Right engineering? The redesign of privacy and personal data protection

Citation for published version:
van Dijk, N, Tanas, A, Rommetveit, K & Raab, C 2018, 'Right engineering? The redesign of privacy and personal data protection', *International Review of Law, Computers and Technology*, vol. 32, no. 2-3, pp. 230-256. https://doi.org/10.1080/13600869.2018.1457002

Digital Object Identifier (DOI):
10.1080/13600869.2018.1457002

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
International Review of Law, Computers and Technology

Right engineering? The redesign of privacy and personal data protection

N. van Dijk [a], A. Tanas [b]*, K. Rommetveit[c] and C. Raab[d]

[a]*LSTS, Law, Science, Technology and Society Studies, Vrije Universiteit Brussel, Brussels, Belgium;*

[b]*LSTS, Law, Science, Technology and Society Studies, Vrije Universiteit Brussel, Brussels, Belgium;*

[c]*SVT, Centre for the Study of the Sciences and Humanities, University of Bergen, Bergen, Norway.*

[d] *School of Social and Political Science, University of Edinburgh, Edinburgh, UK.*

Provide full correspondence details here including e-mail for the *corresponding author

Alessia Tanas VUB - Vrije Universiteit Brussel, Multidisciplinary Research Group on Law, Science, Technology & Society (LSTS), Researcher, Pleinlaan 2 1050 Brussels, Belgium, Tel:+32 (0)2 629 24 60, Email: alessia.tanas@vub.ac.be,

Right engineering? The redesign of privacy and personal data protection

The idea of building safeguards for privacy and other fundamental rights and freedoms into ICT systems, has recently been introduced in EU legislation as 'Data Protection by Design'. This article studies the techno-epistemic network emerging around this idea historically and empirically. We present the findings of an 'extended peer consultation' with representatives of the emerging network: policy makers, regulators, entrepreneurs and ICT developers, but also with jurists and publics that seem instead to remain outside its scope. Standardisation exercises here emerge as crucial hybrid sites where the contributions and expectations of different actors are aligned to scale up privacy design beyond single technologies and organizations, and to build highly interconnected ICT infrastructures. Through the notion of 'privacy by network', we study how the concept of privacy hereby becomes re-constituted as 'normative transversal', which both works as a stabilizing promise for responsible smart innovation, but simultaneously catalyzes the metamorphosis of the notion of privacy as elaborated in legal settings. The article identifies tensions and limits within these design-based approaches, which can in turn offer opportunities for learning lessons to increase the quality of privacy articulations.

Keywords: privacy by design; data protection by design; privacy engineering

1. Introduction

Smart cities powered by smart infrastructures are seen as a major opportunity for societies and their economies. They are also a challenge to fundamental rights and freedoms such as privacy and personal data protection. Sensing, communicating and interacting devices gather and use enormous amounts of information about people's everyday lives. In Europe, the protection of these rights is deemed necessary and is specified in the European Convention on Human Rights and in the EU Charter of Fundamental Rights.

At the same time, we see the emergence of a design-oriented approach that aims at building safeguards to privacy and personal data protection into ICT. This involves concepts such as 'privacy by design' (PbD) and 'data protection by design and by default' (DPbD) introduced into European Legislation by the recently adopted EU

General Data Protection Regulation (GDPR)[1]; these have also stimulated a nascent field of privacy engineering.

The design-based approach to fundamental rights and freedoms reflects two topical trends in EU legislation that are key to the re-articulation of privacy and personal data protection. First, it belongs to a broader risk-based turn that brings the regulation of personal data processing towards prospective and anticipative management practices in organizations. Second, it belongs to an increasing delegation of part of the governance of information technologies from the public to the private sector through industrial standard setting, certification schemes, codes of conduct and best practices (von Schomberg, 2011) as mechanisms to 'responsibilise' the actor in control of the processing of personal data.[2]

Developments around the idea of designing privacy and personal data protection in ICT catalyze these trends by gradually moving part of the task of dealing with the scope of protection of fundamental rights away from traditional legal settings such as courts and civic actors and corresponding procedures, into more private and technocratic, upstream processes of technology development.[3]

We argue this cannot be understood without also looking at changes in the articulation of fundamental rights and freedoms. On the one hand, the hardcoding of legal safeguards and principles into technology seems a logical development given the ubiquitous proliferation of privacy-threatening and surveillance-based practices and technologies[4]. On the other hand, this evolution may imply changes in the connotations of the concepts of 'personal data protection' and 'privacy' in ways and with effects that are hard to predict[5].

In the 1990s, the privacy activist Simon Davies claimed that the character of privacy and data protection became 're-engineered'. From the 1970s to the 1980s privacy had metamorphosed from an issue of societal power relationships to one of strictly defined legal rights. In the space of a generation, the concept had shifted from a civil- and political-rights issue to a consumer- and rights issue underpinned by the principles of data protection (Davies 1998,143).

[1] European Parliament and Council Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

[2] See article 24 GDPR on 'responsibility of the controller'.

[3] Data protection through extra-legal instruments and processes in addition to law has developed gradually in most jurisdictions (see Bennett and Raab 2006).

[4] It seems to follow similar logics as approaches such as value sensitive design (Friedman, 1996).

[5] In ways analogous to those described as mediation of values and technological artefacts by sociologists of technology (Latour 1999).

In this article, we document parts of the further unfolding of this story, as, from the 1990s onwards, a second transformational wave takes this idea of 're-engineering' quite seriously. Privacy and data protection began to be conceptualised as techno-organisational measures. As in the first wave, this involves the migration of the articulation of these notions towards different sites where they begin to be dealt with by different actors. The actors that originally emerged and stabilised around the concept of personal data protection can be described as an *epistemic community* (cf. Haas 1992, Bennett and Howlett 1992). This community mobilised a relatively stable set of existing principles and knowledge base (mainly originating in law) around a set of managerial practices (mainly pertaining to private undertakings). Embraced by regulators, it gradually evolved into a proper field encompassing legal scholarship, regulators, private actors and institutions, and supported by some segments of civil society (Bennett 1992, 2008). In more recent developments, we observe a further transition to the constitution of a *techno-epistemic network* (Rommetveit et al. forthcoming 2018; see also Doty & Mulligan 2013).

Through the notion of 'privacy by network', this article elaborates on the predicament of this nascent network. It describes some main historical origins and recent developments of this network around the idea of building privacy and data protection into information technologies, captured in different concepts and approaches including 'Privacy Enhancing Technologies' (PETs), 'Privacy by Design' (PbD), 'Data Protection by Design and by Default' (DPbD) and 'Privacy Engineering' (PE) This serves as the basis for engaging in an 'extended peer consultation' in the context of the EU-funded Project CANDID[6], with representatives of this emerging techno-epistemic network such as regulators, entrepreneurs, software engineers, interaction designers, as well as with representatives from communities outside its scope like civil rights associations, 'savvy' users, ethical hackers and jurists. It discusses their views on the novelties that these new engineering practices bring to the protection of privacy and personal data in contexts of increased interconnectedness such as the Internet of Things (IoT)[7]. By letting the informants' voices come to the fore, it addresses the question of what happens when fundamental rights and principles that have traditionally served as guarantees for governing practices and actions related to personal information are now mobilised to shape technical specifications for

[6] CANDID – Checking Assumptions and promoting responsibility in smart Development – was an EU Horizon 2020 project, Grant no—732561. The project aimed to critically appraise smart technologies and to explore their prospects.

[7] The IoT is a key priority for the EU Digital Single Market. The European Commission estimates that the number of IoT connections within the EU will increase to almost 6 billion in 2020, leading to a trillion euro market (Commission Staff Working Document Advancing the Internet of Things in Europe, SWD/2016/0110). Privacy by design has been singled out as a key concern for all IoT stakeholders, especially ICT product developers (Article 29 Working Party 2014).

designing information and communication technologies[8].

The double sense of the notion of ‘right engineering’ in the title, captures two related aspects of these developments. On the one hand, the article studies different sites, actors, and challenges involved in turning legal rights and principles into matters of organisational management and into engineering requirements. On the other hand, it orients us towards the ‘extension’ of the network towards other actors dealing with privacy, which allows for the identification of tensions and limits relating to these organisational and design approaches. These, in turn, might offer opportunities for learning lessons from other relevant epistemic practices for increasing the quality of privacy articulation within and amongst these practices.

The article is structured as follows. Section 2 focuses upon the ‘second transformational wave in re-engineering privacy’. It provides a basic description of important developments leading to the present configuration of privacy, data protection and design, described as the emergence of a techno-epistemic network. Section 3 elaborates upon the notion of an extended peer consultation with various peer actors situated in and outside of this network. The results are presented in sections 4 and 5. Section 4 elaborates on four main ‘privacy articulations’ arising within the communities that are tied to the emergence of design-based approaches to privacy and personal data protection and the ways in which they are becoming networked together. Section 5 adds two privacy articulations obtained by ‘extending’ the peer consultation to jurists and publics. The conclusions in section 6 draw things together through reflection on the significance of privacy by network and describe tensions, limits and lessons of these privacy-design approaches.

2. Privacy and design, a short history

From the emergence of the Internet in the mid 1990s rapid developments of information technologies took place. Governments and businesses struggled to encourage public acceptance and adoption of technologies seen as increasingly privacy-invasive (Clarke 2009). In Europe and beyond, the main legal source of reference for privacy and personal data protection principles was the European Data Protection Directive 95/46/EC, adopted in 1995. The discourse about technological solutions for privacy protection was introduced into the data protection regulatory

[8] This shift to the articulation of rights in the sociotechnical design of ICTs does not imply that other modalities like written text disappear. ‘Just as written law has not replaced the role of unwritten law but complemented and changed it, written law as well as unwritten law will continue to play a key role in providing legal protection’ (Hildebrandt and Koops 2010, 454).

community where the regulation of privacy and data protection was still mostly comprehended from a legal perspective.

Privacy by Design (PbD) has its roots in this period, which, in turn, derives from Privacy Enhancing Technologies (PETs) and Privacy Impact Assessment (PIA). PIAs emerged in the 1990s in response to increasing public reaction against excessive data processing practices, and to manage the risks of damage to reputation of organizations. A main argument was that rights infringements identified in the assessment could be mitigated through changing the technological design. PETs marked a shift from conventional legal regulation to privacy information systems, so that 'when a new information system is being engineered ... the designer can take the user's privacy into account during the different phases of the design process'[9]. These digital technologies centered on protecting people's identity through anonymization and minimizing the use of personal data.[10]

The intersection of technology and privacy opened up a 'new landscape' (Agre and Rotenberg 1998) with important consequences for existing institutional constellations. Law started to be perceived as having regulatory limits, captured in the image of a 'law lag': law always lags behind the speed of development of ICT technology (e.g. Reidenberg 1998). In several famous publications (Reidenberg 2008; Lessig 1999) law and technology were portrayed as alternative regulatory choices in directing the behavior of individuals. These writings provided academic and theoretical authority and made the model more generic. They sparked heated academic debates on the nature of law and technology as regulatory instruments (Brownsword 2005; Gutwirth, De Hert and De Sutter 2008; De Vries and van Dijk 2013) and the formulation of alternative concepts like 'techno-regulation' (Leenes 2011; Koops and Leenes 2014) or 'legal protection by design' (Hildebrandt 2011). Others saw law and technology as part of a broader and complementary array of policy instruments (Raab 1997; Bennett and Raab 2006).

From the start of the new millennium, the ICT sector was increasingly seen as a major driver of economic changes at global scale (OECD 2006). Information security and privacy gained attention, and globalisation and convergence of business practices linked to networked ICT infrastructures led privacy commissioners to demand uniform privacy criteria (Cavoukian 2006). There were many efforts to formulate privacy standards and principles for the design of IT systems, and privacy commissioners were highly vocal through a series of initiatives and resolutions. These

[9] Hes and Borking 2000, 41.

[10] These technologies had been developed since the 1980ies by computer scientists and cryptographers, most notably David Chaum (1981).

included the 2004 Wroclaw *Resolution on a Draft ISO Privacy Framework Standard*, the 2006 *Global Privacy Standard*, the 2007 Montreal *Resolution on Development of International Standards* for the use of privacy technologies, and *The 2009 Madrid Privacy Declaration*. The latter was signed by some 300 civil society representatives and experts concerned about the expansion without 'independent oversight' of personal data processing by corporations and about 'unaccountable surveillance'. It supported 'genuine Privacy Enhancing Techniques' whilst also calling for respect of human rights, support for democratic institutions, and full participation of civil society in the privacy protection framework. The Montreal Resolution called for 'the involvement of the data protection and privacy community' in the 'interpretation of legislation in the context of technology standards'. Here law was conceived to have regulatory limits *vis-à-vis* technological developments, but technical settings were also considered insufficient to ensure consistent interpretation of, and compliance with laws.

Work initiated by the International Organization for Standardization (ISO) working group on 'Identity Management and Privacy Technologies' led to the adoption in 2011 of standard *ISO/IEC 29100,* a general privacy framework for information technologies, which enhanced existing security standards by adding a focus on the processing of personal data. The standard primarily addressed organisations engaged in the processing of personal data but it was also envisaged to aid in the design of ICTs. Work on an ISO standard on privacy engineering is currently ongoing (ISO/IEC AWI 27550).

Specific co-regulatory standardisation initiatives for privacy by design have followed in Europe. In 2015, the EU Commission issued a mandate for the European Standardisation Organisations to develop standards for service providers, but also manufacturers[11], to execute 'Privacy by Design' during the design of security technologies.[12] Similarly, the European Commission *Rolling Plans for ICT Standardisation* (issued from 2013 to 2017), referred to cross-cutting ways of dealing with privacy in technological domains that are key to the Digital Single Market such as the IoT, big data, smart grids and smart cities.[13] Work was also undertaken to create a common EU methodology for privacy and data protection risk assessment for RFIDs and smart grids. Two 'templates' were established in 2011 and 2013, through processes of co-regulation by many stakeholders including the European Commission,

[11] European Commission M/530 Implementing Decision C(2015) 102 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management.

[12] See Kamara 2017 on this case as an example of an increasing co-regulation approach to EU data protection.

[13] See for instance, European Commission Rolling Plan for ICT Standardisation 2015, GROW/H3.

data protection authorities (DPAs), industry and academia (Beslay and Lacoste 2012; Article 29 Working Party 2010).

Thus the idea of designing privacy protection into ICT systems started circulating in various institutions and domains, and gradually became consolidated as an approach, complementary or alternative to a 'deficitary' legal lag, calling for the vacuum to be filled. An international network of privacy and data protection authorities, technology developers, businesses, standards development organisations, and privacy advocates took shape around this idea, originally the notion of PETs. This was gradually accompanied by an endorsement of greater self-regulation for the corporate sector. Eventually the broader approach of Privacy by Design (PbD) was developed for addressing privacy concerns by going beyond specific technologies, and aiming at the overarching organizational level. It focuses on the broader socio-technical dimensions of ICT development within organisations and includes business methodologies, models, guidelines for management, marketing, customer relations and trust, use cases, accountability and legal compliance. The 'philosophy' of PbD was further consolidated into seven 'foundational principles', applicable throughout the whole life-cycle of software development and maintenance (Cavoukian 2009).

Finally, the notion entered legislation through the adoption of the General Data Protection Regulation (GDPR) in 2016. Known as Data Protection by Design and by Default (DPbD) in article 25, it will be mandatory for organisations ('data controllers'). The DPbD notion seems to have roots in PETs and PbD (i.e. pseudonymization, data minimization, etc.).· On the other hand, it is inscribed explicitly within the logic and scope of European Data Protection Law and does not necessarily cover all aspects of the right to privacy[14].

These developments have further strengthened the move 'from policy to engineering' (Danezis et al. 2014), since a strong gap is perceived to exist between the regulatory discourse on PbD, based on generic techno-organisational principles, and the growing field of 'privacy engineering' (cf. Spiekermann and Cranor 2009; Cavoukian, Shapiro and Cronk 2014; Gürses, Troncoso and Diaz 2015; Finneran Dennedy, Fox and Finneran 2014; Notario et al. 2015, Gürses and van Hoboken 2017). Although this field existed since the 1990s especially in the context of ubiquitous computing systems (Bellotti and Sellen 1993; Langheinrich 2001), it received a boost from 2011 onwards (Gürses and del Álamo 2016) and quickly emerged as 'a hot new career' opportunity (Cranor and Sadeh 2013).

[14] Enshrined in article 7 of the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.

Privacy engineering mainly comes from software engineering, a subfield of computer science, but extends towards other fields such as information security, human-computer interaction, and machine learning. Generally, the main aim of the field is to turn (abstract) ethical and legal principles into practices and methodologies that can be used to hardcode privacy and data protection requirements into ICT. Different approaches to privacy engineering can be distinguished. The first, 'privacy by architecture', builds on the tradition of data minimization and pseudonymization pursued in PETs and is very technological in nature. The second, 'privacy by policy', has a more organisational and legal orientation, focussing on implementing principles of notification, specification and choice for data subjects about data processing operations (Spiekermann and Cranor 2009), and on the rights of the user as granted by data protection law. A third approach, 'privacy by interaction', focuses on the sociotechnical aspects of design intended to improve users' agency in different contexts (Gürses and del Álamo 2016). This is more social in nature and would include contributions by social scientists, ethicists, humanities scholars and the participation of data subjects in design processes. In the conclusion we will introduce a fourth conception of 'privacy by network', which is a specific quality of socio-technical networking processes aimed at designing privacy in highly interconnected ICT infrastructures.

2.1. Remarks on historical developments

Efforts to deal with the design of privacy and data protection have been undertaken at heterogeneous sites and by a plethora of different actors in complex hybrid ecologies of practices. This implies that in the association of these concepts with design, the general goals may be set by regulators and legislators to protect fundamental rights and stimulate markets, but specific means must come from engineering techniques, standards and technical specifications that are agreed upon collectively in sectoral and international multi-stakeholder fora, including standardisation.

Hence, the nascent techno-epistemic network of privacy engineering, taking on the 'by design' task, has its main site of operation in technical domains and crucially relies upon the contributions of actors from regulation, risk assessment, standardisation, certification, etc. As we show in following sections of this paper, this is not the only option available for the constitution of the techno-epistemic network. The network could for instance also take its mandate directly from privacy-concerned publics.

3. Extended peer consultation on privacy-design

A main question related to privacy engineering pertains to the ways in which notions of rights are re-negotiated and re-designed as a consequence of these processes. A right will acquire new imagined characteristics when dealt with in contexts of risk management by organisations having the task to protect data. On the other hand, a right acquires material characteristics when hardcoded into ICT systems and infrastructures. We enquired about these issues in the EU CANDID project[15] in which we explored the ways in which the fundamental rights and freedoms of privacy and personal data protection are concretely being evaluated and translated into ICT systems. Based on the mapping of the techno-epistemic network of privacy design, we conducted an extended peer consultation exercise.[16] We contacted a wide range of actors engaged within and situated outside the emergent network described in Sections 1 and 2. Among the 60 peers consulted, 24 had a role in activities related to the assessment and design of privacy and personal data protection in contexts of digital technology. We consulted with representatives from the communities that have played a role over time in the evolution of the notions of PETs, privacy engineering, PbD and DPbD, namely DPAs, universities, standardisers and business experts and consultants. The exercise also involved technology developers, engineers, social sciences and humanities scholars, specialists in interaction design and value-sensitive design. We also involved actors positioned outside this network, extending the consultation on these design-based approaches to other peers with relevant experience and knowledge in articulating privacy. These included legal scholars and judges in European high courts, civil rights organisations representing concerned publics, and ethical hackers and technology 'savvy' users who themselves participate in developing privacy-friendly technological systems.

We engaged with these peers by means of written questionnaires or interviews through which they were presented with issues concerning DPbD and DPIA. We wanted to understand from peers what constitutes privacy and personal data protection in design. A main result is that different ways of imagining, understanding and articulating these notions exist. We found that most peers referred to 'privacy' rather than to 'personal data protection', in line with the historical developments within the network of designing 'privacy' into ICTs (as captured in the notions of

[15] *Supra* note 6.

[16] We draw inspiration from the notion of 'extended peer review' elaborated by Funtowicz and Ravetz (1993). An extended peer review is the process of including people and groups that have experience and knowledge beyond academic science when trying to assure the quality of research, thus increasing the reliability of results. Here we apply the concept within a techno-regulatory context, also with the aim of extending to other epistemic sources.

PET, PbD, PE).[17] We thus were able to identify a list of ‘modes’ in which privacy becomes articulated as:

- protection by the data controller
- an organizational risk
- an engineering requirement
- a transversal concern for infrastructure standardisation
- a human right
- a public and civic freedom

As we see in Section 4, the first four points pertain to actors that played important roles in establishing and perpetuating design-based approaches, positioned at core nodes of the privacy-design network. This review shows certain tensions among the ways in which privacy becomes articulated. In Section 5, we address the latter two privacy articulations in the list and proceed to describe the ‘extension’ of the consultation to actors situated outside the network and holding disparate views. This will point to new tensions and to the possibility of learning lessons. The presentation of each ‘privacy articulation mode’ in Sections 4 and 5 is split into two parts. The first lets the peer voices come to the fore, while the second is followed by an elaboration that extrapolates the meanings, limits, tensions or lessons discerned.

4. Articulations of privacy across the design-based network

4.1. Protection by the data controller

A representative of a DPA who is involved in regulatory processes at national and European level describes DPbD as a development that ‘could really make a change’ as an instrument ‘backed by the force of law’ and associated with the principles of transparency and accountability. The peer sees in this a shift from privacy-focused technologies towards the design of personal data protection, implying a difference between these approaches:

> Peer (DPA): we know (…) privacy by design, privacy enhancing technologies (...), but now we have a different approach because of the GDPR. It’s not totally different. But we have to make sure that now the main focus it’s about data protection...The GDPR, assumes that there is a data controller.

[17] From this perspective personal data protection, as captured in the notion of DPbD, becomes another such articulation on top of these earlier privacy design developments, in spite of the fact that privacy and data protection are often considered distinct in legal practice.

The notion of personal data protection by design predominantly centers on the role of the controller as the responsible entity for the protection of individuals. This is not necessarily the case, for other type of protection systems such as PETs that can also be directly deployed by users themselves. Because of this, according to the peer, the GDPR is not 'technology neutral'.

She is in favour of a regulatory framework that puts the burden of personal data protection on organisations as 'powerful players' rather than 'on the shoulders of the citizens'. This is related to the complexity inherent in current algorithmic data processing practices:

> Peer (DPA): the idea is that it's possible to understand what is happening otherwise you cannot decide, and this is a big challenge. (...) If there are algorithms working on databases that are collecting data all the time then it's simply too complex. (...) there's so many automatic decisions where I'm not even aware that this decision had been done.

The peer argues that this points to the limits of the right to informational self-determination according to which subjects need to have the capacity to make autonomous decisions about data processing. She also explains that the current emphasis on the data-controlling organisation in data protection legislation may not be sufficient as it mostly overlooks the important role of manufacturers and system developers. These are the actors that actually integrate data protection safeguards into technology but GDPR merely 'encourages' them to practice DPbD in product development[18]. For this reason she believes that GDPR '*has a flaw*' and would like to see manufacturers addressed in a direct way. She maintains that the Regulation should be interpreted in a way that also allows individuals to make use of 'self-defence' technologies as this would reinforce the array of protective instruments.

The possibility for individuals to make use of such technologies is also an important point of attention for other peers. The most emblematic example comes from representatives from the Quantified Self, an international movement of ICT prosumers that has recently developed plans for realising a user-centric personal data management system. The system places the user at the point of integration for

[18] Recital 78 of the GDPR states that '*producers* of the products, services and applications *should be encouraged* to take into account the right to data protection when developing and designing such products, services and applications [emphasis added].' Bygrave (2017) remarks that 'the Regulation evinces an expectation that the duty imposed by Article 25 on controllers will be passed both 'downstream' to processors and 'upstream' to technology developers.' (p. 116).

different data-streams. Individuals thus act themselves as data controllers. At the core of the approach is a specific understanding of privacy:

> Peer (ICT prosumers movement): Privacy (...) has to be created with autonomy because it's about you shaping your own identity vis-à-vis the external world. If you have no privacy, how can you have identity?

Such a definition of privacy as essential for autonomous identity formation, resonates with the ability to take autonomous decisions within the right to informational self-determination. The peer however argues that promoters of user-centric systems of the kind described face the difficulty of finding a business model that could sustain them, including venture capital and investors. Due to such a 'practical imperative', the original idea usually 'moves towards something completely different to what had been imagined'.

4.1.1. Data Protection by Design: refocusing from individuals to controlling organizations

The introduction of the notion of DPbD in the GDPR fortifies a trend within the larger techno-epistemic network of privacy design. Strong emphasis is put on data controlling organizations for ensuring DPbD, but they must rely on solutions developed by technology producers who, in turn, are only 'encouraged' to take personal data protection into account.

In such a context, it is unclear whether alternative design systems for individuals to act autonomously towards data protection remain available. Complexification of data analysis and automated decision-making is an important justification for a regulatory framework solidly based on the role of a data-controller organisation. This corresponds to a departure from solutions focused on the individual and his or her capacity to control data and make autonomous decisions, as is for instance recognised in the understanding of privacy as informational self-determination[19]. Instead these solutions are increasingly focused on the protection of personal data by an organisation, under the header of DPbD. This regulatory trend finds a concrete matching in the financial difficulties encountered by promoters of alternative user-centric systems.

[19] This right was first recognised by the German Constitutional Court in 1983 (BVerfGE 65, 1). It can be understood in association with the free development of personality according to which subjects need to have the capacity to decide autonomously (See Gonzalez Fuster 2014).

4.2. An organisational risk

Many peers depict a situation in which organisations still find it difficult to act as data controllers. In particular, a reputed public and private sector consultant, with long-standing experience in data protection regulation, explains that they ‘have to realise that there is a risk’, otherwise they ‘will not do anything’:

> Peer (Consultancy DPIA and DPbD): to understand this, organisations have to analyse in depth their data flows and most organisations haven’t done that (...) and actually do not know what kind of processing is taking place.

She proposes a definition whereby the possible damage to a fundamental right is compared to the damage to assets of the organisation:

> Risk is a probability that, due to a particular threat, a particular vulnerability exploits it and causes a damage to an asset. In this case, it would be damage to the fulfilment of a human right.

She sees evaluation of risks in contexts of DPIAs as the pre-requisite for adequate deployment of DPbD but explains that although the GDPR makes it compulsory, it may take time before it will be accepted as ‘something you have to do’. DPbD is ‘low’ in the general administration and industry agenda, ‘it takes time and money’ and data are of high value.

The peer believes the situation may change if DPbD is accompanied by development of a DPIA according to specific templates that should be developed within multi-stakeholder fora. She mentions the example of the (D)PIA methods for RFIDs and smart metering systems developed by market, policy actors and ‘people that understand those processes’ endorsed by the European Commission (see section 2). The peer also believes the development of standardised ‘building blocks’ for PbD could meet organizations’ needs, helping them to overcome the difficulty of customized solutions.

Another peer from a data-controller organisation expresses the need to conduct discussions over privacy and security as risks at ‘chain level’. She explains that all chain actors are currently trying to assess their own risks:

> Peer (energy distribution utility): organisations should think broader than their own responsibility and create a common mind-set of which risks there are in a chain. And that is very difficult if you have multiple stakeholders in the chain.

In her view, organisations should thus develop joint strategies to face common challenges beyond their own responsibility.

4.2.1. Towards standardised risk assessment methodologies for DPbD

The association of personal data protection with the 'risk to an asset' corresponds to a conception of 'rights as risks' for an organization that have to be managed (Murphy and Whitty 2009; van Dijk, Gellert and Rommetveit 2016). On this conception, human rights become economic resources that can be controlled through risk management and design in order to produce value, or in this case, used to prevent damage to the company.

Networked efforts to develop methodological risk assessment templates for (D)PIAs (as for RFIDs and smart grids) and the development of design methods based on standardised building blocks are believed to be more effective than customized solutions. These standardised solutions are developed by expert professionals (regulators, risk assessors, sector stakeholders, etc.) who mobilise their different (disciplinary) knowledge bases. The underlying *rationale* is that many actors and fields become aligned with standardised risk assessment methodologies in support of specific design frameworks. This mirrors the point on chain evaluation of risks, raised by the peer from the energy infrastructure field. The standardised templates and building blocks function as stabilising promise for all actors in the chain and as solutions to many concerns such as ensuring action towards rights' protection for regulators, addressing regulatory uncertainties for organisations, etc.

4.3. An engineering requirement

We have engaged with representatives from the privacy engineering community, working in departments of applied research of technical universities, ICT engineering experts cooperating closely with DPAs, and consultants for the regulatory and the private sectors. There is a level of indeterminacy with regard to the concept of privacy. For instance, some peers report problems understanding what exactly should be protected. They refer to privacy as insufficiently rigorous to translate into a 'formal definition':

> Peer (engineering - user interaction design): privacy is too vague and is difficult to align with the concrete character of engineering requirements and things engineering needs to consider.

She moreover points to a disjunction between the reasoning styles of engineering and law. Most of the time, 'legalese' is not enough to 'bake' protection in an algorithm or system.

> Peer (engineering - user interaction design): There is a difference between the moral reasoning linked to human rights and the attempt of solving an engineering problem, which is technically and mathematically specified.

There is considerable difficulty in translating legal principles into 'engineering requirements'. Such abstract values often 'do not acknowledge the level of specificity required by engineering' where many decisions have to be made all the time that 'pass under the radar' but 'we still have to stick a 'privacy label' to them'. Another peer from privacy engineering mentions that some exercises end up focusing on design solutions that are based on 'somewhat arbitrary goals' that can be 'easily defined' in mathematics. This is problematic to the extent that design goals are meant to articulate the problem that the technology tries to solve.

Other peers are more optimistic and refer to methodologies that can contribute because they try to 'minimise the data that is kept for a long time in machine learning applications by means of selective data systems'; 'seek to integrate fairness in machine learning predictions'; 'identify and develop privacy requirements that are built based on interdisciplinary insights'; or 'try to make the bridge between technical system building and social findings'. At the same time, most peers agree that what works in one context may be unsuitable in another and some ready-made solutions could have unforeseen side effects. The combination of two best available technologies with good privacy features may for instance cause the loss of protection, due to increased data linkability and loss of anonymisation guarantees.

One peer argues that impact assessment for privacy and personal data protection can provide important orientations for design, since their outcome 'gives you chances of understanding the design space' and thus to come up with better PbD choices 'because you understood better the data you are collecting, the reason for collecting it, the impact that the data might have, the weaknesses that you may encounter, the vulnerabilities and so forth'. At the same time, she acknowledges the lack of determined instructions:

> Peer (engineering - ubiquitous computing): you could argue that Privacy Impact Assessments are part of Privacy by Design Processes, but I really think there isn't a fixed recipe for Privacy by Design unfortunately. I think there are few books now out there but there isn't really a 'look-at book' to tell people what to do and how to do it.

4.3.1. Legal principles and engineering requirements: in search of mediators

It is possible to identify recurring traits in the privacy engineering exercises described. A first noteworthy finding is that most peers do not clearly differentiate between the concepts of privacy (PbD) and data protection (DPbD) in discussing programming frameworks, a distinction that is for instance firmly enshrined in the EU Charter of Fundamental Rights.[20] At the same time, privacy clearly emerges as a real engineering challenge when it has to acquire material characteristics of ICT. Peers report a significant degree of uncertainty about how to translate such a polysemic concept into technical and mathematical language. Whereas the translation of legally significant principles into technical specifications is important as it determines how rights are protected, major difficulties emerge because of differing reasoning styles in human rights and engineering disciplines. This difference is worth exploring. Our peers explain that it takes substantial research to achieve a good outcome. The way rights become *de facto* implemented ultimately depends on discretionary decisions about code, hardware and software, requirements as well as technical and mathematically specified language.

Such processes are not very flexible. They are tailored to the specificities and constraints of engineering practice (a particular 'goal' or algorithm) and a small change can require a lot of work. The scope of interpretation for good outcomes in terms of rights protection is framed within relatively fixed boundaries, even when including the guidance that could be found in DPIA. There is a considerable difference with the types of hermeneutic at stake in legal approaches. These instead consist in complex articulations within a case between polysemic legal principles, disputed facts, resonance with other cases, authorization by sources and procedural

[20] The Charter recognises privacy and personal data protection as two distinct fundamental rights in articles 7 and 8. The right to privacy protects the individual by warranting a certain level of opacity to the citizen (Gutwirth and De Hert 2007). Opacity guarantees non-interference in individual matters by the state and, more recently, by private actors. The right to personal data protection instead imposes a certain level of 'transparency' and accountability on the exercise of power.

conditions, whereby certain contents are qualified, formalised and 'jurimor-phed' (Gutwirth 2015), (van Dijk 2015).

4.4. A transversal concern for infrastructure standardisation

Some peers explain that today's increasing big data processing and growing interdependencies in the Internet of Things imply an adaptation of current approaches to privacy design, in close association with security practices. This is because in situations of increased interconnectedness privacy and security risks can escalate and become systemic. Privacy in the IoT thus not only concerns single devices but also the communication links with other points in this ecosystem. Several peers explain that there is a need to go beyond the organisation as the unit for achieving privacy protection in order to shift focus from single ICT technologies to highly interconnected ICT infrastructures.

Novel technical aspects thus emerge through the need to establish interoperability and standards. This is not an easy task because the degree of consistency between sub-systems required by an IoT ecosystem is high and '99% focus of technical people is about solving this as the '*sine qua non* condition for the market to happen'. A peer explains that many efforts within standardisation bodies are currently aimed at 'integrating things and applications so that we have something consistent'. This has implications for the way privacy safeguards are conceived and become articulated.

> Peer (consultancy DPbD): When we want to take into account privacy and other concerns, we have to take them into account as transversal concerns (...) security, privacy, safety, energy consumption or taking into account ethical aspects and things like that. (…) we need to be able to engineer transversal concerns and 'capabilities' in things.

The peer argues that building these systems is a very complex exercise. Standardisation efforts are often aimed at integrating privacy concerns as horizontal capabilities for IoT products and systems in such a way that interoperability is granted. Privacy here enters as a 'transversal concern' that needs to traverse, connect and align different social and technical aspects of these complex systems. First, there is the complexity of the technical aspects, since the IoT depends on interoperability among (at least) three levels: applications from service providers, things with certain capabilities enabling service provision, and semantic points of interconnection between the other elements. Privacy thus has to be designed into each level to allow interaction among them, by being translated into a 'service description' and standardised through semantic interoperability specifications.

Secondly, complexity is related to the fact that in the IoT many different applications and things that are often built by different companies, will have to communicate with each other, but frequently lack coordination. In this respect, the peer sees a need of a 'chain perspective' in developing the IoT: 'we know "from the start" that there is an issue of not having IoT devices built with the involvement of stakeholders'; including end-users.'Co-creation' is proposed as a solution, involving customers and application providers in the design of IoT, including privacy concerns. The concept of privacy is here operationalised according to an approach from customer relations management and applied to the technical semantics of IoT architecture presented above.[21] This privacy terminology feeds into the standardisation exercises to achieve the required coordination between the different actors involved.

The peer explains that the technical complexity of this IoT architecture is often not grasped, whereas it determines the bulk of the work by technical people. This complexity reduces the scope of co-creation, since it can limit the feasibility of solutions sometimes deemed desirable by users or social scientists (e.g., those formulated in use cases). In this sense, the peer states that:

> Peer (consultancy DPbD): You can only suggest to user things you are sure you can implement otherwise you break the trust link between the user and the designer.
>
> and
>
> Peer (consultancy DPbD): The gap is just too big between the user and the engineer that knows the capability of the robot (…) it is really about building a language for co-creation (…) This vocabulary must be mapped with technical capabilities that the engineer has in mind. (...) We look at privacy and user. We should be able to explain the user the capability of the technology and then we are sure that he understands.

The engineers have thus to take the lead and start by mapping and describing the technical capabilities of the product and service. Users only come in after technical

[21] Co-creation is an approach for the joint creation of value by the company and the customer. Its principles are: dialogue with users, access to data, risk assessment and transparency of information (Prahalad and Ramaswamy 2004).

capabilities have been transformed into a 'user taxonomy' that is sufficiently intelligible to test the user's 'trust'. Social scientists can also be involved if they can help to ascertain the acceptable level of trust for users; the peer considers that 'trust is about psychology'.

A similar perspective is taken when the peer comments upon advantages of IoT technologies for smart cities. She refers to initiatives within the European Innovation Partnership on Smart Cities and Communities (EIP-SCC)[22] where a 'Citizen Centric Approach to Data-Privacy by Design' is taken. She explains PbD processes should be done by 'independent' people who 'understand how privacy is built, people that citizens trust', for assurance that 'a product is done properly', while citizens' associations could verify the process.

4.4.1. Assuming compliance in complex network inclusions

We learn that in current contexts of increased interconnectedness, it is highly probable to inherit or contribute to a systemic escalation of risks, thus raising issues of code reliability and shared responsibility for market actors in ICT ecosystems. We have described efforts to neutralise risks not uniquely at the level of single technologies but from an infrastructural perspective, and how standardisation facilitates these attempts. By reconciling the views of market actors on how to foster integration of components for the IoT, standardisation also supports their collective decisions about distributed responsibilities.

There is generalised confidence that once standards are established, they can support conformity of IoT products to legal requirements. Standards *per se* are however not a guarantee of legal compliance[23]. Their conformity to law is presumed. Yet standardisation has acquired an increasingly important role in public policies to spur technological innovation[24]. This leaves a number of important legal issues open in the recent European approach, such as how far delegation of public rule-making to standardisation bodies may go and who is responsible for the content of the standards.

[22] EIP-SCC is a PPP supported by the European Commission bringing together cities, industries, SMEs, investors, researchers and other smart city actors. http://eu-smartcities.eu/initiatives/2/description

[23] Standards imply a process through which organisational claims about adherence to norms can be more objectively tested (Bennett and Raab, 2006).

[24] Standards 'play a very important role within the internal market (...) in the presumption of conformity of products to be made available on the market with the essential requirements (...) laid down in the relevant Union harmonisation legislation'. Recital 5 of European Parliament and Council Regulation 1025/2012 on European standardisation.

Other tensions with law come to the fore in the way that courts are striking down certain standards through judicial review (van Gestel and Micklitz 2013).

Some have even argued that ‘techno-policy’ standards for privacy design of digital technologies (e.g., the internet) constitute new modes of governance beyond traditional state governance, but also beyond self-governance, towards co-governance in multi-stakeholder fora where certain actors become interdependent and regularly interact (Doty and Mulligan 2013).

In the case of co-creation, privacy becomes articulated into different (infra)structural levels in the form of the technical specifications needed for the IoT to function. The concept also becomes co-articulated and associated with other transversal concerns, especially security, safety but also trust and interoperability. Adequacy of privacy protection is associated with degrees of consumer trust, but what this means remains underdetermined. The connotation of privacy and protection of personal data as fundamental rights does not seem to play a determining role in the legitimation of the system described. The criteria for the interplay between privacy protections *vis-à-vis* standardisation concerns and for decisions on potential trade-offs between them are not clear. Apart from being tied to technical constraints – i.e., capabilities, semantics, specifications – such decisions are generally oriented by the technology development culture embraced by manufacturers, developers, innovators. These types of interplay deserve more attention in light of the central role of privacy for societal power relationships and its transformational waves described in Section 1.

Lastly, other interesting transformations can be observed with privacy assuming a ‘transversal’ role. The European Commission explains that work on the basic infrastructure for ICT systems is of horizontal relevance[25]. In such a perspective, privacy standards apply to very different policy areas and sectors, and must also serve various purposes by dealing with both protection of personal data (including, where needed, through PbD) and the free movement of such data in order to foster progress in key technologies that are critical to the completion of the Digital Single Market and to innovation initiatives, such as the one on smart cities and communities (EIP-SCC). The citizen-centric dimension of the latter addresses the need for all supply-chain actors involved in making smart cities to coordinate efforts. This serves to meet the demand for compliance checks and privacy standards from policy-makers and to

[25] In this view, work on the basic infrastructure for ICT systems is of horizontal relevance and ‘standards should be considered as building blocks. Metaphorically, one could see these technologies such as Lego pieces that can be utilised to build complex architectures.’ (EC Rolling Plan 2015, p. 5, *supra* note 13). Privacy aspects are a prime example.

scale-up privacy solutions by establishing guidelines for PIAs, PbD, and ‘chain oriented’ standards[26]. Nevertheless, whereas users or citizens are frequently placed up-front as prime beneficiaries of ICT developments, their views cannot be fully included due to systemic and technical complexity, intrinsic to the development of an interoperable, smart ICT infrastructure. Where the techno-epistemic network is stabilising, other main important aspects of privacy, i.e. law and civic concerns, are more bottom-up and local in nature, and may struggle to keep up with the direction of these activities, as we describe in the next Section.

5. Extensions towards legal practices and publics

> Privacy by design is a technical approach to a social problem. Obviously technology cannot help with all related aspects. Especially in the field of privacy, which touches various basic rights topics, such as freedom of expression and press, or protection from discrimination, issues have to be tackled in a grander scheme by society as a whole. (Danezis et al. 2014, 48)

In the historical overview (Section 2) we have already noted important points of divergence within the processes that led to the formulation, stabilisation and proliferation of design-based approaches to privacy. These coincide with the two historical transitions through which the concept of privacy has become ‘re-engineered’: from a civil-political right dealing with societal power relations, to a more narrowly-defined right to data protection and consumer issue, and recently to a matter of socio-technological design of ICTs.

In this section we link back to those two points of divergence by consulting with disciplines and practices currently situated outside the techno-epistemic network and which also hold experience and knowledge with regard to privacy in ICT technologies. This is why the notion of ‘extension’ is at the heart of the ‘peer consultations approach’ described in Section 3. It allows the inclusion of other actors who have contributed and still contribute to making privacy a public concern and a legal right. These outside views may provide further clarity about the limits of the network, of possible tensions in its making, and of disciplinary constraints that should not be transgressed.

[26] Especially ISO 27550 standard on Privacy Engineering (see Section 2).

5.1. A human right

In section 4.3 we have learnt that a significant gap exists between practices of law and design that makes it difficult to turn legal principles into engineering requirements. We entered into dialogue with jurists with privacy and data protection experience to learn more about the nature of this gap, now seen from the legal side of the equation. A judge from the Court of Justice of the European Union explains that 'obviously' jurists understand that engineers and other technical experts 'do not think about human rights when they work', this being the reason why 'the law' must play a role 'which is of course posterior' to that of design, and that 'technical experts should be aware of the limits of their activities'. Legislation gives 'orientations' for data-collection activities to be respectful of fundamental rights and freedoms, but it cannot foresee all possible situations:

> as the case-law shows, situations are so different (...) even if you provide for detailed rules in law, in certain cases they will not be applicable or their application would create a bad result (...) this is the task of law, of doctrine, of case law to find in a concrete case a justified solution.

In this perspective, decisions on rights safeguards, taken in contexts of technology design, are not constitutive of law. Law intervenes *ex-post* to articulate and ascertain whether the scope of protection of a fundamental right has been correctly formulated. The judge explains that interpretation is not an easy task:

> we know the cases when the producers do not understand the legislation, do not understand a judgement. This self-restriction is a difficult task and they can never be sure that their way of limiting themselves would be appreciated correctly in a future court case.

Similar limitations were pointed out by a human rights lawyer[27]. From the perspective of human rights, impact assessment practices could trap rights inside a regulatory and legalistic cage.[28] Assessment based on organisational techniques relocates the seat of

[27] This contribution was made in a peer public session focused specifically on DPIA. See van Dijk and Rommetveit 2015.

[28] The peer states that contributions from ethics and social science may not be able to counter this tendency but could rather enhance them. Such shifts could imply epistemic divisions concerning who is articulating what within these processes. She argues that this poses the risk that human rights such as privacy are separated in two components, in which the articulation of privacy as a value is delegated to ethics and social (ELSA) studies and the articulation of privacy as a right to jurists. This externalizes values from human rights.

articulation of fundamental rights such as privacy to risk managers and privacy impact assessors, away from traditional actors and institutions such as courts, but also in wider society from citizens and human rights activists. This peer remarks that if such assessments are to be made, they should be anchored in the discourse of human rights rather than in risk management.

She also argues that an exclusive focus on privacy and personal data protection in these design practices implies a narrowing of the subject. Other human rights such as dignity, non-discrimination and equality also have to be considered by engineering disciplines. A peer from the field of technology regulation formulates a similar argument but sees such broadening of design focus as a complex task. She argues that if the notion of DPbD is 'confined' to data protection, then it is possible to provide transparency regarding compliance with the GDPR (with respect to the purposes of data processing, for instance). However, 'if DPbD is supposed to cover rights (beyond data protection) things are much more complicated'. The peer believes that jurists should participate in impact assessment to evaluate GDPR requirements and other possible legal consequences of data processing.

Along these lines, the human rights lawyer believes impact assessment and design processes should grow from human rights commitments and identify attributes of these rights from case law. She specifies that lessons can be learnt from international human rights law and international binding treaties and from attempts to incorporate human rights into commercial practices, as in human rights impact assessments.[29] She expands on this more co-constructive approach to risk and design by proposing a few suggestions:

> Peer (Human Rights Field): There might be a rights-based alternative like sustainable development for better ICTs, or the notion of 'good science' formulated by Charis Thompson. Perhaps the notion of good engineering could be helpful here? There needs to be a conversation between risk, design and engineering people, but herein some legal guarantees may be lost and this must be acknowledged.

The peer refers to the notion of 'good science', relating to a co-production of science with ethics in innovation.[30] Instead of just following after, or impeding research and

[29] See Harrison 2013.

[30] Thompson 2013. This both goes beyond the ideas of ethics having to 'clean up' after science (ethics lag), or of merely describing the ethical, legal, and social implications of scientific research and development (ELSA studies).

development, it has a pro-active role in intervening in science-in-the-making and is thus co-constitutive within this process.[31] In the context of engineering rights, it implies a co-production between design, risk and right-based actors including engineers, lawyers, risk managers and publics, which might imply mutual transformations in the contributions of each. In direct response, a social scientist peer working in the context of IoT design argues that good engineering implies the need to develop local infrastructures and is associated with contextual technology.

5.1.1. Towards good engineering: lessons from law

The discourses on 'privacy by design' and especially 'code as law' have evoked the promise of bridging the gap between law and technology both in practice and in theory. As such they have often functioned as useful conditions for different actors to cluster together, but also to draw legitimacy from and through law. We have however already seen that in practice this exercise is riddled with difficulties of mutual incompatibility. Hence, we see that various peers from the legal field also reinstate a firm divide: legal practice needs to maintain a critical distance to check technical articulations of rights, based on its own quality procedures, resources and concepts. Perhaps it reminds us of the obvious: that what the privacy engineers do is not itself something juridic, but the obvious might have become blurred by such analogies, and may become further blurred as these practices expand and become powerful norm-setters. Certain principles that have become enshrined in the law over time (and existed earlier as political freedoms or social values) are now articulated according to the concepts, tools and methods of the practices of engineering and risk management, moving these notions away from the idea of rights articulated in courts with all the longstanding procedural guarantees and checks of epistemic quality (due process).[32] This points to a need for a firmer embedding of design-based approaches to rights within extended ecologies of practice. Further principles and procedures might be needed for proper checks and balances to be exercised: between different epistemic and normative commitments, between disciplines, and as provided for by robust legal and public guarantees.[33]

[31] Similar arguments have been made about the co-productive role of law in techno-scientific innovation, criticizing the image of a 'law lag' and arguing for the constitutive role of law within scientific work itself; see Jasanoff 2007.

[32] On the crucial difference between law and technology in this context of techno-regulation, see (Brownsword 2005; Gutwirth, de Hert and de Sutter 2008; De Vries and van Dijk 2013).

[33] It has been noted that design-based approaches to fundamental rights and freedoms raise concerns about lack of democratic legitimization and the unambiguous self-enforcing character of 'code as law' leaving no room for deliberation (Hildebrandt and Koops 2007, 2010).

Design practices also provide opportunities for a co-productive role of law within techno-scientific innovation processes. This can be captured by the notion of '*right* engineering', which implies the learning of important lessons from legally relevant fields. These lessons can be derived from case law, pertaining to the crucial concepts to be assessed in PIA or DPIA such as risk, probability and harm, but also pertaining to the quality of the articulation processes themselves (van Dijk, Gellert and Rommetveit 2016).[34] Other lessons might be learnt from legal approaches to fields like human rights impact assessment or environmental impact assessment, thus broadening the scope of privacy in relation to other human rights such as data protection, discrimination and dignity on the one hand, and to sustainable technology development on the other.

5.2. A public and civic freedom

As seen in Section 2, civil society actors have engaged in the historical developments related to PETs, supporting their implementation. They also reclaimed participation in frameworks for privacy protection, reaffirming a decisive role for democratic institutions and human rights against threats of 'unaccountable' surveillance. In our peer consultation we contacted representatives of civil rights organisations and inquired about recent developments in the privacy-design field. One peer is, in principle, also positive towards privacy-design processes if implemented in 'honest' ways. At the same time, she strongly argues the need to look at the whole regulatory, economic and political situation, because the current focus on the GDPR could detract attention from the expanding role of surveillance practices and technologies in a number of areas. Thus the peer asserts that one 'should not just focus on the GDPR and should also address other laws that restrict freedoms'.

The peer also sees problems in the growing reliance on PIA and PbD with the argument of increased 'efficiency', often also raised in support of privatising public services. She remarks that in the Netherlands, the emergence of public-private partnerships holding tasks related to services of general interest (for instance in the health and insurance sector) that process vast amounts of personal data, marks a worrying trend of a fast-emerging surveillance economy. The protection of fundamental rights may here be regarded as 'an "obstacle"' to be overcome as soon as a new opportunity for the economy arises. She believes that the use of DPIA and DPbD can here play an instrumental role, in serving as 'an excuse for innovation' and, when deployed by companies, to further the 'privatisation' of fundamental rights and

[34] See also De Hert 2012.

freedoms. These tools can also serve for avoiding ‘hopes and concerns’ being raised from public opposition, thus deflecting and discarding them:

> Peer (civil rights organisation): ‘We do a PIA so it is okay’. It is used as a palliative to make it impossible for people opposing, to raise issues that certain developments infringe fundamental rights. (...) Our living base is regarded as a market commodity and not as a fundamental freedom. It is changed into a risk dimension: stealing the rights of citizens in change for risk management.

A lack of checks on these processes, and on their focus, also worries her:

> Peer (civil rights organisation): no one opposes them and no one checks the quality of the process. Politicians have no notice of the contents. A PIA should start with honesty. The focus should not be on mere compliance.

In her view, governments should force companies to provide adequate information on these processes and laments that in fields such as the IoT or smart energy meters the current level of general information released to users is ‘very poor and simplified’.

5.2.1. Towards ‘honest’ design: avoiding blue-washing and public palliatives

In the account just presented, DPIA and DPbD, introduced as compliance instruments to personal data protection legislation need to be situated within a larger constellation of actors and broader articulations of privacy and personal data protection as civil and political rights and freedoms and as important social values. Salient arguments and sources of justification for their centrality in western democratic societies come from the 1960s and 70s civil rights movements (cf. Bennett 2008; Davies 1998; Clarke 2009, etc.). These rights have also been forcefully articulated by ‘privacy advocates’ (Bennett 2008), i.e., privacy- and fundamental rights lawyers and activists, as demands based on the general interest, to be upheld and protected by governments.

Here important limits and tensions can be discerned about what the practices currently involved in the operationalisation of DPIA and PbD can do, especially in a broader regulatory context in which part of the competence of dealing with privacy and other fundamental rights and freedoms is delegated to companies acting independently or within public-private partnerships. This is strongly formulated in the notion of DPIA as ‘a public palliative’ when these practices thwart public mobilisation around privacy issues. Several such public protests have proved to be quite effective in influencing future technology designs. In this sense they also mediate between the dissatisfaction of end users and expert decision-makers. The obstruction of mobilisation raises questions about the justification for introducing these tools, bearing in mind that addressing these publicly voiced concerns was a historical driving force behind developing PIA (Clarke 2009).

An important question is whether these tools could further the protection of privacy, or whether they could actually make things worse. This might be the case when they function as tick-box exercises focused on achieving mere compliance, without the possibility to oppose and without real substantial or procedural checks on the process. In the worst case, such practices might contribute to a phenomenon we could call '*blue-washing*', which similarly to 'green-washing', entails that they allow an organization to paint a picture of itself as more privacy-friendly than actually is the case.[35]

In an early discussion of PETs, Burkert (1998) already stated that such design-based approaches have important external limitations, in both narrowing down the broad political concept of privacy from its active participation-oriented elements to a more passive anonymity one, and thus also pre-empting public mobilisation. He points to the need of opening PET design to public participation. Here we get to a second important point: public involvement no longer revolves outside or around, but inside these spaces and processes of ICT design.

6. Conclusion: 'privacy by network', limits, tensions and lessons in re-designing privacy

> This is an issue that's much wider than even legal or deeper or more fundamental than legal (…) Going even deeper which is our attitudes, our philosophical underpinning of how do we see with increased technology, increased autonomy on the individual sometimes by nature of technology, generally speaking, how do we redress the balance between the individual and the system? (Peer Quantified Self, CANDID consultation 2017)

[35] The color blue here pertains to privacy as one of the first-generation human rights as civic and political freedoms often called blue rights. This is in contrast with second-generation economic, social and cultural rights (red rights) and third-generation environmental and other rights (green rights).

This article has focused on the design of privacy and personal data protection safeguards into smart artefacts, smart infrastructures and smart cities. We have sketched a short history of different but complementary approaches to realise this, such as Privacy Enhancing Technologies (PETs), Privacy by Design (PbD), Data Protection by Design (DPbD) and Privacy Engineering (PE). We have observed the formation of a techno-epistemic network around designing privacy, over time gathering an array of actors from different practices including regulation, technology development, software engineering, standardisation, organizational management, risk assessment, business entrepreneuring, digital security, consultancy and academia. There have been efforts to stabilise the idea through networking around methodological frameworks such as guidelines, impact assessment templates, design strategies and standardisation. The debate around privacy and data protection in design saw these notions circulating throughout the expansive network of these practices, being articulated differently at each site, where they operate through different concepts, implementing tools and (techno-)epistemological bases.

We can distinguish three different levels at which networking efforts have become manifested: the individual, the organizational, and the infrastructural. In the evolution of the techno-epistemic network we have observed how certain actors have gradually become aligned, while others become unaligned. First, we have observed a focus on protecting the privacy of the individual. This includes the possibility for individuals themselves - directly and autonomously - to engage in information processes of identity disclosure by means of PETs, but also of other types of self-defence technologies. Such a perspective corresponds to an articulation of privacy of which the legal counterpart would be the right to informational self-determination (see section 4.1). Second, data protection legislation moves privacy-design solutions away from the individual level and centers on the organization as the unit for achieving effective privacy protection. The regulatory counterpart of this privacy articulation is the legal right to personal data protection provided by data controllers (see section 4.2). The scope of data protection legislation however, does not directly address the manufacturers of data processing technologies and software developers. These technology producers become involved when we move to the third, infrastructural level. Here multiple stakeholders in the ICT chain gather in standardisation exercises that are used to expand the design dimension of privacy beyond single devices – thus beyond single organisations (see section 4.4). This expansion of design requirements throughout the stakeholder chain transversalises the notion of privacy to reach across, and align the different actors and levels of privacy articulation.[36]

Here we can introduce the notion of "privacy by network" as a result of our study, which can be added to the three other privacy-design orientations mentioned in section 2: privacy by architecture, privacy by policy and privacy by interaction. The notion of privacy by network, by contrast, does not describe an approach oriented towards building privacy friendly ICTs, but rather highlights a certain predicament of the networked and distributed efforts to design privacy and data protection. The ambition of having privacy and personal data protection designed into complex ICT infrastructures that have to be 'smart', interoperable and highly interconnected, come with the need of strategically aligning many sectors and actors around specific design frameworks. Here, different articulations of privacy according to the specific vocabularies and procedures of organizational and engineering practices become linked. This occurs through increasing networking and coordination efforts within multi-stakeholder and co-regulatory fora[37], standardisation platforms for achieving sociotechnological interoperability, and public private partnerships on smart environments and cities[38]. In this sense, 'privacy by network' is crucially linked to the notion of the 'network society' in which networked ICT infrastructure is fundamentally linked to hybrid organizational (economic, regulatory) forms based on social networks (Castells 2010)[39].

Privacy here becomes a normative transversal. On the one hand, it has to be built along the smart digital infrastructure of the networked society (like the IoT, smart grids, smart cities), following the technological roll-out of computing systems that are becoming more and more 'ubiquitous', 'pervasive' and 'hyperconnected'. On the other hand, privacy starts to also permeate and align the efforts of the practices and disciplines that have become mobilised to co-produce responsible ICT innovation. In such a process privacy becomes itself 're-engineered'. In the example of the IoT for instance, standardised privacy-design had to cross-cut different technical components of the system to make them interact, while allowing the coordination of efforts of different ICT manufacturers, data controllers, privacy engineers and organizational risk managers (see section 4.4). There is an important role for networkers (often with hybrid affiliations) within these socio-technical processes, who position themselves

[36] The chain perspective is also relevant for understanding the interdependencies of data processing across multiple stakeholders, which can give rise to systemic privacy risks at the level of the broader ICT ecosystem.

[37] Like those involved in developing DPIA templates for RFID and smart metering technologies.

[38] See sections 2 and 4.4.

[39] A second source is Actor Network Theory (Callon 1986), (Latour 1999).

between leading institutions. They endeavor to set up specific methodological frameworks for privacy-design as ‘obligatory passage points’ for these broader networks.[40] These are presented as solutions to the concerns of multiple public and private actors, such as addressing the ‘law lag’ problem and favoring free flow of data in making the digital single market (for regulators), building consumer trust (for companies), standardising and operationalising the privacy-design conceptions (for organizations and engineers), etc. Different knowledge bases thereby become mobilised and linked to operationalise the notions of PbD, DPbD and DPIA in the process of meeting high infrastructural ambitions. Within this setting, privacy-design functions as a cross-cutting and stabilising promise.

Different tensions can be observed here: those between various levels and practices within the techno-epistemic network and those that become apparent by extending our look to other practices engaged in PbD and DPbD (e.g, by legal and civic actors), which are currently situated outside, or at the margins of privacy by network activities.

A first tension pertains to the *distributed responsibility* within the network. In the introduction, we pointed at an increasing delegation of part of the responsibility for the (privacy) governance of information technologies from public institutions to (public and private) data-controlling organisations. However, this move overlooks important aspects. For instance, whereas from the legal viewpoint, the controller is the entity that can be held liable, brought to court and made to respond *de jure* to allegations of breaches to the rights of data subjects, responsibility becomes *de facto* distributed and decentralised. Part of the responsibility starts moving towards other practices and sites in the network like privacy engineering and standardisation bodies with ensuing transfer of the concrete task to protect rights.[41] There is therefore a *lacuna*, in the GDPR as well as in the theories and practices intended to follow up on the requirements of DPbD, pertaining to where to place responsibility.[42]

A second problem pertains to the existence of a *gap between law and engineering*. We have learnt from peers that there are struggles at the operational level to meet the high-level policy expectations of privacy-design, since legal principles cannot readily

[40] For this notion, see Callon 1986.

[41] Some have argued that this hybrid innovation governance situation requires a shift from individual role responsibility to ‘collective co-responsibility’ for the innovation process, partly through such ‘responsibilisation’ methods like standardization, certification and codes of conduct that go beyond the limits of positive law (von Schomberg 2011).

[42] Beyond responsibility (performance of roles) lies accountability, in the sense of the requirement to give an account to the public and/or regulators of how a certain role has been carried out and conforms to legal and ethical requirements (Raab 2012). The ability of distributed responsibility-holders in the privacy-design network to give such accounts would be in some doubt.

be translated into engineering requirements. In legal practices, these principles are abstract, open-ended and have different possible interpretations, whereas engineering practices require unambiguous meanings and formal definitions of design concepts. The translation into code seems often to be possible only through mediating concepts that address the work of managers of these design processes, *e.g.*, as a range of different 'privacy design strategies', or in terms of 'co-creation' principles based on managing customer relations. We have argued that the nature of privacy changes at the design table, where it is not articulated as a fundamental right, but according to very different vocabularies as a protection goal for design, a formal definition for technical specification, or a transversal infrastructural concern. The term stays as a main signifier but the attributed meanings vary. Thus, rather than a metamorphosis or transformation of rights in design we observe a kind of rupture.

This point was strengthened as we extended our peer consultations towards jurists. Here, we have seen that both judges, human rights and privacy scholars point to decisive limits in terms of how far law, in its various aspects, can and should go in order to accommodate the needs and requirements of design-based solutions.[43] This poses the question how jurists could engage with design and engineering in better ways. This was one aspect of the notion of *'right engineering'*, pointing to learning lessons from legally relevant fields on how to increase guarantees on the quality and procedures of privacy articulations within design processes, when we take the notion of privacy as a fundamental right more seriously.

A third type of tension pertains to the space for user engagement and to participation of publics to processes of ICT design. We have observed strong standardisation efforts where co-creation is organised around consumer trust issues to include 'transversal values' for interoperability and standardisation. However, the margins for co-creation with users are restrained by arguments about systemic complexity and technological functionality that engineers must address and the infrastructure has to satisfy. The scaling up to make smart technologies produced by multiple organizations interoperable within larger ICT interconnected infrastructures (IoT, smart grids) serves the need for making new Europe-wide or global markets. It however also leads to network exclusions and to vulnerabilities at the lower scales (i.e. at local levels, with data subjects and rights holders, publics, etc). Privacy and data protection (by design) in this context seem to correspond with the need for external 'legitimation' of current technology-driven visions underlying the digital economy. This overstretching of scalability in large infrastructural network

[43] On crossing this 'Rubicon' between law and engineering in privacy design, see Rommetveit, Tanas and van Dijk (forthcoming 2018).

alignments thus leads to frictions that cast fundamental questions about rights' engineering and privacy by network in a different light, namely one pertaining to the (right) scales and (right) sites for the articulation of rights and freedoms and the requirements of engineering.

Lastly, in extending towards publics, important limits need also to be recognised about the role and promises of such design-based practices at the intersection of ICT innovation governance, new economic opportunities from the digital market and the threats of un-checked and unaccountable surveillance. We have seen that design exercises often focus on mere compliance, which has nevertheless the potential of having pre-emptive effects on *public mobilisation* ('public palliatives'), whereas such mobilisation has already proven to be an effective alternative avenue for obtaining privacy protection. In the worst case, they might even allow organizations to portray themselves in a more privacy-friendly light than is factually justified ('blue washing'). These developments, raise questions about the reasons for introducing such design-based approaches in the first place, namely to address publicly voiced privacy concerns and to mitigate data processing powers that large organizations increasingly wield over individuals. Privacy is here taken as a political and civic freedom faced with the threats posed by the new surveillance economy. This brings us back to where this article started: describing the waves of re-engineering the concept of privacy. It reminds us of situating these design-based approaches in a broader context of unbalanced societal power relationships, in the light of their justification, and in order to attain 'right' insights in both their strengths and limitations.

Acknowledgements

This work was supported by the European Commission funded Project CANDID – Checking Assumptions and promoting responsibility in smart Development – EU Horizon 2020 project, under [Grant no—732561] and by the Research Foundation Flanders (FWO). Belgium. We wish to thank Katja de Vries for her consultations at the start of the research process and Dr. Antti Silvast for his instructive comments on an earlier version of this text.

References

Agre, P. E., and M. Rotenberg. 1998. *Technology and privacy: the new landscape*. Cambridge, MA: MIT Press.

Article 29 Working Party. 2010. *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*. Brussels.

Article 29 Working Party. 2014. *Opinion 8/2014 on the Recent Developments on the Internet of Things*. Brussels.

Bellotti, V., and A. Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer Supported Cooperative Work* (ECSCW 93), 77-92. Milano: Kluwer.

Bennett, C.J., and M. Howlett. 1992. The lessons of learning: Reconciling theories of policy learning and policy change, *Policy Sciences* 25: 275 - 94.

Bennett, C., and C. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Bennett, C. 2008. *The Privacy Advocates. Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Beslay, L., and A.C. Lacoste. 2012. Double-take: getting to the RFID PIA framework. In *Privacy impact assessment,* ed. D. Wright and P. De Hert, 347– 62. Dordrecht: Springer.

Brownsword, R. 2005. Code, control, and choice: Why east is east and west is west. *Legal Studies* 25(1): 1–21.

Burkert H. 1998. Privacy-Enhancing Technologies: Typology, Critique, Vision. In *Technology and privacy: the new landscape,* ed. P.E. Agre and M. Rotenberg, 125-42. Cambridge, MA: MIT Press.

Bygrave, L. 2017. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review* 4 (2): 105 – 20.

Callon, M. 1986. Elements of a sociology of translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In *Power, Action and Belief: A New Sociology of Knowledge?* ed. J. Law, 196-233. London: Routledge.

Castells, M. 2010. *The Rise of The Network Society*. Vol. 1 of *The Information Age, Economy, Society and Culture,* (2nd edition with a new preface). Oxford: Wiley-Blackwell.

Cavoukian, A. 2006. *Creation of a Global Privacy Standard*, November 2006.

Cavoukian, A. 2009. *Privacy by design: The 7 foundational principles*. Inf. Priv. Comm. Ont. Can.

Cavoukian, A., S. Shapiro and R.J. Cronk. 2014. *Privacy Engineering: Proactively Embedding Privacy, by Design*. Inf. Priv. Comm. Ont. Can.

Chaum, D. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2): 84–88.

Clarke, R. 2009. Privacy impact assessment: its origins and development. *Comput Law Secur Rev*, *25*: 123–35.

Cranor, L., and N. Sadeh. 2013. Privacy Engineering Emerges as a Hot New Career. *IEEE Potentials* 32(6): 7-9.

Danezis, G., J. Domingo-Ferrer, M. Hansen, J-H Hoepman, D. Le Métayer, R. Tirtea and S. Schiffner. 2014. *Privacy and Data Protection by Design – From Policy to Engineering*. ENISA.

Davies S. G. 1998. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In *Technology and privacy: the new landscape,* ed. PE Agre and M. Rotenberg, 143- 66 Cambridge, MA: The MIT Press:

De Hert P. 2012. A human rights perspective on privacy and data protection impact assessments. In *Privacy impact assessment*, ed. D. Wright and P. De Hert, 33–76. Dordrecht: Springer.

De Vries E., and N. Van Dijk. 2013. A bump in the road. Ruling out law from technology. In *Law as code meets law as literature*, ed. M. Hildebrandt and J. Gakeer, 89-121. Dordrecht: Springer.

Doty N., and D. K. Mulligan. 2013. Internet Multistakeholder Processes And Techno-Policy Standards, Initial Reflections On Privacy at W3C*, Jour. on Telecomm. & High Tech* 11: 135- 82.

Finneran Dennedy M.F., J. Fox, and T.R. Finneran. 2014. *A Privacy Engineering Lifecycle Methodology The Privacy Engineer's Manifesto - Getting from Policy to Code to QA to Value*. Apress.

Friedman, B. 1996. Value-sensitive design. *Interactions* 3: 16–23.

Funtowicz, S., and J.R. Ravetz. 1993. Science for the post-normal age. *Futures* 25: 735 - 55.

Gonzalez Fuster, G. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Dordrecht: Springer.

Gürses, S., C. Troncoso, and C. Diaz. 2015. *Engineering privacy by Design Reloaded*. Amsterdam Privacy Conference, October 2015, hosted at: https://iapp.org/media/pdf/resource_center/Engineering-PbD-Reloaded.pdf

Gürses, S., and J.M. Del Álamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security & Privacy* 14(2): 40 - 46.

Gürses, S., and J. van Hoboken. 2017. Privacy After the Agile Turn. In *Handbook of Consumer Privacy,* ed. J. Polonetsky, O. Tene and E. Selinger, 579 - 98. Cambridge: Cambridge University Press.

Gutwirth, S. 2015. Providing the missing link: law after Latour's passage. In *Latour and the passage of law,* ed. K. McGee, 122 – 59. Edinburgh: University Press.

Gutwirth, S., and P. De Hert. 2007. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In *Privacy and the Criminal Law,* ed. E. Claes, A. Duff, and S. Gutwirth, 61 - 04. Antwerpen-Oxford: Intersentia.

Gutwirth, S., P. De Hert, and L. De Sutter. 2008. The trouble with technology regulation from a legal perspective. Why Lessig's optimal mix will not work. In *Regulating Technologies*, ed. R. Brownsword, K. Yeung, 193 – 18. Oxford: Hart Publishers.

Haas, P. M. 1992. Knowledge, Power, and International Policy Coordination. *International Organization* 46(1): 1 - 35.

Harrison, J. 2013. Establishing a meaningful human rights due diligence process for corporations: learning from experience of human rights impact assessment. *Impact Assessment and Project Appraisal*, 31(2): 107- 17.

Hes, R., and J. Borking. 2000. *Privacy-enhancing technologies: the path to anonymity,* (revised edition). Registratiekamer and Information and Privacy Commissioner of Ontario, Netherlands.

Hildebrandt, M., and B. J. Koops. 2010. The challenges of ambient law and legal protection in the profiling era. *The Modern Law Review* 73(3): 428 – 60.

Hildebrandt, M. 2011. Legal Protection by Design. *Legisprudence* 5: 223– 48.

Hoepman, J.H. 2014. Privacy design strategies. In *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco. Proceedings*: 446 – 59.

Jasanoff, S. 2007. Making Order: Law and Science in Action. In *The Handbook of Science and Technology Studies,* ed. E.J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman, 761-786. MIT Press.

Kamara, I. 2017. Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. In *European Journal of Law and Technology,* 8(1).

Koops, B. J., and R. Leenes. 2014. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, 28 (2): 159 - 71.

Langheinrich, M. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing*. Springer: 273 – 91.

Latour, B. 1999. *Pandora's Hope*. Cambridge, Mass.: Harvard University Press.

Leenes, R. 2011. Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology. *Legisprudence* 5(2): 143 - 69.

Lessig, L. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Murphy, T., and N. Whitty. 2009. Is human rights prepared? Risk, rights and public health emergencies. *Med Law Rev,* 17: 219 – 44.

Notario, N., A. Crespo, Y.S. Martín, J.M. del Álamo, D. Le Métayer, T. Antignac, A. Kung, I. Kroener, and D. Wright. 2015. *PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology*. IEEE CS Security and Privacy Workshops: 151- 58.

Prahalad, C.K., and V. Ramaswamy. 2004. Co-creating unique value with customers. *Strategy & Leadership*. 32 (3): 4 - 9.

Raab, C. 1997. Co-Producing Data Protection. *International Review of Law, Computers & Technology*, 11(1): 11 - 24.

Raab, C. 2012. The Meaning of 'Accountability' in the Information Privacy Context. In *Managing Privacy through Accountability*, ed. D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, H. Postigo, 15 - 32. London: Palgrave Macmillan.

Reidenberg, J.R. 1998. Lex informatica: The formulation of information policy rules through technology. *Texas Law Review* 76(3): 553–584.

Spiekermann, S., and L.F. Cranor. 2009. Engineering Privacy. *IEEE Trans. Software Eng* 35(1): 67 – 82.

Thompson, C. 2013. *Good Science: The Ethical Choreography of Stem Cell Research*. Cambridge, Mass./London: MIT Press.

van Dijk, N. 2015. The Life and Deaths of a Dispute. An Inquiry into Matters of Law. In *Latour and the passage of law*, ed. K. McGee, 122 – 59. Edinburgh: University Press.

van Dijk, N., and K. Rommetveit. 2015. *A Risk to a Right? Cross-Cutting Lessons for Data Protection Impact Assessments*, EPINET Project (FP 7) Policy Report to European Commission (EC). 2015, at: http://epinet.no/content/cross-cutting-perspectives#collapse-1

van Dijk, N., R. Gellert, and K. Rommetveit. 2016. A risk to a right? Beyond data protection risk assessments, *Computer Law & Security Review: The International Journal of Technology Law and Practice*. 32: 286-06.

van Gestel R., and H.W. Micklitz. 2013. European Integration through standardisation: how judicial review is breaking down the club house of private standardisation bodies. *Common Market Law Review*. 50: 145- 82.

Von Schomberg, R. 2011. *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. European Union, Luxembourg.

Yee, G.O.M. 2011. *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, 1st IGI Publishing Hershey, PA, USA.

Rommetveit, K., N. van Dijk, K. Gunnarsdóttir, K. O'Riordan, S. Gutwirth, R. Strand, and B. Wynne, (forthcoming 2018). Working responsibly across boundaries? Some practical and theoretical lessons. In *Handbook of responsible Innovation*, ed. R. von Schomberg. Edgar Elgar Publishers.

Rommetveit, K., A. Tanas, N. van Dijk, (forthcoming 2018). Data protection by design: promises and perils in crossing the Rubicon between law and engineering. In *Proceedings IFIP summer school 2017 on Privacy and Identity Management,* ed. M. Hansen, E. Kosta, I. N. Fovino, S. Fischer-Hübner. Springer.