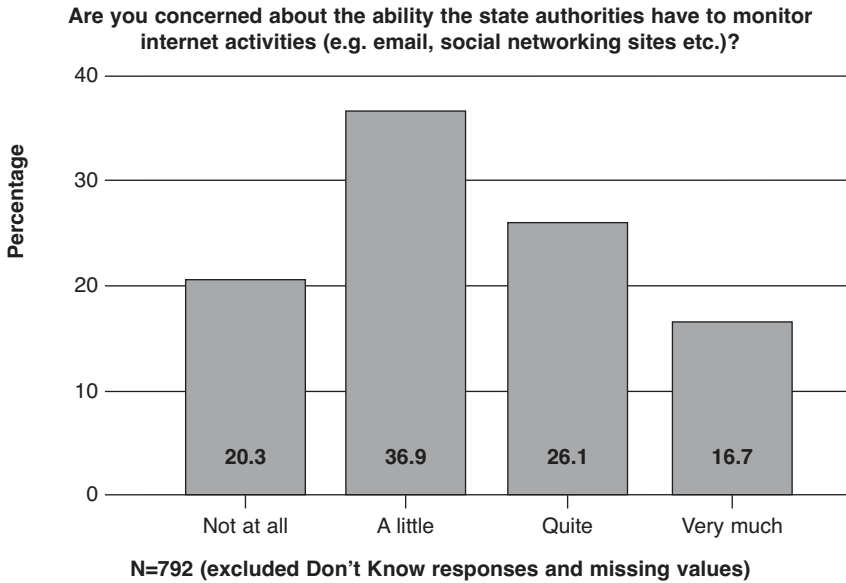
Figure 12.4 Concerns about Internet surveillance

Are you concerned about the ability the state authorities have to monitor internet activities (e.g. email, social networking sites etc.)?

Legend: Not at all/A little ■ Quite/Very much ▩

| Far left/Left | Centre left/Centre/Centre right | Right/Far right | Nowhere/Don't know/Don't want to answer |
| 5.8 14.4 | 19.8 9 | 10 5.8 | 21.6 13.6 |

N=792 (excluded missing values)
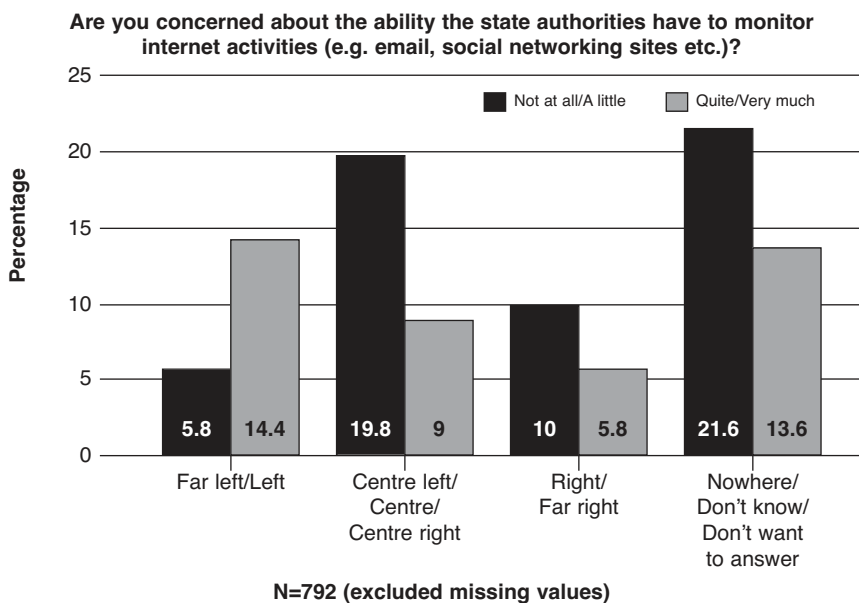
Figure 12.5 Internet surveillance and political positioning

Are you concerned that foreign, transnational authorities also have the above abilities to monitor citizens of Greece?

| Not at all | A little | Quite | Very much |
| 5.8 | 16.5 | 28.8 | 48.9 |

N=792 (excluded Don't Know responses and missing values)
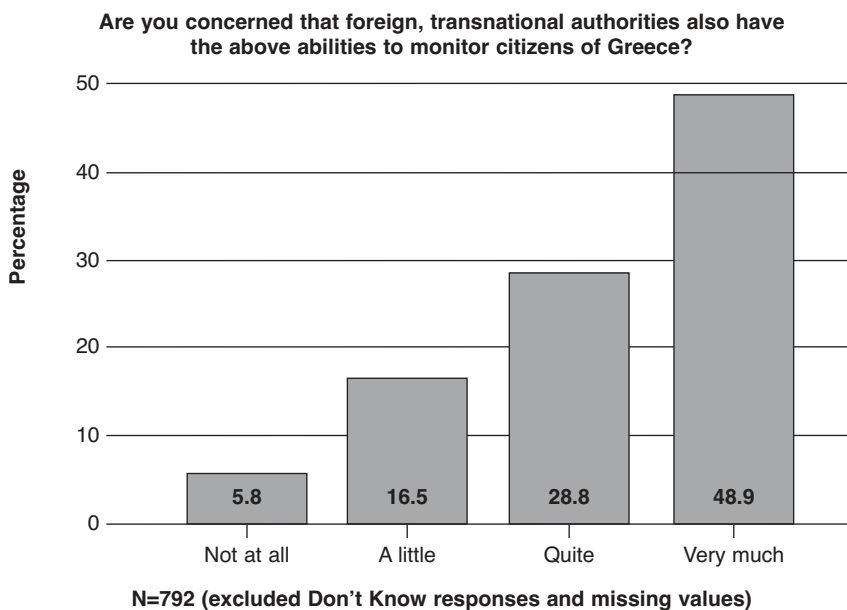
Figure 12.6 Transnational surveillance

to monitor citizens of Greece. Another 29 per cent showed that they were also quite concerned for the same issue. Combined together, a total 78 per cent of the sample appeared to be quite or very much concerned.

Equivalently, by combining both variables, we can see (Figure 12.7) that there is no effect of political positioning on citizens' concerns on foreign surveillance. As we have just discussed, citizens that were self-positioned on the left side of the political spectrum had most concerns about Internet surveillance. This does not mean, though, that they are actively worried about surveillance in their everyday electronic transactions or that they necessarily modify their electronic habits in the context of political communication.

Although most participants in the far-left and left focus groups appeared to be particularly knowledgeable and concerned about state surveillance, most of them did not take any serious measures to protect their privacy and thus resist surveillance. One influential reason for this attitude was personal ideology, which shaped to a large extent their online communication and participation behaviour.

Markos, from the left-wing group, explains that although he is aware of the dangers and has certain concerns, he has chosen to share openly political information online, in the same way he chooses to reveal his political identity offline:

> If somebody at this moment acquires access to my Facebook account, either
> because he/she is my friend and can see the information I disclose there, or
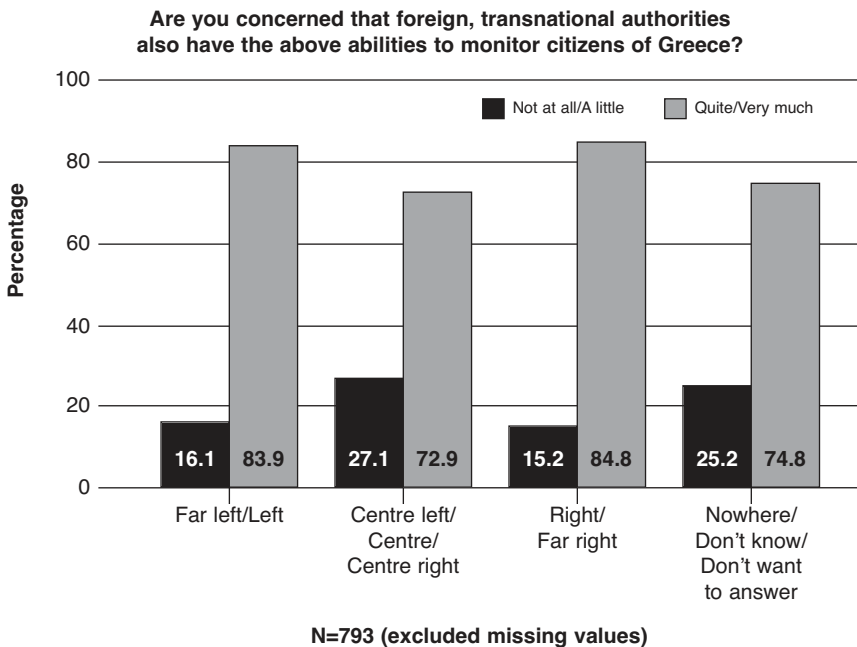
Figure 12.7 Transnational surveillance and political positioning

because he/she has gained access without being a friend, that person can iden-
tify my political ideology, that I am left, that I am a communist etc. In that
sense, exactly because this kind of identification can be done by any other
person who sees me offline in my daily life, because I participate, for example,
in demonstrations, in trade unions etc. … Because anyway these are things
which I am not hiding and I share them openly [offline]; this kind of infor-
mation I also share online.

Kostas, from the far-left focus group demonstrated a similar attitude:

I take for granted that it occurs. Meaning that, I believe surveillance takes
place. It DOESN'T make me emotionally upset. OK, politically speaking, I
disagree [with surveillance] obviously. Because I feel that the state is my enemy
etc. However, I do not want to have any differences in the political discourse
I express outwardly and in the one I express to a narrow circle of acquain-
tances and friends etc. I do not take part in illegal political activity. I do not
undertake actions that could be considered unlawful etc., therefore I don't
enter the process of hiding my views and all these things.

Regime type, quality of democracy and past experiences

Another theme that frequently came up during the discussions, was the role of the
regime type and quality of democracy. Although the vast majority of the focus
group participants and survey participants stated that they were not satisfied with
the quality of democracy in Greece, still, most of them agreed that Greece was a
place where fundamental democratic and legal rights are still safeguarded. On the
other hand, if they were to reside in China or in Turkey (quote below), their elec-
tronic behaviour would have been different. As Markos explains, although he has
chosen to share openly his political identity online, this would not have been the
case if he were living in another country:

Let's say that we are at this moment in China or in Turkey, under a regime that
is enforcing a much higher control over social networking sites and the media
[…] In this example, if I were to organize a mobilization of the Tibetan people,
it should be taken for granted that this effort would be suppressed by the
Chinese government. Although it may have been clear on Facebook that I
support Tibet – because I would have posted pictures of bold people with pink
clothes – however, if I wanted to organize such a mobilization, I would not
have done it, neither via Facebook nor via email.

A critical investigative journalist, infers the same democratic safeguard:

[F]or as long as there are some democratic processes [guarantees], here is the
whole game … There is also the question of claiming such democratic safe-
guards. You would not behave in the same way as someone would have

behaved in East Germany, where there was no de facto concept of protection. Therefore the only thing that could have protected you was secrecy. This is not the situation here, fortunately. This is not the situation in the Western world, nor Greece.

On the other hand, Natassa, a sociology student who participated in the focus group with the university students, revealed that she did not want to express her political opinions online because of her family's past experience with state surveillance:

> Owing to a family history of a [state] 'dossier', I remember that since I was young my parents have always told me to be very cautious with what I would say and to whom, about everything. This happened because my family had been in danger. Therefore, in general and on Facebook, as far as I can, I do not speak politically; I prefer to meet somebody face to face and have such a discussion, instead of posting it [online] while knowing that a third person will get to see it. I do not want to express my opinions online.

Technical vs. legal knowledge and/or perceptions

In the following example, we can see the antithetical attitudes of two participants, both of whom were assessed as particularly interested and active in political affairs. On the one hand, there was the very legally literate professor of law, and on the other, the very technically literate professor of computer science. Both were asked whether they were concerned about surveillance. It is important to clarify here that in both interviews, participants were asked to clarify whether they consider themselves as actual targets of surveillance or potential targets of mass surveillance (e.g. data retention). Both clearly explained that they had often experienced unproven indications that they had been personally targeted due to their political activities. Still, their attitude towards surveillance is contrasting, as the first acknowledges that he is not actively concerned about surveillance although, as he claims, he is certainly under surveillance. The second, on the other hand, states that he does everything possible to oppose surveillance.

> Professor of law: While I am interested in surveillance as an issue, I am not personally concerned; I take for granted that I am a target of surveillance and I don't care […] In any case, if you are a legal expert, you know that even if you are being surveilled, this [data] cannot be used against you […] I personally feel this relative safety.
> Professor of computer science: I know very well that I am being surveilled and I try in every way to prevent the interception of my private files.

Nevertheless, as many participants across methods and groups pointed out, there are certain things they would not disclose in electronic environments. A participant from the left-wing group, Panos, exemplified this attitude and reflected on the legal perspectives of surveillance that are not clear to him:

The legal framework – what is legal and what is not – is not actually clear. There are some crucial moments, in which certain things must not be shared. I may not be [a member] of a terrorist organization but many of the things that you could possibly do, do not fall within the framework of bourgeois law (αστική νομιμότητα (*astiki nomimotita*) in Greek) […]. Some of them may be more extreme, some others not. In any case, in order for these things to be achieved […] what I mean is that, if you want to give a surprise party for a friend of yours, in order for the party to be successful, the surprise element is crucial […] In that sense, I think this is the limit, what the other [the government] can use against you legally or practically in order to obstruct you. It is the trade-off between lawfulness and usefulness. If somebody can use a certain piece of information [against me], even if not legally, in that case I wouldn't use the Internet, not even the phone.

Between self-censorship and apathy

The majority of the participants in the focus groups and interviews were developing different sorts of strategies when it came to political use of ICTs and their personal cybersecurity. On one extreme end of the spectrum of attitudes is, for example, the attitude of a former cybercrime unit officer who stated that he was essentially self-censoring himself in all electronic environments with regards to any political communication, despite his high level of politicization. On the other end of the spectrum, the legal expert is characterized by apathy, as he believes that no matter what he does, surveillance cannot be tackled. In the middle of the spectrum of attitudes, the expert in computer science argues that a person with strong IT skills can fully protect himself/herself against surveillance.

Former cybercrime unit officer: I am totally apolitical in my electronic communications; I have never expressed any political views there.
Professor of computer science: [A]n IT expert can be protected 100% against surveillance.
Professor of law: [I don't take any measures] because I am convinced that whatever I do at an amateur level, somebody who will want to have access [to my data] will have it. Therefore, why should you bother?

The large category of apolitical citizens

Another interesting theme that occurred among the self-proclaimed apolitical participants who appeared to have limited or no knowledge regarding technologies and practices of contemporary surveillance, is that their (imaginative) understanding of surveillance was much more intrusive and darker, than other, more knowledgeable participants, as well as than it is in reality. Zoe, for instance, takes for granted that not only metadata, but also the actual content of all communications is being surveilled:

> Everybody is being surveilled. The phones and movements of all of us. They can at any time track you, see anything, what you said, what you did, with whom you were, where you were […]. I believe that when I speak on the phone to anybody, with my mother, my friends, my colleagues, all of these are being surveilled at any particular moment.

Another participant of the same group, Petros, is certain that the content of every single phone call of every citizens of the country is being recorded and stored:

> I believe that when we speak on the phone, everything is being recorded in the databases of the [telecommunication] companies. Therefore, when the police want to search for me for example, they ask for this data [from the telecommunication companies] and they find what they want.

Thomas, also from the apolitical group, explains that he does not care about surveillance because he has nothing to hide:

> Personally speaking, it is not of my concern even if I am under surveillance 24 hours a day, I don't care, I have nothing to hide or to be afraid of.

Lastly, another common theme that was often discovered during this particular discussion, was the consideration of privacy as luxury. As Petros blatantly put it:

> As I have been unemployed for one and a half years, I have much more important things to be concerned with, rather than surveillance.

Discussion

This study was conducted on a mixed-method research basis that included a survey, expert interviews and a series of focus groups. To my knowledge, this is the first empirical study in Europe that explored the relationship between electronic surveillance and political participation. This chapter limits itself to discussing some of the main findings, while it does not claim to offer strong assumptions that would lead to safe conclusions. Nevertheless, I hope that the demonstrated methodology and insights will be of interest and useful to other researchers working on this complex subject.

A significant percentage of the survey participants were found to be quite or very much concerned about state surveillance capabilities. The significant figure is not surprising when taking into consideration the country's legacy of surveillance (Samatas 2004) and most importantly, the very frequent news coverage about surveillance during the financial crisis.

The research also illustrated that participants who place themselves on the left in politics, tend to be much more concerned about Internet surveillance (including landline, mobile and CCTV surveillance) than any other category of the (a)political spectrum. This can possibly be due to the long legacy of anti-left

surveillance in Greece (Samatas 2005) but also due to the intensification of surveillance during the crisis era since 2008, as discussed previously. Furthermore, the survey results showed a particularly high concern about transnational surveillance among all participants, regardless of political ideology. The magnitude of these percentages can potentially be attributed to the fact that the survey sampling took place a few months after Edward Snowden's revelations about the US and British electronic surveillance practices. Similarly, possibly due to the frequent stories that can be traditionally and historically found in the Greek and international mediated public sphere regarding the intelligence activities of embassies, such as the US (Samatas 2004; Bamford 2015).

Despite the fact that activists on the left side of the political spectrum have traditionally been the main target of surveillance in Greece, and contrary to as one would expect, they frequently appeared in this study as unwilling to take any precautionary measures to protect their privacy against state (or other) surveillance. Their personal ideology appeared to play a significant role in encouraging this unwillingness. To this may be also added the fact that most of them still consider Greece as a place where important democratic and legal rights are safeguarded. This comes as a surprise, given the fact that a significant percentage of participants across research methods and groups appeared to have a particularly high level of concerns about surveillance practices in Greece but also high levels of distrust in public and political institutions and actors, as it was noted earlier. However, many respondents explained that their stance would not have been the same, should they have lived in more authoritarian regimes.

There has been a lot discussion over the last few years around potential chilling effects of surveillance. Contrary to the phenomenon pointed out in the previous paragraph, Greece's legacy in state surveillance (Samatas 1986; 2004) appeared to have left its imprint upon certain people's online attitude in the context of politicization. Concerns about electronic surveillance did indeed create chilling effects on several occasions, as this study has shown. This was the case particularly with younger participants, like the aforementioned sociology student, whose willingness to participate online was cautious due to past surveillance experiences. Moreover, in the case of the compared attitudes of the three experts (that entailed characteristic discrepancies with regards to their political use of ICTs) one of them explained that he essentially self-censors his political views online, despite the fact that he is very much interested and active in politics in the offline world.

Another interesting finding is that those who have very strong computer skills and are politically active (example of the professor of computer science), appear to be more proactive in resisting to surveillance by taking personal cybersecurity measures. On the other extreme spectrum of behaviour, those who are very knowledgeable about the legal aspects of surveillance (as for instance the professor of law) tend not to be afraid of such practices, as they feel that their legal capacities would protect them from facing any consequences. In that sense, legal and technical knowledge/perceptions played an opposing role in modifying attitudes towards personal cybersecurity mobilization against surveillance. Interestingly enough and to complicate things further, citizens' online attitude and behaviour in

the political context appeared sometimes as a trade-off between lawfulness and usefulness, as the quotation from the left-wing activist earlier indicated.

The large category of apolitical citizens would also deserve further investigation. The insights discussed earlier have two broad implications for theorists, advocates, and journalists. First, the simple raising of individuals' awareness regarding surveillance practices, does not seem to suffice in mobilizing apolitical citizens to take measures to protect their privacy and/or anonymity. The reason is that, even if these individuals would increase their level of knowledge and understanding – by reading for instance more about Snowden's revelations – they would only come to confirm their gloomy a priori imagination and perception of surveillance. Second, although new media and ICTs offer new affordances of democratic participation to those who are disengaged, this very presumption could potentially chill in advance any willingness for such participation.

An important conclusion is that perceptions, attitudes and behaviour regarding privacy, personal cybersecurity and surveillance are multidimensional, can be linked to numerous issues and vary significantly across different contexts. Similar to Helen Nissenbaum's argument for the importance of contexts (2009), this study shows the importance of neglected aspects that need to be taken into consideration when studying surveillance and political behaviour, such as the ideology and the sociopolitical context of the explored sample or population. Researchers need to pay closer attention to important critical questions that are tied to the political economy of surveillance (Fuchs and Trottier 2015), ones that would reveal power asymmetries, inequalities and effects of the capitalist crises in attitude and behaviour. For instance, it is fundamentally different to analyse the attitude and behaviour of left-wing activists, right-wing citizens, and apolitical citizens in Greece during the period 2008 to 2014. Another characteristic example was that of the attitude of the apolitical citizen who emphasized that he did not care about surveillance as he had 'much more important things to be concerned with', which can be attributed to his precarious position during the crisis era.

Limitations

This study attempted to operationalize a mixed-method approach in order to better understand the relationship between electronic surveillance and political participation in Greece. In doing so, it conducted a survey, and a series of focus groups and interviews with experts. However, due to restraints, the survey used a convenience sampling technique that limits a researcher's capability in forming strong conclusions and in operationalizing inferential statistical analysis, which could test in a more accurate way such assumptions. Equal restraints were imposed upon the number of participants recruited for the interviews and focus groups. Future studies could interview a wider range of experts, as well as include citizens who position themselves upon the right or far-right of the political spectrum. In addition to that, future research could conduct comparative analysis that would explore the aforementioned insights in different national, social, and political contexts.

Notes

1   The field trip for the collection of the empirical data presented in this chapter was supported by funding from the International Office of the University of Vienna.
2   Although the Greek crisis continues up to the moment of writing, this study focused on the period between 2008 and 2014.
3   In this example, the main opposition is the left-wing political party SYRIZA that came in power in 2015.

References

Apostolakis, S. (2013) 'Interviewing Is a Crime', *Eleutherotypia*, In Greek, Online. Available at: www.enet.gr/?i=news.el.article&id=393947 (accessed 25 March 2014).

Bamford, J. (2015) 'A Death in Athens. Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?', *The Intercept,* Online. Available at: https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/ (accessed 24 October 2015).

Best, S. J. and Krueger, B. S. (2011) 'Government Monitoring and Political Participation in the United States: The Distinct Roles of Anger and Anxiety', *American Politics Research,* 39(1): 85–117.

Coleman, R. and Sim, J. (2000) 'You'll Never Walk Alone: CCTV Surveillance, Order and Neo-Liberal Rule in Liverpool City Centre', *British Journal of Sociology*, 51(4): 623–639.

Cunningham, D. and Noakes, J. (2008) 'What If She's from the FBI? The Effects of Covert Forms of Social Control on Social Movements', in M. Deflem (ed.) *Surveillance and Governance: Crime Control and Beyond,* Bingley: Emerald Group Publishing, 175–197.

Denscombe, M. (2010) *The Good Research Guide. For Small-Scale Research Projects,* Fourth Edition, Maidenhead: Open University Press.

Dinev, T., Hart, P. and Mullen, M. R. (2008) 'Internet Privacy Concerns and Beliefs about Government Surveillance – An Empirical Investigation', *Journal of Strategic Information Systems,* 17: 214–233.

Doyle, A. (2003) *Arresting Images: Crime and Policing in Front of the Television Camera*, Toronto: University of Toronto Press.

European Social Survey (2010) ESS Round 5 Data, Data file edition 3.0. Norwegian Social Science Data Services, Norway – Data Archive and distributor of ESS data for ESS ERIC. Online. Available at: www.europeansocialsurvey.org/data/download.html?r=5 (accessed 30 April 2013).

Flash Eurobarometer 225 (2008) Data Protection in the European Union. Citizens' Perceptions, 'Gallup Organization Hungary' upon the request of Directorate-General Justice, Freedom and Security of the European Commission.

Fuchs, C. and Trottier, D. (2015) 'Towards a Theoretical of Model of Social Media Surveillance in Contemporary Society', *Communications*, 40(1): 113–115.

Habermas, J. (1962; 2nd edn 1989 [1962]) *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*, trans. T. Burger, and F. Lawrence, Cambridge, MA: MIT Press.

Haggerty, K. D. and Samatas, M. (2010) 'Surveillance and Democracy: An Unsettled Relationship', in K. D. Haggerty and M. Samatas (eds) *Democracy and Surveillance,* New York: Routledge, 1–16.

Katrougalos, G. (2013) 'How and Why Surveillance Takes Place?', *Eleftherotypia,* In Greek, Online. Available at: www.enet.gr/?i=news.el.article&id=392223 (accessed 25 March 2014).

Klandermans, B. and Oegema, D. (1987) 'Potentials, Networks, Motivations, and Barriers: Steps towards Participation in Social Movements', *American Sociological Review*, 52(4): 519–531.

Marx, G. T. (1974) 'Thoughts on a Neglected Category of Social Movement Participants: The Agent Provocateur and the Informant', *American Journal of Sociology*, 80(2): 402–442.

Mitrou, L. (2008) 'A Pandora's box for Rights and Liberties', in *Digital Privacy: Theory, Technologies and Practices,* in A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis and C. Labrinoudakis (eds) *Digital Privacy: Theory, Technologies and Practices*, Boca Raton, FL: Auerbach Publications, 409–433.

Nellis, M. (2007) 'Electronic Monitoring and the Creation of Control Orders for Terrorist Suspects in Britain', T. Abbas (ed.) *Islamic Political Radicalism*, Edinburgh: Edinburgh University Press.

Nissenbaum, H. (2009) *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford, CA: Stanford University Press.

Ravanos, A. (2013) 'Disagreement between the Government and Syriza on Phone Surveillance from the National Intelligence Service', *To Vima*, In Greek, Online. Available www.tovima.gr/politics/article/?aid=533978 (accessed 25 March 2014).

Samatas, M. (1986) 'Greek McCarthyism: A Comparative Assessment of Greek Post-Civil War Repressive Anticommunism and the US Truman-McCarthy Era', *Journal of the Hellenic Diaspora,* 13(3, 4): 5–75.

Samatas, M. (2004) *Surveillance in Greece. From Anticommunist to Consumer Surveillance*, New York: Pella.

Samatas, M. (2005) 'Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture', *Surveillance and Society,* 3(2/3): 181–197.

Samatas, M. (2010) 'The Greek Olympic Phone Tapping Scandal. A Defenceless State and a Weak Democracy', in K.D. Haggerty and M. Samatas (eds) *Democracy and Surveillance,* New York: Routledge, 213–230.

Smith, H. J., Dinev, T., and Xu, H. (2011) 'Information Privacy Research: An Interdisciplinary Review', *MIS Quarterly*, 35(4): 989–1015.

Solove, D. J. (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet,* New Haven, CT: Yale University Press.

Special Eurobarometer 359 (2011) Attitudes on Data Protection and Electronic Identity in the European Union, TNS Opinion and Social at the request of Directorate-General Justice, Information Society and Media and Joint Research Centre of the European Commission.

Wolff, B., Knodel, and Sittitrai, W.. (1993) 'Focus Groups and Surveys as Complementary Research Methods: A Case Example', in David L. Morgan (ed.) *Successful Focus Groups. Advancing the State of the Art,* Newbury Park, CA: Sage, 119–136.

13 In quest of reflexivity

Towards an anticipatory governance regime for security[1]

Georgios Kolliarakis

Public policy resembles large-scale, real-time complex experiments with uncertain outcomes. While policies may deliver on their set objective, at least partially, they more frequently than not misfire, by making no difference, or even backfire, by triggering undesirable side effects. This applies particularly to contemporary security policy, and, by default, to security research policy. 'Security' has advanced in the past decade to a *master frame* in Western politics, substituting 'peace' or 'welfare' as the guiding narratives in a hyper-connected world of consecutive crises and new forms of violence (ESF 2015). At the same time, provision of security bears all traits of a controversial *wicked problem*: Security is subject of a value-laden, contentious public policy field, with ill-defined problems (threats and risks), where available solutions often define the challenge, instead of vice versa (Kolliarakis 2013). What is more, security policies seem to be intimately dependent upon economic, social and, not least, legal policies. The complexity of the networked, multi-layered policy environment, the ambiguity due to diverging values and ideologies, and the uncertainty in cause-effect relations, render security policy into a moving target, difficult to evaluate and assess its future impacts. The specific focus of the present volume on security and privacy addresses exactly such a 'moving target' policy problem (Friedewald and Pohoryles 2013). In the face of the recent terrorist attacks in Europe, and the recurrent patterns of security responses pushing for more intrusive control, this chapter takes the controversies about privacy, data protection, and security, to be symptomatic for a second-order clash about the normative and empirical premises of public policy. In this regard, this chapter will zoom out from the many cultural and legal aspects of the specific privacy–security issues, and will, instead, address the fragile and, in some respects, biased epistemic regime for security policy and research at EU level. In this context, research is taken to be a key proactive form of security policy by generating a pool of potential solutions in the short or middle term (Kolliarakis 2014).

Knowledge available at the Science-Policy interface (SPI) in the form of data, ex-ante assessments and ex-post evaluations, ought to flow in policy design in order to ensure that security policies are *fit for purpose* and effective for the sake of public interest, and they do not *misfire,* causing opportunity costs, or even worse, *backfire*, causing undesirable non-intended consequences (European Commission 2012b). Ironically enough, scarcely any comprehensive evaluations of effectiveness,

appropriateness, or proportionality of measures, or any systematic democratic control, have taken place so far. Unlike other contentious public policy fields, such as those of public health, education, or welfare policy, lack of transparency and inclusive deliberations, has been the standard mode of security policy exchange, even in the EU liberal democracies. What is more, citizens, as principal stakeholders and ultimate beneficiaries of security policies, are habitually sidestepped when deliberating about the diagnoses of threats, about the desirable goals of security policies, and about the measures and instruments to achieve them. The nature of security as a *public good*, enshrined in most constitutions as such, gets inadvertently or intentionally left out of sight thereby.

The chapter proceeds by elucidating key dimensions of a reflexive governance regime. First, in the context of the emerging 'civil security' paradigm in Europe, security is described as a *wicked problem* par excellence. Such problems routinely receive 'clumsy', piecemeal solutions, which are often ineffective, or may even blow back. The contested, shifting relationship between privacy and security, as either competing or mutually reinforcing relationship, serves here as an illustrative case. The various and fluid trade-offs between security and privacy, non-discrimination, equality, seem to curtail civil liberties without guaranteeing higher levels of societal security.

Second, the chapter goes over to the *problematique* of the elusive evidence base for security policy. Secrecy around 'sensitive' security-relevant data, make policies vulnerable to ideological arbitrariness and to particularistic interests. For example, it has been often criticized by security practitioners and critical activists alike, that it is not the lack of citizens' data, but, reversely, the abundance of such data which poses a problem. It seems, at least in some cases, that public authorities store far more data than they can usefully process. The security domain ought to follow step in the more inclusive deliberative direction other contentious public policy fields, such as public health, have taken. In the realm of social policy, an international NGO, the Campbell Collaboration, has examined from a criminological perspective, effectiveness of CCTV surveillance, and of counter-terrorism strategies. While evidence-informed practices, such as RCTs (Randomized Control Trials) in medicine and public health are standard in order to prove whether a drug is effective and efficient in its practical impact, policies about public security are far from following similar guidelines. Moreover, integrating citizens' values and ethical concerns into the scientific evidence base for security policy in the face of rising complexity, ambiguity and uncertainty, seems to be a precondition for delivering socially robust knowledge for sustainable policies. In line with accounts of *post-normal science* and *Mode-2 knowledge production*, this would entail integrating, upstreaming and streamlining citizens' participation into the security research and policy cycle.

Third, this chapter will turn to the dimensions of reflexiveness for security (research) policy. Besides the 'backward-looking' aspect of *legal and ethical compliance*, which provides normative cues for agency, it is, moreover, the anticipatory, 'forward-looking' mode which provides prospective responsiveness and responsibility in going about with a contentious societal issue. Codified as mandatory for

EU-level policies, regulatory impact assessments (RIAs) should consider the effects of a certain policy in economic, environmental, and social aspects, and also comply with sustainability and fundamental rights principles. RIAs should guarantee that a policy is *fit for purpose*, and that non-intended negative side effects are acceptable and overbidden by the benefits. Following that, the chapter makes a strong plea for putting an *anticipatory governance regime for security* in place, focusing particularly on security research as a proactive, high-risk/high-gain domain of public policy. This would, on the one hand, be in line with the precautionary principle, as well as with the guidelines for good governance at EU level, transgressing and involving politics, policies, and all relevant stakeholders on the ground. Anticipatory governance aims, in that respect, at preserving values, and social fabric of polities, while minimizing the probability of disruption of an acceptable way of life.

The chapter concludes with an outlook on the prerequisites for a *responsive and responsible* security research policy. Power asymmetries among stakeholders go hand in hand with divergent interests, and influence in setting the agenda in favour of the one or the other side. So it occurs more often than not that societal actors from the civil society with crucial stakes in public security and safety have very weak leverage as a result of poor access to decision-making processes. With several policy principles and legal provisions already in place, pursuing inclusive, legitimate and accountable security agendas, including security research, is an increasingly obvious precondition for informing effective future policies. Yet, without establishing a reflexive anticipatory mechanism around inclusive knowledge production, and comprehensive impact assessments, security policies are bound to remain susceptible to political opportunism and actionism, and captive to particularistic economic interests. There is currently a pressing need to open up the security (research) policy regime to citizens' and civil society actors, and sensitize it for organizational and institutional, non-tech aspects of security measures within the context of application.

Security as a 'wicked problem' in public policy

Security has traditionally been one of the defining traits for the modern (and, surprisingly, even more so of the post-modern) state. From Thomas Hobbes' seventeenth-century *Leviathan*, to twentieth-century Michel Foucault's studies on surveillance and social control, security has provided, if always at a price, the foundational legitimacy, the *raison d'état*, constituting the relationship between citizens and political administration. Security has been inscribed, more or less visibly, into the political cultures of societies, by establishing membership criteria for the inside/outside of the community, and by defining red lines and zones of threat acceptance or intolerance, constructing thereby political 'normality', or political 'exception', respectively. The current controversies about how far counter-terrorist policies of surveillance should go before infringing fundamental rights in the name of providing more security, reflects the above tension.

The current state of affairs, where the clear-cut Cold-War-like orders and taxonomies have given way to messier and fuzzier threat landscapes, has given rise

to the paradigm of 'civil security', a European variant of the US 'homeland security' (Kaunert *et al.* 2012). Citizens are seen to be at risk from omnipresent, yet not always easily identifiable threats. First, the domestic and foreign dimensions are blurred, resulting in an unsettling of the traditional civil/police and military/defence fields. Second, cascading accidents cannot always be clearly distinguished from attacks, or vice versa, mixing thus discourses about 'safety' with discourses about 'security'. Third, the *logic of prevention* has been complemented in competing policy and academic discourses by the *logic of resilience*, signifying a creeping shift of focus from the source of the threat, towards the target of the threat (Kolliarakis 2013).

Currently, security research as practised in Europe since the middle of the first decade of the twentieth-century, attempts to respond to gaps both in knowledge and in capacity with regard to emerging security challenges, by prioritizing areas such as cybercrime, counter-terrorism and radicalization, organized crime, crisis management, and border control. It has done so, though, by narrowing down the possible paths, focusing on the technological side of security, namely, detection of CBRNE (chemical, biological, radiological, nuclear, and explosive agents), research on biometrics and pattern recognition for profiling and predictive analytics as in CCTV, RFID (radio frequency identification), or on remote positioning identification, as in the case of UAVs (unmanned aerial vehicles), such as drones, and DPIs (deep packet inspection) for data flow interception, mining, and matching purposes (European Parliament 2014, ESF 2015). The – more implicit than explicit – assumption behind that research direction, is that such high-tech tools substantially enhance early-warning and prevention capacity, in order to protect citizens and critical assets. However, rather scattered indications but by no means compelling evidence has been brought to light so far to support the assertion that such technologies are appropriate, effective and proportional for the defined purposes.

This chapter maintains that governance of public security under those circumstances needs to be recast: from effective implementation of security measures, which should not generate more problems than they solve, back to security research, which ought to anticipate and analyse threats and reflect their optimal societal remedies and measures. The term governance alone hints at the multi-actor, multi-level assemblages of diverging problem framings and interests, of technological artefacts, and of legal, institutional, and cultural contexts in which security policy decisions are made and implemented. Governance of security policy comprises an array of instruments, from 'hard' legal codification, to 'soft' policy incentives, rules of conduct, and, not least, research funding. It is not always obvious, that security research policy is an integral, core component of security policy by providing crucial epistemic lenses to identify and evaluate phenomena as security relevant. With a strong proactive dimension, security research creates a series of focal areas for security policy makers, along with a pool of instruments to be drawn upon in the short to middle term by future security policies. In such a governance context, citizens are most of the time taken to be addressees and objects, but not active agents and influencers of security architectures.

It has been critically observed by scholars and civil society activists alike, that the security research regime, established in the EU in the aftermath of the New York, Madrid and London terrorist attacks of the past decade, has been predominantly supply-driven, taken captive by the defence technology industry in search of new markets (Statewatch 2009, European Parliament 2014). This came at the cost of an explicitly demand-driven foundation, led by evidence-informed analysis of security providers' and citizens' needs on the ground.

Having said that, it becomes increasingly visible that in certain domains of public policy, decision makers cannot conclusively 'solve' problems, but, at best, cope with them for a period in time and in a certain geographical context. The development of more scientific expertise and technological innovation cannot conclusively respond to interconnected societal challenges by applying 'engineering' rationalist approaches. Security qualifies as an archetypical *wicked problem* of public policy. Wicked problems are generally defined as the result of interest and value divergence among competing stakeholders, institutional complexity due to multi-level and inter-organizational governance, and, not least, of scientific uncertainty as in lack of reliable cause-effect relationships (Head and Alford 2015). The domain of wicked policy problems can in this respect depicted as the convergence area of complexity, uncertainty and ambiguity, as in Figure 13.1 below.
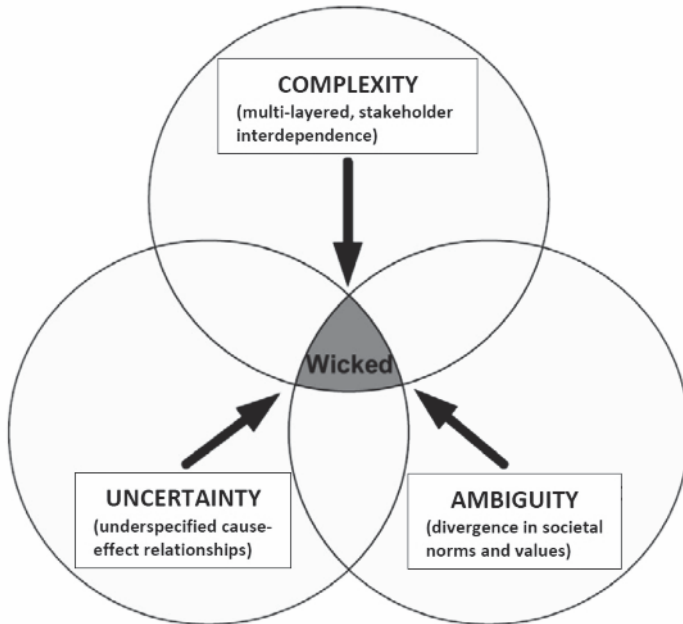
Figure 13.1 The dimensions of wicked problems

Source: adapted from: Head 2010, p. 22.

Rittel and Webber had already pointed to wicked problems in 1973 by identifying a series of common characteristics in them: from the existence of contested, ill-contoured definitions, to the absence of a shared validation mechanism about when the problem is solved, to the interconnectedness and second-order effects they trigger (Rittel and Webber 1973). Stakeholder disagreement in framing the problem on the background of incompatible interests, and consequently, the contest about what counts as a problem in the first place, and what is the preferred course of action, are essential in grasping the dynamics of wicked problems, such as public security. The role of values, institutions, and culture visibly compromises the power of scientific evidence to deliver unequivocal solutions to policy puzzles. As Head and Alford stress, provision of certitude through knowledge is only one part of dealing with complexity and ambiguity. Besides cognitive-analytical challenges, there are communicative, political, and institutional ones in order to proceed to solutions (Head and Alford 2015: 719). Yet, what happens most of the time is the delivery of 'clumsy' solutions, trapped in between bureaucratic inertia and interest-group politics. Such policy solutions are characterized by 'muddling-through' and contradictory or ambiguous goals (Lindblom 1979, Rainey and Jung 2015), which are often either self-undermining, and do not bear fruit, or are not fit for purpose, and prove to be counterproductive.

Security research as security technology research manifests an additional twist in the above analysis. In the field of science, technology and innovation, it is often the case that research generates not merely solutions to policy problems, but also new controversial value-laden policy problems, raising interest conflicts among the involved stakeholders (Biegelbauer and Hansen 2011). Citizens in Europe, as documented in a series of large-scale comparative Eurobarometer surveys, asked about 'Internal Security', 'e-Identity', or attitudes towards 'Science and Technology', and 'Responsible Research and Innovation', have mixed feelings when it comes to deciding between risky impacts of technologies contrasted with the immediate benefits they draw out of them: while EU citizens seem to accept the intrusion of online technologies with all their accompanying risks in their everydayness, yet they would prefer to stop technology R&D with uncertain or negative impacts on their fundamental rights. Accordingly, most of the time security concerns need to be balanced against or reconciled with privacy and freedom of expression, along many other societal values, of economic, legal, or ethical natures. As in most areas of public policy, the resort to the *trade-off model* delivers pragmatic compromise formulas (often 'clumsy solutions'), in most societal areas in a pluralist democratic polity. This is the angle from which this chapter views the variable relationship between 'security' and 'privacy', as interdependent moving public policy targets.

The wicked ambiguity between security and privacy

If one wishes to delve more deeply into the shifting 'wicked' dynamics between privacy and security in the face of the proliferation of security-relevant technologies, the scheme of a normal distribution in the function between *citizens' perceived privacy* and the *intensity of security provision* respectively, could visualize the

ambivalence. A bell curve, formed as a function of the two variables, 'privacy' (verti-
cal axis) and 'security' (horizontal axis) respectively, could offer some theoretical
insight into a scarcely explored heuristic. The normal distribution can be roughly
split into three distinct phases: In the first one, 'security' is low but 'privacy' grows
exponentially. Symmetrically, in the third phase of the curve, security provision is
very intense, but privacy sinks exponentially. It is at the rather narrow middle-top
field of the curve, where one could say that an optimum balance area for both secu-
rity and privacy exists, as could also be described by a Pareto equilibrium. In that
phase of the curve, 'security' and 'privacy' are more or less in a balanced relationship.
After that narrow 'top' phase of the curve, which can be seen to be a 'tipping point'
in the curve between the two slopes, the function between 'security' and 'privacy' is
reversely analogous, in plain words, an *antagonistic trade-off*: the more security, the less
privacy. Citizens complain whenever they perceive a deficit in protection which
hinders them from fulfilling their day-to-day business, but they also reject security
provisions which violate established freedoms with no plausible justification. For
example, Americans who otherwise stated since 2004 that the US government did
not do enough to protect them, responded in July 2013 (after the revelations by E.
Snowden) in a survey conducted by the Pew Research Center saying that the US
government security policy had gone too far in restricting civil liberties.[2]

   A paramount consequence of the relationship between 'security' and 'privacy' as
moving targets in public policy, is drawn from the law of 'diminishing returns', that
is, there is always a point where the beneficial effects of security provision, if it goes
too far, will strike into the opposite direction and, unintentionally, backfire. This
dynamic lies behind phenomena such as the 'security paradox' (the higher security
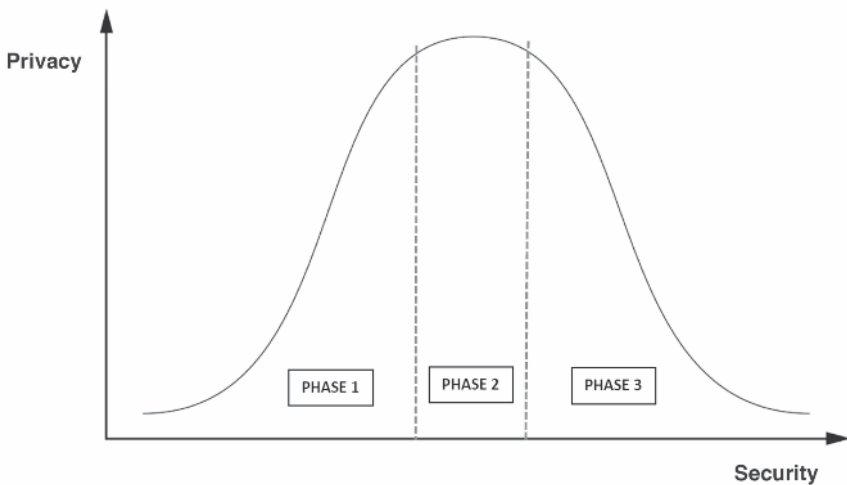
Figure 13.2 A heuristic model of the variable privacy–security relationship

levels, the more insecure people feel), already elaborated in the 1980s by Adalbert Evers and Helga Nowotny (1987).

This 'wicked' ambiguity is consequential for security policy practice: different stakeholder communities premise their claims for security action upon framing privacy (as a fundamental or derivative right) and security (as an enabling precondition for freedoms, or as a pretext for violation of freedoms) with different weight within one of the three phases of the curve as depicted above. Security technology developers for example, criticize that when privacy has priority, security measures cannot intrude deep enough to tap relevant information in order to guarantee effectiveness (phase 1). Human rights advocates, or 'critical security' scholars, on the contrary, claim that whenever security considerations take the lead, then rights and liberties get necessarily undermined and this leads, counter-intuitively to more instead of less insecurity (phase 3). Policy makers and, among others, many authors in this volume, support a win-win frame for privacy and security, as it is found in phase 2, at the top of the bell curve. Such an optimistic 'positive-sum' angle to view the security–privacy relationship allows for introducing corrective instruments, such as privacy-enhancing technologies (PETs), in order to pursue security objectives without compromising on civil liberties. At the same time, the top of the curve visualizes a very unstable equilibrium on a rather narrow area. The heuristic model above can accommodate all conflicting manifestations of the relationship, and can serve as an evidence-informed compass to security policy-making. The ongoing debates about the utility of indiscriminate, pre-emptive surveillance, or the feasibility of preventive targeted surveillance, particularly in combination with 'big data' mining, also from social media, underline the point. Furthermore, a series of EU initiatives in the context of the European Border Surveillance System and the 'Smart Borders' policies, but also with regard to the Passenger Name Record and the Terrorist Finance Tracking Programme, to name only a few, still need to undergo rigorous regulatory impact assessment (European Parliament 2013). Yet, the path to flesh out such security–privacy heuristics with evidence has still to be taken, both by researchers and policy makers, and this is premised upon a series of conditions, as laid out in the two next sections.

The elusive evidence base and the need for socially robust knowledge for security

The generalized trend since the turn of the millennium toward evidence-based public policies, originating in public health and in environmental politics, aims at providing scientific tools for their assessment and evaluation in order to make them less vulnerable to ideological arbitrariness, to manipulative spin, or to particularistic interests (Watts 2014). Nevertheless, there is a series of enabling and constraining conditions in order to open up the science-policy interface for the production, dissemination, and uptake of evidence. Quality of data, transparent methodologies allowing scrutiny, independent knowledge brokers, but also a receptive policy-making environment are some of them both from the supply and from the demand side (Banks 2009). In this context, Rob Watts has questioned not merely the

capacity, but also the will of public institutions, despite the reiterations about rational problem solving, to adopt evidence instead of 'political ideology', or opportunistic spin as a guide to designing policies (Watts 2014). If evidence-informed policy is not only a supply, but also a demand problem, then one should always be wary of politically constructed and sustained 'ignorance', which denies, suppresses or distracts from uncomfortable knowledge and non-mainstream alternatives, creating itself risky *unknown knowns* (Kolliarakis 2017, forthcoming). On the other hand, 'science' cannot be expected to deliver unequivocal or uncontested evidence along a single, jointly shared paradigmatic narrative to policy makers, as they would like to have it. Public policy decisions have to be made, almost invariably, against the background of missing, diverging, or contradictory evidence and conflicting interests, yet always taking into account the 'public good' dimension (Slob and Staman 2012).

Concerning European citizens' wish-lists about levels of security and of privacy, even properly designed and conducted large-scale comparative surveys, which make an important step towards delivering snapshots of the 'public opinion', provide at the end of the day less than meets the eye in order to inform robust security policy. Even more so, the latest mantra of 'Big data' generated to a high degree through transactions by citizens themselves, are (mis-)taken to speak directly for themselves, by providing a patterned representation of reality. This fallacy systematically conflates the distinct processes of transformation of *data* into *information*, of *information* into facts and evidence, and of evidence into *actionable knowledge*, relevant and usable for policy. Policy blinders through vested interests, or distortions and errors due to the new 'algorithmic' objectivity, interfere in the process of *making sense* and *making use* of the 'raw' data material for justification and regulatory purposes. The 'big data' hype is not, of course, merely an illustrative case for the methodological challenges faced by contemporary research, but also extremely consequential for the self-disposal of citizens and the data they intentionally or non-intentionally generate (Kitchin 2014, Lyon 2014). Warnings about the potential misuse of massive and indiscriminate data collection for intelligence purposes in the context of pre-emption after 9/11 have been voiced long before the Snowden revelations in 2013 (Amoore and de Goede 2008), and such concerns have long related directly to the theme of the present volume.

The reality on the science-policy interface (SPI) is still for the moment dominated by a strong quantitative, econometric paradigm. Evidence, evoking the claim of objectivity, encompasses accordingly everything that can be made visible, quantifiable, measured via indicators, and compared through various metrics (Porter 1995, Saltelli and Giampietro 2016). This positivistic, empiricist phantasy of modernity about the objective and reliable scientific knowledge has been a trap for security policy as well (Neal 2013). The issue of what and whose facts qualify as policy-relevant evidence is bound to remain a contentious issue, particularly in 'wicked' public policy fields vulnerable to ideology and spin. When it comes to 'evidence-marketing' contests, factors, such as economic and political interests, but also ethical, cultural, and institutional parameters, come into play. Science and technology delivering 'new' knowledge seems to be only one part of the equation. Research, particularly in fields such as that of security, must increasingly address

issues that cannot be reduced to purely scientific or purely technical facts, and link them with organizational and institutional practices (Nowotny 2003). Transforming research results into socially robust knowledge takes considerably more effort and conflict, since it raises thorny questions about *whose knowledge is to be incorporated into official public policy, for which purposes, and for whose benefit* (Nowotny 2007).

Liberatore and Funtowicz (2003) have listed four models for the SPI which reserve different roles for evidence as produced and used by stakeholders in policy-making: the *precautionary model,* the *demarcation model,* the *framing model,* and the *extended participation model*. In the *precautionary model*, scientific uncertainty allows and mobilizes other types of knowledge, in order to avert irreversible consequences. In the *demarcation model*, scientific expertise provides an external justification template to support policy-making, which remains the responsibility of democratic institutions. In the *framing model,* policy reflects contests by competing stakeholders to set or influence the agenda, so the required evidence is often influenced by political commitments. Last, the *extended participation model* postulates that science is a crucial but not exclusive form of knowledge, and citizens can also be, besides users, also producers of knowledge. This inclusiveness ought to enhance procedural legitimacy and quality of knowledge (Liberatore and Funtowicz 2003: 148–149).

At EU level, the latest since the 2001 White Paper on Good Governance, aimed at reducing risks out of policy choices, there exists a normative frame of open and inclusive deliberations, along with the codification of the precautionary principle in the Treaty of the European Union (§ 191). Yet, the reality of which 'facts' flow into the policy-making process as relevant evidence is characterized by strong lobbying by economic interests (Stirling 2015). EU institutions seem to follow the 'demarcation' style, claiming to separate policy from science, while, simultaneously, they allow public and private organizations to compete for promoting their particular problem and solution frames. Since the launch of the European Security Research Programme (ESRP) in 2004 as a research instrument to serve the European security strategy, the share of stakeholders engaged from the established and the emerging (defence) industry, and from research and technology organizations has been disproportionally strong. This has been the case in all *ad hoc* and semi-permanent advisory organs of the European Commission (e.g. the Group of Personalities 2003–2004, the European Security Research Advisory Board (2005–2006), and the European Security Research Innovation Forum (2007–2009) (European Parliament 2014). The unbalanced, weak participation from the side of socio-economic sciences and humanities, and civil society organizations, has resulted into a bias in the sort of 'facts' which dominated the agenda, and pushed security research along a technology-driven path. The rather scarce external evidence about the effectiveness of counter-terrorism measures (Campbell Collaboration 2009), and the non-significant effect of CCTV surveillance on crime (Campbell Collaboration 2008), has been delivered by the Campbell Collaboration, an international NGO dedicated to delivering evidence-based systematic reviews on social-policy issues in order to improve decision-making.[3] In

contrast, the vast majority of the commissioned studies by the European Commission address the potential of civil-military synergies, the structure and competitiveness of the EU security industry, and the overcoming of research-to-market barriers for security technologies market.[4]

Although ethical, and 'societal' aspects are integrated at large in the practice of research conducted at EU level, the predominant focus in the *context of technology development*, largely blends out societal, political, legal and ethical controversies, which arise in the societally 'thick' *context of application*, where a different mix of stakeholders, responsible for implementation of security measures and the interaction with citizens come together. Embedded into the EU master narrative that technological R&D should foster innovation, employment and enhance competitiveness, most current research about the interrelation about privacy and security is premised on the commercialization aspect of research results, such as for example PETs and encryption. Substantial dialogue, not to be mistaken for co-optation-disguised-as-integration, among the researchers', the technology developers', and the policy makers' communities, and, not least, citizens and civil society organizations, is sorely missing there.

Participatory science and technology research, ranging from consultation to co-regulation, takes on board citizens and other societal stakeholders by transforming them from addressees and passive recipients into active shareholders and agents of innovation. This, in turn, has an impact on the topics of the agenda, which become better anchored in the practical realities on the ground. Allowing for plural knowledge via engagement of civil society actors in S&T research issues has been promoted, not least on the grounds of enhancing transparency, accountability, and institutional trust (Kolliarakis 2016, Rask *et al.* 2012). The European Commission has explicitly addressed those issues in the face of conflicting views and interests of involved stakeholders also in the context of impact assessments for regulatory measures. These provide a good starting point for reflexive and responsive governance of security.

Reflexiveness and the mechanism of impact assessments

How does one *make sense* and how does one *make use* of evidence in order to turn security policy more effective but also reflexive with regard to safeguarding civil liberties and fundamental rights? Reflexiveness evokes the image of responsive exchange between policy-in-the-making, on the one hand, and established principles, for example in law, on the other, whereby the former should be informed by the latter. That form of 'backward-looking' reflexiveness has been so far studied as *normative compliance* to existing laws and ethical principles over the past decade. However, there is a second, far less pursued path, which connects with the 'forward-looking' dimension of reflexiveness, namely the *anticipatory* one. Anchored in the precautionary principle, it aims at imagining desirable and undesirable future outcomes out of probable and possible technology application. Participatory foresight and a series of targeted technology assessment methodologies with regard to ethics, privacy, or societal issues have produced a growing body

of literature, yet all proposed tools have to ripen and get consistently transferred into the practice of security policy both at EU and at national levels (Giesecke 2012; Wright and Friedewald 2013).

The core rationale behind assessments of security policy, and, by default, of security research, is exactly to sensitize here and now about the eventualities of the context of application. Three core questions thereby relate to whether the actions pursued are about to 1) *deliver* on the set objectives; 2) *misfire*, that is, make no significant difference; or 3) *backfire*, that is, have counterproductive negative effects. In the two latter cases, it is obvious that regulatory interventions may be proactively needed, in order to minimize opportunity costs, as in the second case, and avert non-intended non-desirable and non-reversible consequences, as in the third case (European Commission 2012a). No comprehensive, publicly accessible, ex-ante or ex-post assessments exist as of now for the multiple instruments deployed under the priority areas of the 2010 Internal Security Strategy, and its further development after April 2015 (European Commission 2015b). Partial critical assessments have been initiated by diverse committees of the European Parliament, regarding concrete subfields, for example 'Cybersecurity and Cyberpower' (European Parliament 2011), drones (European Parliament 2012), or the performance of the foreign dimension of the European Security Strategy (European Parliament 2015). Particularly in the field of counter-terrorism, recent studies have, however, demonstrated that policy makers are inconsistent when it comes to applying evaluation criteria to check for effectiveness of implementation (de Londras and Doody 2015).

Besides the lack of transparency, mostly due to 'security considerations', which is a major obstacle, it is the lack of institutionalized, systematic and comparable data collection about implementation and performance of policy measures across national and international security agencies, and the practice of 'lamp-posting', looking for data where it is convenient, but not necessarily at the relevant places, three central barriers hampering availability and quality of evidence. As far as ex-ante assessments are concerned, the studies published by the European Commission have been almost exclusively focusing upon economic, market and industrial competitiveness dimensions around security research actions. A series of policy documents (European Commission 2007, 2009, 2012; ECORYS 2009, 2012c) seem to cover a narrow, market relevant aspect of security technology R&D, but not the effectiveness or the desirability of their application.

The multiple, and partially competing objectives of the ESRP mandate (European Commission 2014a, p. 1) could account for the path dependency in the direction of evidence gathering. The so called 'societal dimensions' have been treated as corollary, side aspects, relevant when it comes to the acceptance of security R&D in society, by providing ethical and legal pedigrees in order to enhance marketability (European Commission 2015). Blending out the 'soft' societal context from the high-tech solutionist master frame for security is risky: it deprives evidence, evaluations and assessments from crucial knowledge about enabling and constraining conditions for the prospective effectiveness, legitimacy, accountability, and sustainability of the promoted security solutions. Those aspects need to be present in the considerations of decision makers throughout the policy cycle.

Regulation development in contentious policy fields at EU level (besides security policy, also renewable energy, GMO authorization, shale gals, endocrine-disrupting chemicals, Nano-tech, etc.) should undergo a regulatory impact assessment (RIA) to check that legislative/non-legislative measures are: *fit for purpose* (effective); *proportional* (benefits outweigh costs); *informed by scientific evidence*; *value-adding to other EU policies* (coherence, compatibility). The guidelines (see Table 13.1 below), originating in the EU 'Smart Regulation' programme and anchored in the Treaty for the Functioning of the European Union (TFEU), have been evolving since 2002, and after a major revision in 2009, an update is due in the course of 2016.

It should be stressed here that, besides being evidence-informed, transparent, proportionate, and as unbiased as possible, the guidelines place explicit weight upon the procedural criteria of inclusiveness and stakeholder pluralism. Last but not least, RIAs ought to address economic impacts, environmental and social impacts, and, most crucially, take into account the Charter of Fundamental Rights (SEC(2011) 567 final, May 2011), and also take into account the principle of Sustainable Development (OECD/COM, February 2012). The mechanism of

Table 13.1 Criteria for regulatory impact analyses

Comprehensive	IA analysis should encompass besides economic, also social, and environmental impacts of envisioned policies.
Proportionate	The scope and depth of the IA should follow the proportionality principle with regard to the cause–effect relationship, the political/societal salience of the problem, and the expected effects of the policy solutions.
Evidence-based	EC policy proposals should be guided by the best available scientific evidence in a transparent manner.
Inclusive to stakeholders' views	All stakeholders' views must be documented and taken into account in the IA Report. The EC ought to collect a wide and balanced range of views, including dissenting ones.
Unbiased	RIAs ought to stick to an objective and balanced analysis. Evidence should inform policy, not the other way around.
Conducted in inter-institutional cooperation	A RIA is carried out by the lead DG, with the contribution of other relevant DGs, via establishing an Impact Assessment Steering Group.
Embedded in the policy cycle	Insights from ex-post evaluations from implementation, as well as ex-ante assessment of future monitoring needs should be considered.
Transparent	The credibility and reliability of RIAs depend upon the transparency with which results are presented, choices and estimations justified, and limits acknowledged.

Source: adapted from European Commission 2014b, p. 8

RIAs bears the promise of making policy designs more responsive to needs and concerns of societal stakeholders in a forward-looking manner, and of rendering more robust policies against factual error, or capture by particularistic economic interests.

Establishing an anticipatory governance regime for security

In terms of governance, the EU security (research) regime is embedded into a threefold, *political, institutional, and epistemic* context. The *political* context, vulnerable to sensationalist media coverage, opportunistic party politics, or actionist shifts of priorities in national and EU administrations in the aftermath of crises, creates waves of variable commitment for certain issues on the agenda. The current linkage in security terms, for example, between the refugee crisis and deficits in counter-terrorism policies, has played in the hands of populist right-wing politicians across Europe in a non-constructive way. The *institutional context* of security resembles a multi-layered (national/EU), and overlapping (several policies covering different parts of one issue) architecture. The European Commission (DG Migration and Home affairs) defined the coordinates for the EU agenda on security, with three priority areas ranging from tackling terrorism and preventing radicalization, to disrupting organized crime, and fighting cybercrime (European Commission 2015a). Their implementation is, yet, subject to a series of supranational agencies, such as the European Border and Coast Guard (ex FRONTEX) and EUROPOL, but also national law enforcement and data protection authorities, acting under UN conventions, EU regulations, and national law. The European security research programme provides, a major *epistemic context* in which potential solutions to serve the policy goals are generated. A series of questions can be raised in this respect: Are the results from R&D for example in border management technologies appropriate to meet the complex, humanitarian challenge faced at EU borders? Are pattern recognition or data mining technologies appropriate and successful in preventing attacks? Or are failures in security provision rather attributable to non-technological, institutional and organizational reasons? Security technologies, despite remarkable advances, still commit considerable type I errors, producing 'false positives', by picking up the wrong individuals, as well as type II errors, producing 'false negatives', by blending out the real targets. When applied *in vivo*, and not merely *in vitro*, as in the context of R&D, it seems that security technologies often cannot cope with the uncertainties associated with the societal context, and thus fail, at the end of the day, to turn high-tech tools into innovative, effective solutions (Kolliarakis 2013).

In the context of the recently emerged EU policy of *Responsible Research and Innovation*, numerous debates have already arisen concerning the regulatory challenges for a governance regime for emerging ICT- and security-relevant technologies (European Commission 2012). Indispensable components are located at three levels, which can be seen to correspond with the threefold governance template above: *legal governance* implies binding and coherent implementation of legal provisions and norms on proportionality, data protection, and fundamental

rights, aims at catching up the time-lag from the emergence of new technology applications. T*echnological governance* responds via evaluations and impact assessments, putting in place technological correctives, as in the case of privacy-by-design, or privacy-enhancing technologies, such as encryption, yet with the risk of kicking off a perpetual technological 'Red-Queen's race', reminiscent of Lewis Carroll's figure which was running and running, only to realize that no progress was attainable. Third, a major challenge is *self-regulatory governance* for empowering societal stakeholders, such as citizens and the organized civil society, in order to acquire informed decision capacity. The diffusion and consolidation of norms and standards in business and research seems to be of key importance in this respect. The European Group of Ethics, advising the European Commission on security and surveillance technologies, has recently made a step in that direction by suggesting a series of ethical safeguards to be put in place during the R&D process (EGE 2014).

Anticipatory governance is an inclusive exercise, involving also societal stakeholders who are affected but have limited influence. It entails reflecting about undesirable and desirable futures, in order to mobilize (political, institutional, and epistemic) capacities in the present, and if necessary correct and complement deficient governance arrangements. According to David Guston, anticipatory governance is

> … a broad-based capacity extended through society that can act on a variety of inputs to manage emerging knowledge-based technologies while such management is still possible. … (A)nticipatory governance motivates activities designed to build subsidiary capacities in foresight, engagement, and integration.
>
> (Guston 2014, p. 219)

A major objective of an inclusive anticipatory regime is to diversify sources and kinds of knowledge, minimize 'blind spots' in strategic policy vision, and foster a higher adaptive potential. Knowledge production in mutual dialogue with policy practice can address emerging techno-social challenges in a timely way, without suppressing controversies, but, moreover, by motivating debate about priorities in society. Ethical, legal, and societal aspects (ELSA) assessments, along with variants of participative and constructive technology assessments, can be key components of such reflexive anticipation, and integration of science and technology in society (ESF 2013).

Increasingly more international bodies point to the need to address uncertainty, complexity, and ambiguity in a hyper-connected world. A recent UNESCO study made a plea for promoting anticipatory literacy among experts, policy makers, and citizens in order to promote consciousness and accountability about difficult policy choices (Miller *et al*. 2013). Risk experts from the International Risk Governance Council have presented a phased model for stakeholder engagement in situations involving variable degrees of complexity, uncertainty, and ambiguity (see Figure 13.3 below).

While in the context of day-to-day policy business the bureaucratic practices of regulatory bodies are usually well-equipped to provide solutions, with rising

degrees of complexity, uncertainty, and ambiguity, the nature of tasks and the mix of stakeholders at consultations should expand outwards, including more societal stakeholders. When complexity is at play, then pluralism in expert opinion is required. With higher levels of uncertainty, affected stakeholders need to sit at the decision table as well. Last, when conflicting societal values are at stake, as in the controversies surrounding the relationship between privacy and security, then broad societal dialogue is additionally needed in order to raise awareness and co-decide about feasible and desirable trade-offs (International Risk Governance Council 2008).

Outlook: how to inform responsive and responsible security research

This chapter directed its attention toward the governance modalities of security (research) policy at European level. It zoomed out from the concrete tension between 'privacy' and 'security', and zoomed into the incomplete and imperfect epistemic modalities which frame their dual relationship within contemporary security research. The chapter argued for a second-order level for strengthening and expanding the evidence base for security policy, unlike in positivist and empiricist understandings, into an inclusive, *socially robust knowledge-informed regime*. A core condition for achieving that is to expand civil society engagement beyond the current citizen polling and *ad hoc* consultation practices. Besides making security R&D compatible with fundamental rights, the precautionary principle, and
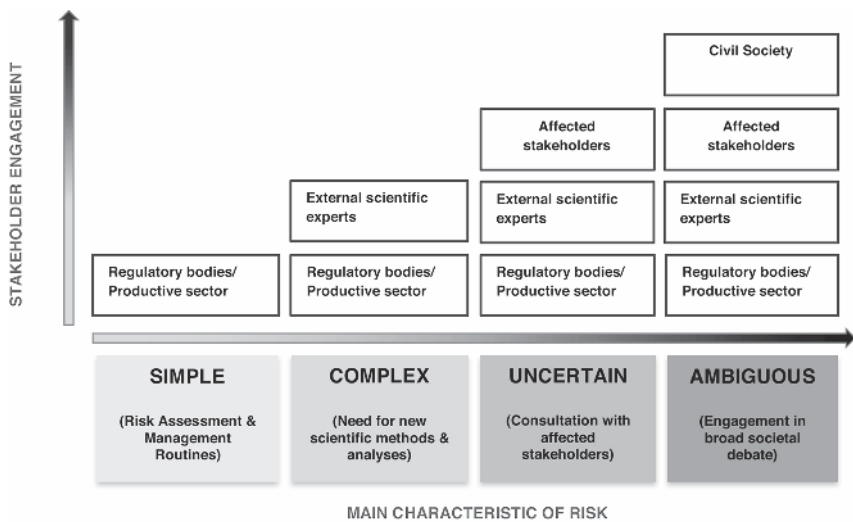
Figure 13.3 Risk–stakeholder involvement matrix

Source: adapted from International Risk Governance Council 2008, p. 18.

sustainability objectives, European and national research programmes need to become more responsive and responsible in a *forward-looking* manner by accommodating emerging citizens' needs and concerns in a sustainable way. The tension between the evolving practices for privacy and for security, as two 'moving targets' of contemporary EU public policy, has provided a plausible case in point for that.

The imbalance in various stakeholders' engagement in the security policy cycle reflects alarming power asymmetries with regard to handling 'security' as a crucial public good, and it has resulted into epistemic frames too narrow to grasp societal dynamics, or deliver effective results in the context of application of security technologies. Based upon that observation, the paper argued for a shift toward an *anticipatory governance* paradigm which aims at calibrating the envisioned ends to factual needs, and help develop here and now necessary and adequate *techno-social* capabilities. If consistently pursued in practice, the anticipation paradigm for security R&D would urgently call for integrating into research the study of *institutional and organizational* rearrangements, but also for more transparency and accountability with recourse to evidence, values, and documented needs which are deployed in order to justify policy decisions.

In an anthropomorphic metaphor from evolutionary biology, anticipatory governance provides the reflexive, learning and evolving 'brain' of the 'organism' of society. Reflexive capacity mirrors the ability of that organism to learn, adapt, and survive in shifting environments. Reflexiveness connects in a continuous feedback loop ends, means, and needs. Taken as such, it is the 'intelligence' of the organism, which furnishes it with the capacity to foresee, act, and adjust, by drawing lessons from successful past actions, but also from misplaced, counterproductive actions. Impact assessments, a multiple and versatile tool not yet widely applied in security (research) policy, can deliver valuable evidence with regard to effective and acceptable security measures by the citizens. Long-established practices in other politically contentious public policy fields, such as RCTs (Randomized Control Trials) in medicine and public health, have long showcased and established best practices and standards for establishing whether and under which conditions a 'therapy' is effective and efficient in its practical application, without causing more harm than good. It is a matter of common logic as of urgency that successful precedence and documented 'good practices' should be tried out in the societal context of application in order to minimize, if not avert uncritical, expensive, ineffective, and risky usage of new intrusive security-relevant technologies.

When it comes to tackling societal insecurities and threats, and enhancing resilience in society, the scarce key resources on the interface among citizens, policy makers, experts, and security providers are not so much new technological solutions, but rather *organizational cooperation, institutional trust, and political legitimacy*. These cannot be supplemented by technological quick fixes, and constitute instead major challenges which also security research has to meet, if it is to deliver on its primary task in the foreseeable future. Therefore, instead of merely fostering 'research-to-market' uptake and promoting acceptance of surveillance and pattern recognition technologies, what is dearly needed are dedicated studies about 'research-to-citizens' to ensure that security measures benefit them without back-

firing on society. A richer and more diverse evidence base is dearly needed, not only in order to guarantee that the outcomes of security R&D comply with ethics and legal norms, but, also that the security research agenda is guided by unbiased threat diagnoses.

The security R&D ecosystem needs to open up for participation of key societal stakeholders, such as practitioners from civil society organizations, not least, in order to avoid 'hammer-nail' fallacies, where readily available technological 'therapies' from the industrial or business/service side dictate convenient but biased problem 'diagnoses'. A multi-stakeholder foresight exercise conducted at the European Commission about the EU research and innovation regime concluded that:

> (F)uture RDI should focus more on the 'intangibles' (human capital, education, design, branding, etc.) and should define and ensure 'responsible innovation' (corporate social responsibility, sustainability and ethics). The coherence between these activities will also be facilitated by the same broad coalition of actors.
>
> (European Commission 2011, p. 58)

It is exactly the *soft*, contextual factors, often rather pejoratively and often indiscriminately dubbed as 'societal aspects', which exercise a non-tangible, yet decisive influence on whether and how technological solutions, which may perform well in the laboratory, will turn out to be beneficial innovations when applied in a given societal reality. There is no automatism leading to success, as a series of failures in the field of civil security, despite the application of intrusive technologies, has demonstrated. It has been a sad realization of the November 2015 terrorist attacks in Paris and the March 2016 attacks in Brussels that the authorities had collected enough and relevant data, yet inter-institutional lack of cooperation, or organizational incapacity of processing were not conducive to preventive action. Unless the focus of security R&D moves from the context of *in vitro* technology development, toward the context of *in vivo* societal application, and addresses the *soft* societal aspects as its cardinal task, and not as a 'fig-leaf' add-on, the reflexive evidence necessary to inform responsible, legitimate, and accountable security policy will remain a distant dream.

Contemporary European security research claims to be 'about' citizens and their well-being. It addresses them predominantly as objects of research, via studies, polls, surveys and *ad hoc* consultations, yet it does not seem to be 'with and for' them.[5] Civil society engagement throughout the security R&D cycle, as advisors, actors of research, and evaluators, implies making the process more *demand-driven*, but also giving more practical attention to the cultural, ethical, and legal premises in the context of application (e.g. *desirability* and *sustainability*), as contrasted to the more technical requirements in the context of development (e.g. *feasibility*). Establishing strong feedback loops from civil society actors would enhance the reflexive quality of security research to meet security policy needs. Reflexiveness is in this respect a crucial self-regulatory mechanism among society, the research, and the

policy communities to help mitigate current, and prepare for, avert, or recover from anticipated threats and risks.

To conclude, here is a disclaimer against epistemic/political naiveté: establishing anticipatory governance regimes, and strengthening the evidence base for security policy will neither deliver incontestable or consistent truths, nor help immunize once and for all against misplaced policies. However, the processes of diversifying stakeholder consultations and bringing transparency in the decision background of security measures will help reflect upon risks, bottlenecks and untapped potential in knowledge production regime for security policy. This plea to continuously match ends, means, and problem definitions, is particularly urgent for security policy, often characterized by non-transparency, and limited democratic scrutiny. Anticipatory reflexiveness is needed, for example, in tackling 'big data', particularly with regard to the EU border and counter-terrorism policies, and the potential to enhance security provision in the near future, but also with regard to the risk of massive abuse of personal information with no tangible benefit.

Bringing societal stakeholders together to negotiate on diverging interests in the context of a wicked problem, such as that of security provision within a liberal democratic state, is bound to generate no perfect solutions, yet it can promote more coherence and shared understandings. Policy mechanisms, such as regulatory impact assessments, can be the locus of such multi-stakeholder interactions via collecting, disputing, and systematizing evidence, and sensitizing about controversies and undesirable risks, institutional roadblocks, but also about hidden alternatives. All elements of an anticipatory governance regime for security policy, as sketched out above, are conducive to a better learning capacity of the organizations and institutions, governmental and non-governmental, involved. It is high time that such reflexive anticipatory policy mechanisms, particularly in the highly contentious security fields of counter-terrorism, border control, and crisis management, gained political traction for better tuning policies to society's needs and concerns.

Notes

1 This chapter draws in part upon thoughts elaborated in the context of the EU research project SecurePART (Increasing the Engagement of Civil Society in Security Research), 2014–2016, Grant Agreement No. 608039. I wish to thank the editors of this volume, and to two anonymous reviewers for their useful suggestions. I am indebted to Wainer Lussoli from the European Commission and to Chris Jones from Statewatch for their critical comments on earlier versions of this text.

2 See the survey analysis under www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/ (accessed 10 October 2015).

3 See the Campbell Collaboration website under www.campbellcollaboration.org/ (accessed 10 October 2015).

4 See the list of studies and reports under http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/reference-documents/index_en.htm (accessed 10 October 2015).

5 I borrow here the framing of the European Commission for its dedicated 'Science with and for Society' research programme under Horizon 2020.

References

Amoore, L. and de Goede, M. (2008) 'Transactions after 9/11: the banal face of the preemptive strike', *Transactions of the Institute of British Geographers* 33(2): 173–185.

Banks, G. (2009) *Evidence-based Policy Making: What Is It? How Do We Get It?* ANU Public Lecture Series, Canberra.

Biegelbauer, P. and Hansen, J. (2011) 'Democratic theory and citizen participation: Democracy models in the evaluation of public participation in science and technology' *Science and Public Policy* 38: 589–597.

Bora, A. (2010) 'Knowledge and the regulation of innovation' *Poiesis and Praxis* 7: 73–86.

Campbell Collaboration (2008) *Effects of closed circuit television surveillance on crime.* Campbell Systematic Reviews 2008: 17, Rutgers Newark.

Campbell Collaboration (2009) *The effectiveness of counter-terrorism strategies*. Campbell Systematic Reviews 2006: 2; Rutgers Newark.

de Londras, F. and Doody, J. (2015) *The impact, legitimacy and effectiveness of EU counter-Terrorism.* Abingdon: Routledge.

ECORYS Research and Consulting, Decision Études & Conseil, and TNO (2009) *Study on the Competitiveness of the EU security industry,* Rotterdam and Brussels. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf (accessed 20 December 2016).

ECORYS Research and Consulting (2012) *Study on Civil Military Synergies in the field of Security*, Rotterdam and Brussels. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/study_ecorys_cimisos_final_report_en.pdf (accessed 20 December 2016).

European Commission (EC) (2007) *Public-Private Dialogue in Security Research and Innovation*, COM(2007) 511 final, Brussels. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0511&qid=1482251245296&from=EN (accessed 20 December 2016).

European Commission (EC) (2009) *A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations*, COM(2009) 691 final, Brussels. Available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/comm_pdf_com_2009_0691_f_communication_en.pdf (accessed 20 December 2016).

European Commission (EC) (2011) *European Forward-looking Activities: Building the Future of 'Innovation Union' and ERA.* Luxembourg.

European Commission (EC) (2012a) *Ethical and Regulatory Challenges to Science and Research Policy at the Global Level*. Luxembourg.

European Commission (EC) (2012b) *Report of the Societal Impact Expert Working Group.* DG ENTR Report, February 2012, Brussels.

European Commission (EC) (2012c) *Security Industrial Policy: Action Plan for an Innovative and Competitive Security Industry,* COM(2012) 417 final, Brussels. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF (accessed 20 December 2016).

European Commission (EC) (2014a) *EU Research for a Secure Society: Security Research Projects under the 7th Framework Programme*. Luxembourg: Publications Office of the European Union.

European Commission (EC) (2014b) *Revision of the European Commission Impact Assessment Guidelines*. Public Consultation Document. Brussels.

European Commission (EC) (2015a) *Ex-Post Evaluation of the FP7 Security Research Programme.* Brussels.

European Commission (EC) (2015b) *The European Agenda on Security*. COM(2015) 185 final. Luxembourg.

European Group on Ethics in Science and New Technologies to the European Commission (EGE) (2014) *Ethics of Security and Surveillance Technologies*. Luxembourg.

European Parliament (2011) *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*. Brussels.

European Parliament (2012) *Drones: Engaging in Debate and Accountability*. Brussels.

European Science Foundation (ESF) (2013) *Science in Society: Caring for Our Futures in Turbulent Times*. Strasbourg.

European Parliament (2013) *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs.* Brussels.

European Parliament (2014) *Review of Security Measures in the 7th Research Framework Programme FP7 2007–2013*. Brussels.

European Science Foundation (ESF) (2015) *The Future of Security Research in the Social Sciences and Humanities.* Discussion Paper. Strasbourg.

Evers, A. and Nowotny, H. (1987) *Über den Umgang mit Unsicherheit*. Frankfurt: Suhrkamp.

Friedewald, M and Pohoryles, R. J. (2013) 'Technology and privacy. Editorial to the Special Issue', *Innovation: The European Journal of Social Science Research* 26(1–2): 1–6.

Giesecke, S., van der Geissen, A., Elkins, S. (eds) (2012) *FLA as a Means of Participation in Modern Democratic Decision Making; The Role of Forward-Looking Activities for the Governance of Grand Challenges*. Vienna: Platform.

Guston, D.H. (2014) 'Understanding "anticipatory governance"', *Social Studies of Science* 44: 218–242.

Guston, D.H. and Sarewitz, D. (2002) 'Real-time technology assessment' *Technology in Society* 24: 93–109.

Head, B.W. (2010) 'Evidence-based policy: Principles and requirements', in *Strengthening Evidence-based Policy in the Australian Federation. Roundtable Proceedings*. Canberra: Productivity Commission, 13–26.

Head, B.W, and Alford, J. (2015) 'Wicked problems: Implications for public policy and management' *Administration and Society* 47: 711–739.

International Risk Governance Council (2008) *An Introduction to the IRGC Risk Governance Framework*. Geneva: International Risk Governance Council.

Kaunert, C., Leonard, S. and P. Pawlak (2012) *European Homeland Security: Connecting Coincidence and Strategy.* London: Routledge.

Kitchin, R. (2014) 'Big Data, New Epistemologies and Paradigm Shifts' *Big Data & Society*, April–June 2014: 1–12.

Kolliarakis, G. (2013) 'Der Umgang mit Ungewissheit in der Politik Ziviler Sicherheit' (Coping with Uncertainty in Civil Security Research), in S. Jeschke, E.-M. Jakobs, and A. Dröge (eds) *Exploring Uncertainty. Ungewissheit und Unsicherheit im interdisziplinären Diskurs. (Uncertainty and Insecurity in Interdisciplinary Discourse).* Berlin: Springer, 313–332.

Kolliarakis, G. (2014) 'Sicherheitsforschung und ihre Schnittstelle zur Sicherheitspolitik: Intendierte und nicht-intendierte Konsequenzen der Wissenschaftsförderung' (Security Research and its Interface with Security Policy), in C. Daase, E. Engert, and G. Kolliarakis (eds) *Politik und Unsicherheit (Poltics and Insecurity)*, Frankfurt; New York: Campus.

Kolliarakis, G. (2016) 'From window-dressing to windows of opportunity: Civil society actors in the EU security regime', in R. Marchetti (ed.) *Partnerships in International Policy-*

Making: Civil Society and Public Institutions in European and Global Affairs. Basingstoke: Palgrave Macmillan.

Kolliarakis, G. (2017) (forth.) 'Anticipation and wicked problems in public policy. The creation of "unknown knowns"', in R. Poli, R. (ed.) *Handbook of Anticipation*. New York: Springer.

Liberatore, A. and Funtowicz, S. (2003) '"Democratising" expertise, "expertising" democracy: What does this mean and why bother?' *Science and Public Policy* 30: 146–150.

Lindblom, C.E. (1979) 'Still muddling, not yet through' *Public Administration Review* 39: 517–526.

Lyon, D. (2014) 'Surveillance, Snowden, and big data: Capacities, consequences, critique' *Big Data & Society*. July–December 2014: 1–13.

Miller, R., Poli, R. and Rossel, P. (2013) *The Discipline of Anticipation: Exploring Key Issues*. UNESCO Foresight Working Paper #1. Paris.

Neal, A.W. (2013) 'Empiricism without positivism: King Lear and critical security studies' in M.B. Salter and C.E. Mutlu, C.E. (eds) *Research Methods in Critical Security Studies: An Introduction*. Abingdon: Routledge.

Nowotny, H. (2003) 'Democratizing expertise and socially robust knowledge' *Science and Public Policy* 30(3): 151–156.

Nowotny, H. (2007) 'How many policy rooms are there? Evidence-based and other kinds of science policies' *Science, Technology, & Human Values* 32(4): 479–490.

Porter, T. M (1995) *Trust in Numbers. The Pursuit of Objectivity in Science and Public Life*. Princeton, NJ: Princeton University Press.

Rainey, H.G. and Jung, C.S. (2015) 'A conceptual framework for analysis of goal ambiguity in public organizations' *Journal of Public Administration Research and Theory* 25: 71–99.

Rask, M., Maciukaite-Zviniene, S., and Petrauskiene, J. (2012) 'Innovations in public engagement and participatory performance of the nations' *Science and Public Policy* 39: 710–721.

Rittel, H.W.J and Webber, M.M. (1973) 'Dilemmas in a general theory of planning' *Policy Sciences* 4: 155–169.

Saltelli, A. and Giampietro, M. (2016) 'What is wrong with evidence based policy?' (manuscript).

Slob, M. and Staman, J. (2012) *Policy and the Evidence Beast*. The Hague: Rathenau Instituut Publications.

Statewatch/Transnational Institute (2009) *NeoConOpticon: The EU Security-Industrial Complex*. London: Statewatch and the Transnational Institute.

Stirling, A. (2015) 'Power, truth and progress: Towards knowledge democracies in Europe', in J. Wildsdon and R. Doubleday (eds) *Future Directions for Scientific Advice in Europe*. Cambridge: Centre for Science and Policy.

Watts, R. (2014) 'Truth and politics: Thinking about evidence-based policy in the age of spin' *Australian Journal of Public Administration* 73: 34–46.

Wright, D. and Friedewald, M. (2013) 'Integrating privacy and ethical impact assessments' *Science and Public Policy* 40: 755–766.

14 A game of hide-and-seek?

Unscrambling the trade-off between privacy and security

Stefan Strauß

Introduction

The complex relationship between privacy and security is not least affected by the rapid dynamics of technical change. To cope with a wide range of security challenges, law enforcement and security agencies increasingly rely upon the employment of technological means, i.e. surveillance-oriented security technologies (SOSTs). The increasing complexity of security challenges reinforced calls for a holistic security concept aiming at integrating different roles and meanings of security. This paradigm shift refers to the so-called 'securitization' that frames security as an enduring process with a seemingly predictive capacity for threats and effective containment of them (cf. Buzan *et al.* 1998, Bigo 2000, Watson 2011). Corresponding developments are mirrored in security policies at national and European level and involve the implementation and use of SOSTs. The employment of SOSTs is mostly based on a model that frames privacy and security as a trade-off. The basic assumption of this model is that a degree of privacy intrusion is required in order to achieve a higher level of security. Similarly, citizens are assumed to accept the trading of their privacy for enhanced security in different settings. However, although citizens are directly affected by security and surveillance measures, little is known about their views and opinions on these issues. To learn more about the interplay between privacy, security and surveillance was a main objective of the EU-funded SurPRISE project. A core piece of the empirical work was a large-scale participatory approach to explore the perceptions of European citizens on privacy and security in relation to SOSTs. Citizen summits were implemented in nine European countries with about 200 participants each.[1] The methodological approach combined quantitative and qualitative methods to explore citizens' perceptions: a predefined interactive survey was used for quantitative data collection and structured group discussions on specific aspects of the core themes of security, privacy and SOSTs allowed getting deeper insights into the citizens' views and concerns.

The complexity of the privacy–security interplay is substantially influenced by a conceptual framing which presents both concepts as contradictory to each other. This trade-off model is closely related to the dominant logic behind the concept of securitization. Taking this interplay as a theoretical backdrop, this chapter opens

up some of the core issues in the conceptual arrangement of privacy and security. It critically reflects upon the rationale behind this model and presents some of the relevant perceptions of European citizens based on data from the SurPRISE project.[2] The empirical exploration of these perceptions enriched with theoretical foundations contributes to improve the understanding of the complex relationship between privacy and security. The results show that participants of the citizen summits do not follow a trade-off argumentation: they neither fully reject security measures nor accept the loss of their privacy. Hence, they deem the trade-off between privacy and security inappropriate, both with regards to the effectiveness of security measures as well as to the protection of privacy. This was underlined by a number of serious concerns about extensive use of surveillance technologies and practices. Instead of a trade-off, effective protection of citizens' privacy was seen as a sine qua non for the acceptability and effectiveness of security measures. A need for alternatives was identified to improve controllability and accountability of SOSTs and security authorities to re-establish trust of the citizens. To arrive at alternatives, a stronger focus on the factors underlying effectiveness and intrusiveness of security technologies and practices is required. This could support the assessment of whether a security measure is appropriate, to what extent it contributes to effective security achievements and to what extent privacy intrusion is a factual necessity or can be avoided (and thus legally prohibited). Such a model can contribute to stimulate technology development that reduces intrusiveness in the field of privacy-by-design and privacy impact assessment.

The chapter is structured as follows. A brief introduction is followed by a discussion of shifts in security policy related to securitization as well as the role and fallacy of a trade-off framing. Then, attitudes and concerns of citizens on privacy, security and surveillance from the SurPRISE project are presented. The subsequent section then focusses on deconstructing the 'nothing-to-hide' argument by revealing how citizens perceive this in relation to privacy concerns. After presenting some of the main results regarding effectiveness, intrusiveness and trust, the final section provides a summary and some concluding remarks.

Securitization and paradigm shifts in security policy

The role and meaning of security has significantly changed since the 1990s after the end of the Cold War. Increasingly complex problems on a global scale reinforced the demand for extended conceptualizations of security. During the Cold War, traditional state-centred security was the dominating concept aiming at protecting the integrity of the state from different kinds of threats mainly with technical and military power (Owen 2004). During the 1990s, this traditional security concept was complemented by a new approach with particular focus on the individual rather than on the national state. In 1994, the UNDP introduced the concept of human security as an issue of international policy with two principal aspects, namely the freedom from chronic threats such as hunger, disease and repression, and the protection from sudden calamities (UN 1994). In 2000, Kofi Annan[3] highlighted human security as a concept that

in its broadest sense, embraces far more than the absence of violent conflict. It encompasses human rights, good governance, access to education and health care (…). Every step in this direction is also a step towards reducing poverty, achieving economic growth and preventing conflict. Freedom from want, freedom from fear, and the freedom of future generations to inherit a healthy natural environment – these are the interrelated building blocks of human – and therefore national – security.

(Annan 2000)

This description pointed towards an extended view but focused on reducing insecurities for ensuring human development in accordance with freedom and health. However, tendencies towards a comprehensive conceptualization of security over the last two decades also affected the original concept of human security. Claims for a holistic approach increased that framed human security as 'an effort to re-conceptualize security in a fundamental manner'; a framework in which '(…) mitigating threats to the insecurity of individuals becomes a central goal of policy recommendations and actions' (Jolly and Ray 2006: 5). This transformation already occurred before the dramatic terrorist attacks on 11 September 2001, although 9/11 led to a further change in security policy on a global scale as the US and many other governments significantly reinforced security and surveillance measures (Ball and Webster 2003, Haggerty and Samatas 2010). Tendencies towards a holistic security concept coupled with a multilateral approach are visible internationally as well as in the European Security Strategy. Tackling new threats, extending the zone of security around Europe and strengthening international order are among the strategic objectives (Quille 2004). The attempt to integrate different domains and sectors into a holistic security concept is ambitious. On the one hand, it corresponds to globalization and the need to cooperate beyond national borders on a supra- and international level towards common security strategies. On the other hand, the conflation of intertwined but different roles and meanings of security in distinct domains complicates the efforts to develop appropriate security strategies to tackle emerging challenges. This is also visible in tendencies to turn away from the traditional separation between external/foreign (e.g. peace missions, military engagement) and internal/domestic security (e.g. fighting crime, ensuring public order, political stability). Hence, the boundaries between internal and external security increasingly blur (cf. Bigo 2000). Moreover, the European Union explicitly supports a closer coordination and cooperation between actors from both domains (Trauner 2011). Stronger coherence between the internal and external dimensions of security and exploiting synergies between both approaches is highlighted in the EU security policies as an important cross-cutting issue. *Buzan et al.* (1998) identified five sectors which play a strong role in the security discourse: the military, political, economic, societal and environmental sector. As each of these sectors follows its own mechanisms and logics, the roles, meanings, and measures in the realm of security may deviate significantly. Striving for a holistic security concept that neglects these different logics can complicate an informed distinction of security domains to develop appropriate measures.

Security as indeterminate process

From a theoretical perspective the paradigm shift in security policy is the effect of what many scholars termed securitization, which makes security a (indeterminate) result of discursive and non-discursive security practices (cf. Buzan *et al.* 1998, Bigo 2000, Balzacq 2005, Balzacq *et al.* 2010, Watson 2011). Different theoretical approaches deal with this issue: the Copenhagen School (cf. Buzan *et al.* 1998; Buzan and Weaver 2003) initially recognized securitization as a speech act, a rhetorical technique where the label 'security' is strategically used to foster political objectives. For the Paris School (cf. Bigo 2000, Balzacq 2005, Guild *et al.* 2008) securitization is also a 'capacity to control borders, to manage threats, to define endangered identities and to delineate the spheres of orders' (CASE 2006: 457). This conceptualization puts more emphasis also on 'practices, audiences and contexts which enable and constrain the production of specific forms of governmentality' (ibid.). In a Foucauldian sense, the Paris School highlights that securitization is a technique of government. In this regard, it is closely linked to 'a mode of governmentality, drawing the lines of fear and unease at both the individual and the collective level' (ibid.). Bigo (2000: 174) highlights the tendency of security discourses towards a self-fulfilling prophecy, whereas securitization is also 'a capacity to manage (and create) insecurity'. Hence, 'the processes of securitization and of insecuritization are inseparable' and can lead to a security dilemma where 'the more one tries to securitize social phenomena (…) to ensure 'security' (…) the more one creates (intentionally or non-intentionally) a feeling of insecurity' (CASE 2006: 461).

From security continuum to privacy vacuum?

The framing of security towards a holistic concept which spans across many different domains might amplify the aforementioned dilemma. Security is conceptualized from a process view 'marked by the intersubjective establishment of an existential threat with sufficient saliency to have political effects' (Watson 2011: 3). In this process, security is not framed as an objective condition but is linked to political discourse (Balzacq 2005). Hence, securitization arbitrarily presents a broad range of political issues in security terms. A consequence is the continuous convergence between internal and external security dimensions as for example observed by Bigo (2000) or Balzacq *et al.* (2010). This is visible in the security strategies of many European countries as well as the European Union. They involve a broad spectrum of different security challenges and threats such as poverty, diseases, climate change, energy supply, terrorism and organized crime. However, the focus of measures seems to lie mainly on combating terrorism and crime. While without any doubt each of these challenges needs to be addressed, a vague distinction between different roles of security can complicate the task of developing appropriate measures. Herein entailed are risks of increasing gaps between security threats and appropriate measures to these threats. With its own particular dynamics, the process of securitization can lead to a 'security continuum' in a problematic sense where the designation of 'certain persons and practices as "threats"' happens

in a rather arbitrary manner (Guild *et al.* 2008: 2). Several scholars point out that the linking of security and (im)migration is a prominent example for the dangerous effects of securitization (ibid.; Karyotis 2011). Securitization becomes particularly problematic if security is presented as a dominant issue of societal concern deserving higher priority than other state functions, and the protection of fundamental rights such as the right to privacy. In such a framing, security issues often become presented as existential threats that require particular 'measures and justifying actions outside the normal bounds of political procedure' (Buzan *et al.* 1998: 28ff.). The claim that 'exceptional times require exceptional measures and thus invoke necessities supposedly brought about exceptional danger' is a questionable logic as '[n]ecessity is a political claim, not an existential condition' (CASE 2006: 466). The 'exceptional security practices can be understood as in the context of ongoing processes of technocratic, bureaucratic and market-driven routinization and normalization' (ibid.). Entailed are risks that security measures become ambiguous and are introduced for self-serving purposes. This can also reinforce an assumed trade-off between privacy and security. In other words: playing the 'security card' tends to trump concerns about civil liberties and human rights. The result can be conflicting interests, lacking public acceptance and increasing resistance against security policy. This may pose the danger that security becomes self-referential without focusing on reducing realistic risks, or is misused to justify other political objectives. 'Security is then, conceptually, reduced to technologies of surveillance, extraction of information, coercion acting against societal and state vulnerabilities, in brief to a kind of generalized 'survival' against threats coming from different sectors, but security is disconnected from human, legal and social guarantees and protection of individuals' (Bigo 2008: 13). Thus, the development and use of surveillance technology extends the toolbox of securitization. Technological progress and the increasing tendency to employ SOSTs accompany and foster the paradigm shift in security policy based on the misleading assumption that security challenges would be manageable preferably by technological means. In line with the logic of securitization, the use of SOSTs is presented as a prerequisite and 'weapon of choice' to tackle current and emerging security threats. In this regard, SOSTs can reinforce the security continuum which can lead to a privacy vacuum where one's private sphere becomes an empty space where every personal detail is disclosed and abundantly available for surveillance technology.

The trade-off fallacy

Security policy and SOST usage is predominantly based on the assumed necessity to trade privacy for security. Hence, privacy intrusions are simply presented as the only option to improve security. The power of this trade-off model lies in its simplicity. However, its validity is increasingly questioned. Several scholars have pointed out that it over-simplifies the privacy–security interplay (cf. Schneier 2006, Nissenbaum 2010, Solove 2011, Pavone and Degli Esposti 2012, Friedewald *et al.* 2015, Valkenburg 2015). Friedewald *et al.* (2015) tested the validity of the trade-off model based on a survey about privacy and security attitudes. They found

statistical evidence against the trade-off at the individual level, as those with high security concerns do not worry less about privacy. In addition to such empirical evidence against the trade-off, also a deeper understanding of its basic functionality is required to come to alternatives. Already the term 'trade-off' implies a contradiction between two items indicating that one wins at the expense of the other. This model operates on two levels: on a political level it frames privacy as a barrier to effective security measures and justifies privacy intrusions as necessary to improve security; on an individual level, it suggests that individuals gain more security but only if they accept privacy intrusions (EGE 2014). Hence, this model represents an 'all-or-nothing fallacy' (Solove 2011) that frames privacy and security as conflicting concepts with perpetual inherent contradictions. Such a framing suborns to neglect the meaning of data protection and privacy as they are presented as a burden to security. This impedes the realization that both concepts have a complementary relationship to some extent. There emerges the constant need to choose between these values as well as a neglect of the (economic and social) costs and effects of security and surveillance measures (cf. Strauß 2015b).

Normalizing privacy interference

The trade-off logic suggests that security measures have to intrude into privacy implying the necessity of gathering personal information. In this regard, the trade-off represents a game of hide-and-seek that frames privacy as hiding information and security as seeking it. Accordingly, it also narrows the view on security measures as it neglects to consider options that do not intrude into privacy. The relationship between privacy and security is reduced to a state of permanent conflict. However, this misleading assumption is ethically problematic and also not determined in legal regulations and fundamental rights catalogues. Both privacy and security are part of the legal frameworks for human rights.[4] Neither security nor privacy is an absolute right or value. Each always has to be seen as a part of the broader public interest. Also the public interest (broadly addressing the well-being of the general public) is not strictly determined and thus, eventual clarifications are part of jurisdiction. The very aim of the principle of proportionality is to come to a 'fair balance between the demands of the general interest of the community and the requirements of the individual's fundamental rights' (Kilkelly 2003). This is meant for cases of conflicts but it does not imply that permanent conflicts exist. Put shortly, as a norm, privacy defines a state where an individual is free from interference. Consequently, legal norms[5] only allow interference with privacy under certain conditions, i.e. to fulfil public interest in accordance with the law and the protection of the foundations of a democratic society. Interfering with privacy is foreseen by the law as a possibility but always as the exception to the rule and thus by no means as a permanent option.[6] Hence, a setting in which the implementation of security constantly entails privacy intrusions is misleading as it falsely frames security as a concept that always has to intrude into privacy without assessing alternative options. To this end, such an assumption would raise the exception to the rule as the norm, namely privacy interference as inevitable for security.

Trading at the cost of liberty

Finally, the trade-off puts liberty at stake as it dismisses that liberty is the defining value for both, privacy and security: 'democracy, the rule of law and fundamental rights are designed to protect the liberty of the individual within the society' (Guild *et al.* 2008: 9). The prominent role of liberty and freedom in legal frameworks is thus no coincidence but underlines this aspect. Against this background, this trade-off model risks neglecting the fact that security is subordinate to liberty and liberty is the superior linkage between both – privacy and security. Privacy understood as a state free from interference and enabler of other rights represents a form of liberty, namely autonomy (cf. Nissenbaum 2010). As outlined above, legal frameworks implicitly highlight that a trade-off is to be avoided for the sake of liberty and only allowed as a case of exception. Privacy-intrusive security practices presented as inevitable and security as seemingly superior value undermine this setting and weaken the essential role of privacy as an enabler to exercise other democratic rights such as freedom of expression, assembly and movement (Lever 2006).

The state of permanent conflict created by the trade-off is in line with securitization (as discussed in the previous section) which entails an extensive framing of security. Particularly, securitization can lead to an increase of exceptional security states where more intrusive security actions (e.g. dragnet investigations, mass surveillance, cooperation between military and police forces) are justified than in normal, rule based situations (cf. Buzan *et al.* 1998, Balzacq 2005). The broad interpretation of security which leads to a limitation of privacy is a worrying development, 'which risks becoming a 'catch-all' clause' (EGE 2014: 38). Thus, the trade-off model is also used as a tool for justifying privacy intrusion by security technology and practices. In this regard, it amplifies securitization (and vice versa) as it provides a relatively simple formula to communicate security action. The trade-off logic also complicates to critically scrutinize its rationale without arguing against security.

To prevent the trade-off from jeopardizing liberty, the individuals' 'rights must not be 'traded' but, quite the contrary, must restrict the trade-off' (EGE 2014: 84). Thus a model is needed 'that does not give up any of the rights, even though it acknowledges that priorities may differ not only between individuals but also differ in different contexts' (ibid: 85). The trade-off is accompanied and shaped by the wrong questions: instead of asking the crucial question of how privacy should be protected, it is frequently asked whether privacy should be protected (Solove 2011). As a consequence the fact that both values – privacy and security – are essential for social development and well-being is often neglected. The important question is therefore how both privacy and security can be respected. In cases where conflicts occur, it is not a matter of giving up privacy or security but of prioritizing rights in a way that considers different contexts and the individuals concerned.

Main outcome of the citizen summits

As outlined in the previous section, securitization contributes to reinforce a trade-off between privacy and security (and vice versa). But how do European citizens

perceive the privacy–security relationship? The SurPRISE project explored these perceptions in relation to the employment of surveillance-oriented security technology (SOST). After delineating the methodological approach, this section presents selected results of the SurPRISE citizen summits held in nine countries (in the first half of 2014).

Methodology of the citizen summits

Three different SOSTs (smart CCTV, deep packet inspection (DPI) and smart phone location tracking (SLT)) were addressed at the citizen summits serving as concrete examples to represent issues affecting different types of privacy (such as visual, communicational and locational privacy); and participants were confronted with a number of questions and discussions about these issues.[7] About 1800 persons in total participated in the events with N=1772 valid responses. Participant recruitment differed across the involved countries. In Austria, Italy, Hungary, Spain and the UK, external contractors were commissioned with this task. In Denmark, Germany, Norway, and Switzerland participants were recruited via a mix of channels (e.g. postal invitations, announcements in online and print media). To achieve a heterogeneous group of citizens and to avoid bias, recruitment considered different criteria such as age, gender, geographical area, educational level and occupation. A basic precondition was that participants have no expertise in privacy, security or similar topics related to the project issue. The panel structure was relatively balanced with regards to age, gender, education as well as citizens from urban (36 per cent), metropolitan (36 per cent) and rural (27 per cent) areas. Eventual differences at national level regarding age and gender were negligible in the total sample: 46 per cent (female) and 52 per cent (male) participants were involved with a relatively even distribution in the different age categories with a slight majority of participants (44 per cent) belonging to middle-aged groups (between 40–59).

The methodology and process design was similar in each country, consisting of a mixed approach combining quantitative and qualitative elements based on three major strands: as a starting point, basic information (booklet and films)[8] about the SOSTs was provided to establish a common foundation for the issue knowledge among the participants. A predefined interactive survey served as a tool for quantitative data gathering. Finally, three thematic group discussions were conducted, and in the last session citizens were asked to develop policy recommendations. This combined approach allowed for the exploration of both the individual views on particular questions and the rationale behind these views.

Citizens' attitudes and concerns[9]

Figure 14.1 below shows some of the participants' attitudes and concerns about privacy and security with regard to SOSTs. The results reveal some of the interrelations between intrusiveness and effectiveness of security measures perceived by the participants. In total, 64 per cent share the opinion that the use of SOSTs contributes to improving public security and the majority does not think that

SOSTs are only used to demonstrate action against crime. However, if the achieve-ment of security by a SOST is acknowledged, this does not imply that privacy intrusion of that SOST is accepted. At the same time, 70 per cent share the opin-ion that SOSTs are likely to be abused and there are a number of high concerns about the abuse of personal information; 70 per cent are concerned about exten-sive information collections 63 per cent fear that the information held about them might be inaccurate; near to 80 per cent fear that their personal information might be used against them and 91 per cent are concerned that their information is shared without their permission.[10] Citizens clearly expressed concerns and fears about abuse of information and power. These results indicate that the intrusiveness of SOSTs and security measures might have a negative effect on their acceptability which becomes more visible in the following sections.
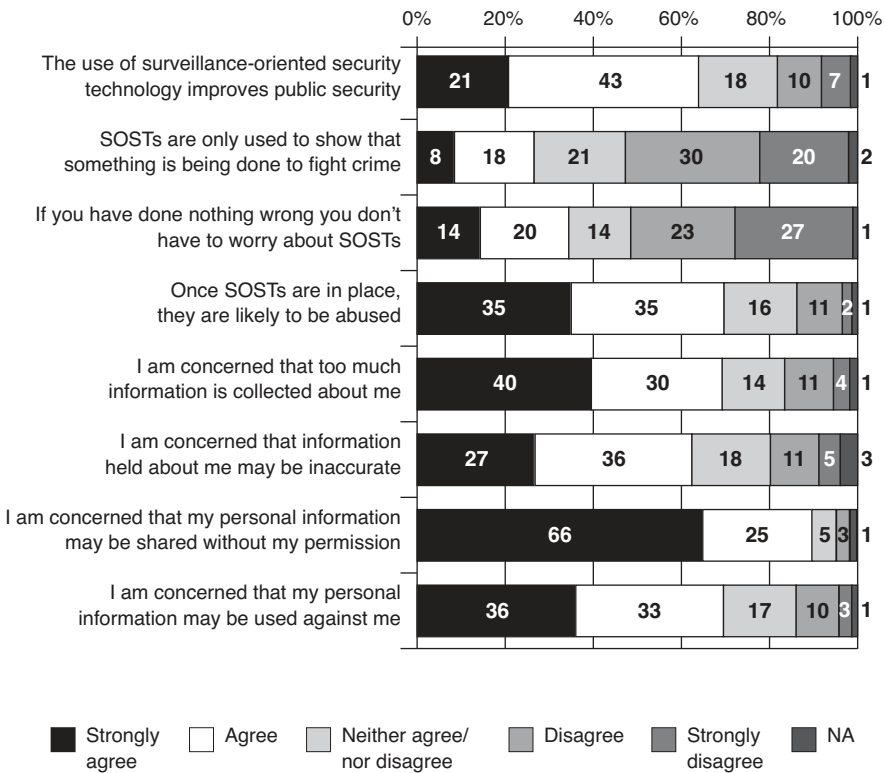
Figure 14.1 Major attitudes about SOST usage

'Nothing-to-hide' unscrambled

A prominent argument to justify security and surveillance measures which intrude into privacy is the statement 'those who have nothing to hide have nothing to fear'. This argument implies that one does not need to worry about privacy infringement and surveillance if one behaves correctly. This argument falsely reduces privacy to a form of secrecy aiming at hiding things. At the same time, it neglects that surveillance can also do harm to a variety of activities that are lawful and essential in a democratic society such as freedom of thought, expression, religion, free association, etc. (cf. Schneier 2006, Solove 2011, Bennett 2008). To explore the citizens' perceptions in relation to this line of argumentation a similar statement was asked: 'If you have done nothing wrong, you don't have to worry about SOSTs' (as shown in Figure 14.1). Fifty per cent of the participants in the total sample do not share this opinion and only 34 per cent do. At the same time, there are high concerns expressed about the misuse of personal information, such as that too much information is being collected, information being used against them and information is being shared without the permission of the concerned individuals.[11]

To explore the differences in the perceptions of the agreers and opponents of the 'nothing-to-hide' argument further, the results were cross-linked with those about the concerns about information misuse (see Figure 14.2 and Table 14.1).
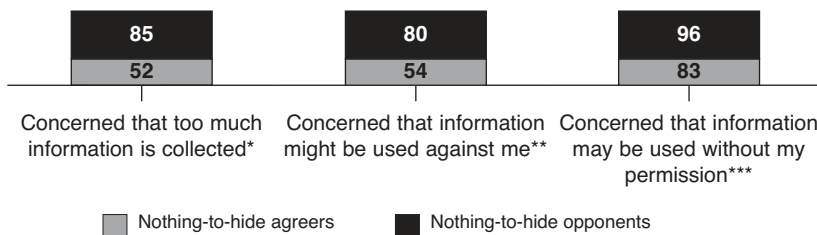
Figure 14.2 Concerns about information misuse of nothing-to-hide agreers and opponents (percentages)

Notes: ★ (N=549 agreers / N=804 opposers), ★★ (N=541 agreers / N=807 opposers), ★★★ (N=549 agreers / N=803 opposers)

Table 14.1 Concerns of nothing-to-hide agreers and opponents (percentages)

		Concerned	Not concerned	Neither nor	NA
Too much information is collected	NTH agreers	52	29	18.5	0.5
	NTH opponents	85	6	8.5	0.5
Information might be used against me	NTH agreers	54	23	23	0
	NTH opponents	80	7	12	1
Information is shared without my permission	NTH agreers	83	9	8	0
	NTH opponents	96	1	2	1

The results reveal some contradictions in those agreeing to the 'nothing-to-hide' argument: on the one hand, with about 85 per cent there is an expected correlation between the 'nothing-to-hide' opponents (participants worried about SOSTs also when perceiving to have done nothing wrong) and participants concerned about extensive information gathering. However, more than half (52 per cent) of the 'nothing-to-hide' supporters (those participants agreeing to have nothing to fear from SOSTs if they have done nothing wrong) are at the same time concerned that too much information is collected about them. Hence, even those individuals who have nothing to hide in the first place are concerned about extensive information gathering. Furthermore, 54 per cent of the nothing-to-hide agreers are concerned that their information is being used against them. Finally, the very high rate of 83 per cent being concerned that their information might be shared without their permission further indicates that the 'nothing-to-hide' argument is misleading. Similar to the trade-off framing, the argument narrows privacy to hiding personal information and represents a rhetoric that rather veils than reveals the reasons for the use of SOSTs. Not least, privacy is also linked to the trust that others respect private life and do not intrude into it against the individual's will. It does not matter if one has things to keep secret or not, but it does matter if personal information is collected and for what purpose. If information collection is unjustified or opaque then insecurity and mistrust might increase.

Effectiveness, intrusiveness and trust

The degree of privacy impact triggered by security technologies, practices and measures not least depends on the amount of interference into an individual's private sphere by the different modes of observation and/or control applied. Or in other words: the level of direct intrusiveness, i.e., to what extent an individual is subject to surveillance (as part of a security action), comprising a sort of interference into one's privacy. To explore further, if there are perceived differences in the intrusive quality of a SOST, citizens were confronted with some statements concerning the three different SOSTs (as shown in Table 14.2).

Compared to smart CCTV and SLT, DPI raised the highest concerns and received the lowest rates regarding effectivity and appropriateness to handle national security threats. Besides these differences, the effectiveness and intrusiveness of the SOSTs are interrelated: those technologies perceived as highly intrusive are also perceived as less effective. Furthermore, also the mode by which security and surveillance measures and SOST usage are implemented and employed raises high concerns: the clear majority (in each case over 60 per cent, regarding DPI even near to 90 per cent) perceives that the SOSTs are forced upon them. This result indicates that the participants do not accept how SOSTs are implemented and perceive a lack of transparency and accountability of the authorities using these SOSTs. The highly expressed worries about the use of SOSTs in future indicate fears about further extension of surveillance.

The results lead to the conclusion that the intrusive capacity of the technologies makes a difference to their acceptability. On a general level, a certain amount

Table 14.2 Major attitudes regarding SOST usage (percentages, N=1772)

		Agree	Neither/ nor	Disagree	NA
… is an effective national security tool	sCCTV	64	18	17	1
	DPI	43	24	32	1
	SLT	55	25	20	0
The idea of … makes me feel uncomfortable	sCCTV	39	20	40	1
	DPI	66	16	17	1
	SLT	45	24	31	0
I feel more secure when … is in operation	sCCTV	43	25	32	2
	DPI	12	25	61	2
	SLT	27	29	43	1
… is forced upon me without my permission	sCCTV	60	16	23	1
	DPI	87	7	5	1
	SLT	68	14	16	2
I worry about how the use of … could develop in the future	sCCTV	67	13	19	1
	DPI	84	9	7	1
	SLT	65	18	17	1

of intrusion seems to be acceptable for the respondents. However, this is only valid under certain conditions. For the participants it is not sufficient that a SOST improves public security. If it is too intrusive it is not accepted as a security measure. This is not only a matter of the technology itself and its functioning but also of the related practices, i.e. its usage. SOST usage is particularly perceived as too intrusive if it intrudes into the privacy of persons without concrete suspicion and without appropriate legal mechanisms to ensure that the technologies are used in a lawful way. In the group discussions during the summits, the need for judicial orders and legal control mechanisms that ensure that SOSTs are only used for plausible and verifiable reasons was often mentioned as very important. Strong concerns were expressed that legal regulations are insufficient to ensure that SOSTs are not misused. As shown in Figure 14.3, only a minority in each case has an opposite opinion (28 per cent regarding SLT, 24 per cent regarding smart CCTV, and 19 per cent regarding DPI). Hence, people expressed that they had little trust in laws and regulations protecting them from misuse of SOSTs. In general, regulation and oversight were seen as crucial elements in the relationship between effectiveness and intrusiveness.

Several citizens' concerns presented here point to the crucial role of trust for the privacy–security interplay. Trust is an essential but also fragile concept that needs a strong foundation to prosper. If this foundation gets shocked or irritated then trust can be cut back to a relatively low level. The results shown in Figure 14.4 reveal some amount of insecurity and uncertainty among the participants as regards the establishment of trust. While several respondents perceived security authorities as
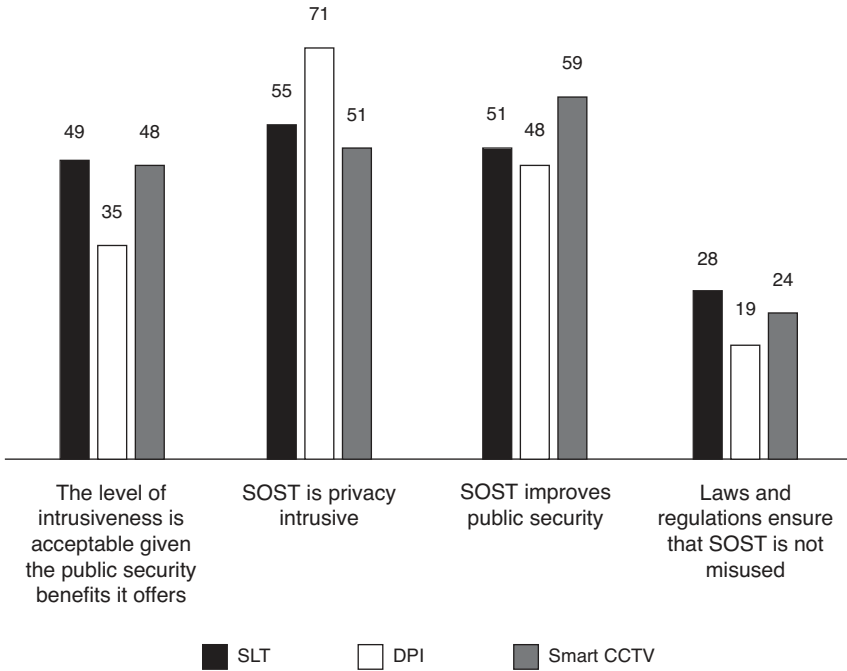
Figure 14.3 Intrusiveness and acceptability (percentages)

trustworthy (36 per cent smart CCTV, 36 per cent DPI, 46 per cent SLT), there was a strong tendency to disagree with the statement that security authorities do not abuse their power, 46 per cent in case of smart CCTV, 34 per cent for SLT and 52 per cent regarding DPI. Thus, the participants expressed a high level of fear about the authorities abusing their power and infringing upon privacy.

Besides the high concerns, with over 30 per cent in most of the items this set of results shows the highest 'neither/nor' values in the whole survey. This underlines that trust and trustworthiness are highly controversial issues for the citizens in the context of SOSTs and related practices. Some explanations can be found for these controversies in the table discussions: as shown in the previous sections, the majority of participants perceive the use of SOSTs as very intrusive and (linked to that) as rather ineffective. Linked to the high concerns about the misuse of information gathered by surveillance technologies are fears about function creep and the abuse of power by security authorities conducting these technologies. The results indicate that the perceived lack of accountability and oversight of security authorities (e.g. visible in expressed uncertainty regarding trustworthiness) and surveillance practices hampers trust. This does not imply that all security efforts made are rejected. Some of the results indicate that security efforts are to some extent understood as useful and relevant. However, in general high concerns

Security authorities which use...

Smart CCTV	8	28	32	16	13	3
DPI	7	29	26	19	15	3
SLT	12	34	32	10	9	3

...are trustworthy

Smart CCTV	7	26	35	17	11	5
DPI	4	23	35	19	11	7
SLT	9	30	35	11	8	6

...are competent in what they do

Smart CCTV	10	29	30	17	12	2
DPI	6	28	29	19	15	4
SLT	8	36	33	13	7	4

...are concerned about the welfare of citizens as well as national security

Smart CCTV	5	17	29	23	23	4
DPI	3	11	28	25	27	6
SLT	5	24	33	20	14	4

...do not abuse their power

0   20   40   60   80   100

Percentage

■ Strongly agree   □ Agree   Neither agree/ nor disagree   Disagree   Strongly disagree   NA

Figure 14.4 Trustworthiness of security authorities

dominate and people expressed a lack of common grounds on which to build their trust. This is aggravated by perceptions of the citizens that security and (mass) surveillance measures are based on a setting of mistrust in the citizens, i.e. everyone is treated as a potential suspect. As a consequence, citizens feel more insecure and uncertain about SOSTs and security authorities themselves. In other words:

mistrust reinforcing itself as mistrust in the citizens creates mistrust of the citizens in the authorities.

Summary and conclusions

This chapter argues that a trade-off between privacy and security is not inevitable but is shaped by surveillance employed as a (technology-supported) security practice, reinforced by securitization. Challenges to overcome the fallacy of trading one against the other include cultivating new approaches that recognize privacy and security also as complementary concepts without supposing a natural conflict. To develop alternatives, it is important to come to a better understanding of how individuals perceive the privacy–security interplay and how the trade-off model functions. The results of the SurPRISE project and findings presented in this chapter contribute to that and draw a different picture from what the dichotomized view of the trade-off suggests. While trade-offs might occur at some point (e.g. if privacy intrusion is factually the only justifiable option) it is important to comprehend that such situations are by no means a permanent necessity. On the contrary, they are exceptional while privacy protection represents the standard mode. This is particularly important as the widespread use and further extension of SOSTs and security practices increasingly risks privacy becoming a hollow concept falling a victim to security. Entailed is a need for alternatives that put greater emphasis upon the factual intersections and differences between privacy and security. This begins at fundamental level reconsidering the fact that security is not a superior value but liberty is the defining value for both. The assumption of a trade-off makes sense only if an inherent conflict between intrusiveness and effectiveness of a security measure is assumed. In other words: If there is no privacy intrusion resulting from a security measure then there is no trade-off. If there is a privacy intrusion and no effectiveness of a security measure there is also no trade-off. A trade-off only occurs if the effectiveness of a security measure cannot be gained without privacy intrusion. However, in this case, it needs to be assessed whether no other options exist to attain effectiveness of security measures, to what extent privacy intrusion is necessary and if it is in accordance with the law. Even if it is assumed that SOSTs benefit security, concerns about privacy intrusions are mostly rated higher than their effectiveness, as the results show. The high concerns about information collection and abuse of personal information indicate that people are more greatly concerned about trading their information than accepting such a trade. Similar is the case among those people who seemingly follow the 'nothing-to-hide' argument: even those who share the nothing-to-hide opinion do not want to be subjected to surveillance and expressed strong concerns about information misuse and privacy infringements. Taken together, the results indicate a need to overcome the trade-off model and attain a more differentiated perspective on privacy and security which includes the relationship between effectiveness and intrusiveness. SOSTs can have different levels of effectiveness for security with different levels of intrusiveness for privacy, and there is no inherent necessity to intrude privacy to improve security. Such a differentiated view is crucial but is currently hindered by

a trade-off framing. Further research is needed for in-depth exploration on how effectiveness and intrusiveness relate in the privacy–security discourse. Assumed effectiveness of SOSTs needs to be verifiable and their intrusiveness needs to be controlled with respect to fundamental human rights. If there are plausible reasons for some intrusive security measures, they have to be communicated and open to public scrutiny. The fears and concerns about privacy infringement, abuse of power, doubts and uncertainties about the practices and technologies of security authorities, as well as a lack of trust underline the crucial role of transparency and accountability to reconcile privacy and security.

While laws and regulations embody an essential means against power abuse, they are barely trusted in terms of their effectiveness by the citizens.[12] Thus, a need for more effective enforcement of privacy and data protection laws and evaluation frameworks to control the implementation of SOSTs and practices compliant with fundamental rights can be identified. Privacy-by-design and − default as a pivotal technology feature and privacy impact assessment prior to technology usage can contribute to improve the effectiveness of legal regulations. Improving privacy protection at an institutional level refers to reinforcing already existing safeguards and the institutions in charge of implementing existing regulations. This suggests the upgrading of capacities of national and European DPAs and other oversight bodies regarding their competences and resources. Core issues to bring back security measures to a more acceptable level are a turn away from mass surveillance and a reinforcement of checks and balances for more effective oversight. Addressing these issues is essential to regain the trust of the citizens and to come towards approaches with respect to the complementary character of privacy and security.

Notes

1   In Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland, and the United Kingdom. Further information about these national participation processes is available at: http://surprise-project.eu/events/citizen-summits/.
2   Parts of this paper refer to Strauß (2015a).
3   Nobel Peace Prize winner and former Secretary-General of the United Nations until 2006.
4   This chapter does not provide a legal analysis but refers to universal human rights catalogues. For an analysis of legal issues regarding the trade-off see the chapter by Somody, Szabó and Székely in this book.
5   Such as Article 8 of the European Convention on Human Rights, Article 12 of the Universal Declaration of Human Rights or Article the European Fundamental Rights Charter.
6   The European Court of Human Rights declared that '[m]ere storage of information about an individual's private life amounts to interference within the meaning of Article 8 (right to respect for private life)' of the European Convention on Human Rights (European Court of Human Rights 2014: Factsheet – data protection) www.echr.coe.int/Documents/FS_Data_ENG.pdf.
7   For further details about the methodology and synthesis of the summits see Strauß (2015a). Further information about all national participation processes, individual country reports, research data, information material and impressions of the summits is available at: http://surprise-project.eu/dissemination/research-results/.

8   For details about this information package see http://surprise-project.eu/wp-content/uploads/2014/04/SurPRISE-D4.3-Information-material-and-documentary-films.pdf.

9   It has to be noted that the presented perceptions have natural limits as regards their meaning as citizens might behave or argue somewhat differently in 'real world' settings outside the citizen summits. However, this does not reduce the validity of their expressed attitudes which are useful for the better understanding of the privacy–security interplay.

10 Fear of unauthorized information usage also refers to the problematic aspects of informed consent as one cornerstone of privacy. While consent is essential for legal data processing, it is often difficult to effectively prohibit or permit the use of information due to a lack of alternatives from the individuals' point of view.

11 The situation is widely similar in the countries with the strongest opposition. Exceptions are given in Hungary and the UK, where the respondents tended to agree with the nothing-to-hide statement. However, also in these two countries the participants expressed concerns about extensive information collection and fears of misuse.

12 For an analysis of the legal issues concerning the citizens' recommendations see the chapter by Porcedda in this book.

References

All URLs were checked last at May 4, 2016.

Annan, Kofi 'Secretary-General Salutes International Workshop on Human Security in Mongolia.' Two-day session in Ulaanbaatar, May 8–10, 2000. Press Release SG/SM/7382. Online. Available at: www.gdrc.org/sustdev/husec/Definitions.pdf

Ball, K. and Webster, F. (2003) *The Intensification of Surveillance*. London: Pluto.

Balzacq, T. (2005) 'The three faces of securitization: Political agency, audience and context', *European Journal of International Relations* 11(2): 171–201.

Balzacq, T., Basaran, T., Bigo, D., Guittet, E-P., and Olsson, C. (2010) 'Security practices'. In Denemark, R. A. (ed.) *International Studies Encyclopedia*. Oxford: Blackwell Publishing, 1–30.

Bennett, C. (2008) *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Bigo, D. (2000) 'When two become one: Internal and external securitisations in Europe'. In Kelstrup, M. and Williams, M. (eds) *International Relations Theory and the Politics of European Integration. Power, Security and Community.* London: Routledge, 171–204.

Bigo, D. (2008) 'Globalized (in)security: The field and the Ban-Opticon'. In Bigo, D. and Tsoukala, A. (eds) *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* Abingdon: Routledge, 10–48.

Buzan, B., Weaver, O., and de Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Buzan, B. and Weaver, O. (2003) *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

CASE Collective (2006) 'Critical approaches to security in Europe: A networked manifesto' *Security Dialogue* 37(4): 443–487.

EGE – European Group on Ethics in Science and New Technologies (2014) *Ethics of Security and Surveillance Technologies.* Opinion No. 28 of EGE. Brussels: European Union.

Friedewald, M., van Lieshout, M., Rung, S., Ooms, M., and Ypma, J. (2015) 'Privacy and security perceptions of European citizens: A test of the trade-off model'. In Camenisch, J., Fischer-Hübner, S. and Hansen, M. (eds) *Privacy and Identity for the Future Internet in the*

Age of Globalization Volume 457 of the series IFIP Advances in Information and Communication Technology. Heidelberg: Springer, 39–53.

Guild, E., Carrera, S. and Balzacq, T. (2008) *The Changing Dynamic of Security in an Enlarged European Union*. Research paper No. 12, CEPS Programme Series. Online. Available at: www.ceps.eu http://aei.pitt.edu/11457/1/1746.pdf

Haggerty, K. D. and Samatas, M. (eds) (2010) *Surveillance and Democracy*. Abingdon: Routledge-Cavendish.

Jolly, R. and Ray, D. B. (2006) *The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates*. United Nations Development Programme, National Human Development Report Unit.

Karyotis, G. (2011) 'The fallacy of securitizing migration: elite rationality and unintended consequences'. In Lazaridis, G. (ed.) *Security, Insecurity and Migration in Europe*. Aldershot: Ashgate, 13–30.

Kilkelly, U. (2003) *The Right to Respect for Private and Family Life – A Guide to the Implementation of Article 8 of the European Convention on Human Rights*. Human Rights Handbooks No. 1, Directorate General of Human Rights. Strasbourg: Council of Europe.

Lever, A. (2006) 'Privacy and democracy', *Contemporary Political Theory* 5: 142–162.

Nissenbaum, H. (2010) *Privacy in Context – Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Owen, T. (2004) 'Challenges and opportunities for defining and measuring human security', *Human Rights, Human Security and Disarmament, disarmament forum* 3: 15–24.

Pavone, V. and Degli Esposti, S. (2012) 'Public assessment of new surveillance-orientated security technologies: Beyond the trade-off between privacy and security', *Public Understanding of Science* 21(5): 556–572.

Quille, G. (2004) 'The European security strategy: A framework for EU security interests?' *International Peacekeeping* 11(3): 1–16.

Schneier, B. (2006) 'The eternal value of privacy', *Wired*. Online. Available at: www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

Solove, D. (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press.

Strauß, S. (2015a) *Citizen Summits on Privacy, Security and Surveillance: Synthesis Report*. Deliverable 6.10 of the SurPRISE project. Online. Available at: http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf

Strauß, S. (2015b) 'Towards a taxonomy of social and economic costs'. In Wright, D., Kreissl, R. (eds) *Surveillance in Europe*. London/New York: Routledge, 212–218.

Trauner, F. (2011) *The Internal-external Security Nexus: More Coherence under Lisbon?* European Union Institute for Security Studies Occasional paper 89.

United Nations (UN) (1994) *New Dimensions of Human Security*. Human Development Report 1994, United Nations Development Programme. New York: Oxford University Press.

Valkenburg, G. (2015) 'Privacy versus security: Problems and possibilities for the trade-off model'. In Gutwirth, S., Leenes, R., De Hert, P. (eds) *Reforming European Data Protection Law*. Volume 20 of the series Law, Governance and Technology. New York: Springer, 253–269.

Watson, S. (2011) 'The "human" as referent object? Humanitarianism as securitization' *Security Dialogue* 42(1): 3–20.

Index