Political Studies

Seeing Like a Citizen: Understanding Public Views of Biometrics

Journal:	*Political Studies*
Manuscript ID	POST-02-17-0044
Manuscript Type:	Article
Keywords:	Biometrics, political discourse analysis, q-method, digital citizenship

Abstract:	Despite its controversial history and the significant diffusion of biometrics from institutional settings such as border control and policing, to everyday use in commerce and personal devices, biometrics is now being re-positioned as a neutral means to safeguard identity in the digital world. Given this proliferation of uses we argue that understanding perceptions of biometrics amongst ordinary citizens is necessary and long overdue. Situating our analysis in the wider context of the views of governmental and biometric industry experts, we deploy Q-methodology in combination with political discourse analysis to examine the range of positions that have crystallized in ordinary discourse on issues arising from the use of biometrics for identification. Our analysis analysis uncovers four distinctive configurations that put into question a simplistic trade-off between security and privacy that dominates government and industry discourse, and underlines the importance of going beyond a narrow view of technology 'users' to understand the political and social concerns that arise with and shape the uses of technology in contemporary society

Seeing like a citizen:

Understanding public views of biometrics[1]

Introduction

In 2004, Giorgio Agamben (2004), a renowned political philosopher, cancelled an academic visit to New York, refusing to go through US border-control procedures involving extensive use of biometrics. More than a decade later, refusing to travel does not protect one from being biometrically identified; the use of biometrics now extends far beyond policing and border control into multiple areas of everyday life. More physiological features are being used as biometric identifiers to identify people across physical and digital contexts. Fingerprints and retina scans are incorporated into personal devices such as laptops and smart phones, and their use is being explored in the banking industry. Face recognition is extensively employed in on-line social networks (Authors 2017); and new forms of biometrics, such as gait and brainwave analysis, are used in consumer electronics to help cultivate healthier lifestyles.

In this article, we examine public views of the use of biometrics for identity management. Our aim is to bring the voices of the lay public back into a debate that has been dominated by security experts and technical policy reports that take little notice of public views. We seek to capture and analyse citizen reflection on this complex policy issue, and to make visible the distinct patterns into which ordinary views of the use of biometrics crystallise (Danielson et al., 2012). We focus on the

[1] Support for this research was provided by the EPSRC (grant EP/J005037/1).

growing use of biometrics in everyday contexts, as well as in institutional settings (e.g. border control, policing). As these new technologies are rapidly altering the economy of rights and duties in society, the need for direct engagement with citizens increases (Callon et al., 2009). We use Q-methodology in conjunction with political discourse analysis (PDA) to capture the full range of viewpoints on the varied uses of biometrics in public life. This combination of methods allows us to provide a unique perspective on public views of biometrics. In contrast to survey methods, we do not seek to collect and aggregate individual views on biometrics. Rather, the combination of discourse analysis and Q method allows us to capture specific subject positions (Foucault) drawn from the available range of discourses on a topic, with which individuals can identify. Thus, using Q method we analyse both the breadth of debate on an issue (concourse), and the distribution of preferences and the distinctive patterns in which they coagulate, situated within the context of the wider discourses generated by actors such as governments, policy-making and civil society organisations. This approach further enables us to move beyond the technological aspects of biometrics to broader concerns over digital citizenship in a context in which citizens as right-bearers are affected by an ever-more widespread use of biometrics in public and private life.

Our approach significantly departs from existing academic research in this domain. The post 9/11 rapid introduction of biometrics into border control settings linked them to controversial efforts to restrict civic rights in Western democracies in the light of terrorist threats (Bigo, 2005; Magnet, 2011; Muller, 2004), and more recently, in the context of immigration policy. As a result, debate has centred on the trade-off between the need for security and the right to privacy. Despite the fact that even in democratic societies security often trumps privacy, remarkably little effort has

been put into challenging the usefulness of these trade-offs for structuring debate and policy-making. Concentration on input from security experts, in the wake of an almost complete lack of research on the views of ordinary citizens (Fischer, 2009; Callon et al., 2009, p.9) and on individual views on privacy (e.g. Madden and Rainie, 2015), has led to a lack of research that situates citizens' views on the uses of biometrics in wider contexts that would foster more active engagement with the lay public in policy making (Omand, 2010, p.73). Similarly, a large number of industry-led studies on biometrics analyse public opinion on biometrics (IBIA), focuses largely on the user-acceptance of specific technologies, without seeking to understand the impact of technology transfers from a security to an everyday context (see Authors, 2017).

In our view, these problems can be attributed to the implicit assumption, by both proponents and critics of biometrics, that the public is not sufficiently informed to negotiate conflicting demands arising from the impact of technological change on their lives (Lanier, 2014). By contrast, we start from the presupposition that citizens are capable of expressing nuanced views that allow for sophisticated engagement with the range of issues at stake here. In this respect our work falls within a wider turn to the 'everyday' and a focus on 'vernacular' constructions of security (Vaughan-Williams and Stevens, 2015), whilst seeking also to go beyond a securitization frame. Our study makes visible how citizens understand biometrics and their uses across a range of situations, without reducing them to zero-sum trade-offs between security and privacy, on the one hand, or treating them as isolated technologies on the other.

Our approach is further distinctive in the emphasis it places on how 'biometrics' is understood and given meaning in and through available discourses that shape what biometric technologies may legitimately be used for, what the role of the

state and the private sector in the use and promotion of biometrics is, and what the legitimate scope for contestation around theses uses are. In this respect, our approach resonates strongly with work on the co-production of technologies and their embedding in social identities, institutions and discourses (Jasanoff, 2004). In seeking to understand citizens' views on the uses of biometrics we need to know how biometrics are represented in wider institutional discourses, and what 'specific assumptions, judgments, contentions, dispositions, and capabilities' these discourses embody (Dryzek and Niemeyer, 2008, pp. 481-2). Drawing on political discourse analysis (PDA) (author 2009), we start from the supposition that discourses – understood as the meanings and practices associated with a given domain that together denote a particular way of apprehending the world, 'enabling those who subscribe to it to interpret bits of information and put them together into coherent stories' (Dryzek, 1997, p.8) - both enable and constrain thought, speech and action - what we say as well as what we do (Author, 2000). They are constitutive of horizons of meaning, and offer positions with which individuals and groups may identify, and that may be contested (Author, 2012).

Our findings indicate a broad spectrum of citizen views on biometrics that goes beyond the aforementioned security vs. privacy trade-off. Views crystallise into four nuanced subject positions, reflecting awareness of the technological possibilities of biometrics but also of the political issues at stake in their deployment in various contexts. Each of these positions draws on wider discursive representations of biometrics in public discourse - analysed in the next section - but represent a distinctive perspective crystallised around a specific combination of concerns. In this respect, our work contributes to policy analysis (March and Olsen 1995, p.6; Fischer, 2009, p.248) that emphasizes the importance of discursive practices, in addition to

more formal rules, in shaping the frameworks within which citizens, experts and officials act.

Discursive representations of biometrics

The documentation of individual identity has historically been closely linked to practices associated with citizenship, and continues to be so. Governments use a variety of bureaucratic, obligatory practices to turn their populations into 'legible people' (Scott, 1998; Noiriel, 2001) However, the establishment of such 'regimes of representation' (Caplan & Torpey, 2001, p.8) is not straightforward. 'Identity' is difficult to stabilise even in the most regimented systems of documentation (Caplan, 2001, p.51). It requires a rigorous set of bureaucratic procedures to record and maintain identity-related information. At the same time, it is political as it constitutes people as political subjects with specific rights and duties, and involves moments of resistance from individuals and social groups, for instance, contesting the specific categories of information, included in or omitted from the official documentation of identity (LSE, 2005; Molokotos-Liederman, 2007).

With industry, governments engage in practices that govern the complex ways in which individuals and groups behave their producing and consuming activities (Tully, 2008 II, 3; Author, 2014). From a governmental perspective, biometrics are portrayed as technological solutions that aid the streamlining of mechanisms for collecting, codifying and verifying citizen identity (Mansfield, 2003; Home Office/UK Border Agency, 2010; Home Office, 2002; IPSC, 2006; Misuraca and Lusoli, 2010). The technological excellence of biometrics constitutes the core argument in favour of their use in a growing number of government activities ranging from border control to the collection of social benefits (Magnet 2011; Liberty Global,

2012). Here biometric technologies are used to stabilize personal identity in two ways: as a means of accurately verifying subjective claims of identity, and as a means to eliminate discrepancies between identity tokens, used as proofs of such claims, and government apparatuses that curates formal identification systems. This is achieved by tracing individual identity back to physiological signs (fingerprints, iris, voice, and so on) through a process that transforms the body into an identity token against which subjective claims of identity can be read (Van der Ploeg, 1999). Focussing identification procedures on the human body allows individuals to be identified without the need for written documents such as passports and identity cards, and is argued to safeguard formal identification systems from human error as it automates every stage of the process. As the IBIA (2013, p.1) argues: 'What makes modern biometric use highly effective is technology that enables precise measurement coupled with computational power that allows measurements to be … converted to unique and secure identifiers that are easily used to determine and protect a person's true identity.' To this end, biometrics promise to establish procedures that can irrevocably identify citizens, granting them access to their rights and preventing them from claiming benefits to which they are not entitled.

Representations of biometrics in industry discourses (BI, 2013; IBIA, 2013 & the Joint Research Centre EU) also emphasize the infallibility of these technologies, portraying biometrics as the endpoint of a long evolutionary path of identification technologies. An IBIA (2013, 1) white paper on biometrics exemplifies this trend: 'Contrary to popular belief, biometrics is not new … Man has used biometrics throughout recorded history to uniquely identify individuals, starting with the first handprint "signatures" of authors of paintings on cave walls over 30,000 years ago.' Older practices (i.e. using thumbprints) are retrospectively recast as biometrics; a

Homeland Security & Defense Business Council (2011) document similarly starts with a historical account of the use of biometrics to prevent fraud in 1882. This strategy seeks to alleviate fears that more advanced technological solutions will alter underlying social practices; biometrics are portrayed as 'merely' automating historical forms of identification. The biometrics industry further annexes other images to this evolutionary view: new technologies are presented as 'neutral,' able to counter threats in the digital world and even to empower users (Ernst & Young, 2011; Accenture, 2006). Driven by the need for convenience, the idea of biometrics as a value-neutral tool underwrites the diffusion of biometrics into contexts far beyond border control. Biometrics are presented as the 'natural' solution to the trouble people have with remembering multiple passwords.

The use of technology that purports to read the truth from a body is not simply a bureaucratic choice. It is a political issue of some significance. This is why academic research has been very critical of governmental policies (Agamben, 1998; Aradau, 2008). Transforming the body into a series of digital signs that can be combined with other data in order to profile the population, changes our bio-political relationship with the state (Agamben, 2004; Fisher, 2015). Hence, it is argued that biometrics compress complex social relationships, reducing identity to a series of algorithms that can irrevocably identify a person without having to rely on cultural cues, deemed inefficient and possibly erroneous (Muller, 2004). As bodies become 'biometrifiable' citizenship is increasingly stripped of its symbolic and cultural attributes (Magnet, 2011, p.280), leaving us with a purely instrumental conception of what it means to belong to a specific state and its allocated territory. The politics of population movements is gradually transformed into a bureaucratic exercise (Amoore, 2006; Bigo, 1998), and techniques initially reserved for 'deviant' social groups, such

as fingerprinting, are now migrated to larger parts of the population, becoming normal practice (Jumb et al., 2015).

Beyond governance as control

These approaches and critiques fall short in two important respects. First, focussing on biometrics exclusively as governmental technology to control populations offers limited scope to make sense of the proliferation of biometrics in everyday life. It specifically fails to address the incorporation of biometrics into consumer devices and on-line media (Authors 2017), which is at the root of growing societal excitement about new technologies and the new forms of social and political interaction they foster (Bennett and Segerberg, 2013). The focus of existing research on identity as a formal transaction between citizens and the state, where biometrics are primarily examined in contexts such as borders and where safety is of primary importance (Aas, 2006, p.144), do not capture these new developments. However, it is precisely such uses that require scrutiny regarding their repercussions for citizenship as they expand the use of biometrics to everyday contexts. They raise significant issues concerning the boundaries between politics and bureaucracy, the actors to be held accountable when collecting biometric information and the economy of rights and duties shaping citizenship in digital environments.

This brings us to the second sense in which existing analyses, critical or not, falls short. Arguably more fundamentally, extant work typically rests on a passive view of subjectivity: citizens are viewed as objects of state policy, rather than active participants who are able to consent, contest, and change identity management practices (incorporating all of the ways in which we identify ourselves online and in everyday life). In this we concur with Vaughan-Williams and Stevens (2015) on the

importance of understanding citizens' views in relation to policy rhetoric. Our approach further allows us to see how citizens draw on available discourses and construct a range of clearly discernable positions on biometrics that undercuts the security/privacy dichotomy.

Our approach challenges both the limited focus of the domains in which biometrics are deployed, and the passive view of subjectivity on which it rests. We focus on more recent developments of biometrics, including their use in personal devices (such as phones and laptops) and in commerce (e.g. workplace time-clocks and methods of access), as well as on traditional uses of biometrics. In addition to this wider empirical lens, we also seek to 'bring citizens back in.' Existing user research tends to concentrate narrowly on the usability of specific technologies. (For a critical overview, see IMPRINTS 2014, pp.7-9.) By contrast, we are interested in the views of users as citizens rather than narrowly as general users of commercial products. This leads to an analysis of wider issues associated with biometrics, to consider how citizens understand, respond to and shape their environments, how they view the relation between security and privacy, and what their demands are in terms of accountability and consent, in both commercial and non-commercial contexts.

Hence, our focus is on the ways in which ordinary citizens actively make sense of and challenge the views expressed by dominant authorities, as well as on the need to take these views into consideration in the policy-making process. Combining Q method and PDA allows us to capture empirically the distinctive subject positions articulated by citizens, drawn from these wider discursive representations of biometrics. As noted earlier, in contrast to survey methodologies our analytical focus is on the discursive positions articulated by ordinary citizens against the backdrop of a

horizon of meanings generated by actors such as governments, policy-making and civil society organisations.

Research design and method

Combining Q-method and discourse analysis

Q methodology, first introduced in political science by Dryzek and Berejikian (1993), is now widely used in public administration and policy studies to understand how government policies are perceived by public servants who implement them (Jeffares and Skelcher, 2011), as well as by citizens as their recipients (Willis and Jeffares, 2011). The benefits of the method lay in its logic of abduction (Watts and Stenner, 2005), also shared by PDA (Glynos and Howarth, 2007), which favours the generation of themes by the research subjects rather than the analyst, endeavouring to make visible the primary ways in which themes are 'interconnected or otherwise related by a group of participants' (Brown, 1980 & 1993). This procedure fits well with our emphasis on the discursive representations of biometrics and the need to understand the particular meanings given to biometrics in different contexts and by different actors. To capture the way in which particular meanings are woven together into distinctive positions, we draw on the discourse theoretical account of 'articulation' developed by Laclau and Mouffe. When discursive elements are articulated together, the meanings of all the elements are altered as a result (Laclau & Mouffe, 1985). It follows that views of 'biometrics' will differ depending on the wider discursive contexts of use in which they are inserted. The use of Q methodology helps us to reveal the dominant viewpoints on biometrics as articulated by ordinary citizens in a systematic, holistic fashion (Brown, 1993; Watts and

Stenner, 2012, p.42). This is achieved 'by modelling subjects in terms of their reactions to a set of statements about a given domain' (Dryzek and Berejikian, 1990, p.50). In this way the method enables us to trace the manner in which specific subject positions are crystallized from an available horizon of meanings, revealing the ways citizens collectively make sense of biometrics and their uses.

The use of this combination of methods adds value both to Q methodology and to PDA. The theoretical resources of PDA furnish Q method with a more sophisticated understanding of both the breadth of discussion, and the actors' viewpoints on the topic under discussion. PDA makes visible the fact that the concourse is not simply a given set of discrete statements, but a discursive horizon that shapes and sets limits to what can be done within a given terrain. As noted above, on this account 'biometrics' is not simply a neutral terrain of techniques deployed for the purposes of identity management. How it is understood depends upon the precise meanings attributed to, and practices associated with it, by a wide range of actors, including governments, commercial and civil society organisations. PDA also provides Q method with a theoretically robust understanding of subjectivity. Q method rejects the behaviourist view that subjectivity is something merely mental or inner, unrelated to the world (Watts and Stenner, 2012, p.19). PDA supplements this work with an account of subjectivity as discursively constituted, rather than as given. Drawing on Foucault, we take 'subject position' as incorporating 'both a conceptual repertoire and a location for persons within the structure of rights for those that use that repertoire. As Davies and Harre (1990, p.46) put it,

> Once having taken up a particular position as one's own, a person inevitably sees the world from the vantage point of that position and in terms for the

particular images, metaphors, storylines and concepts which are made relevant within the discursive practice in which they are positioned.

The factors extracted by Q method – the common or shared meanings crystallizing from the analysis – constitute specific subject positions, that is, places from which individuals can speak and act.[2] Conversely, Q method supplements PDA by providing a robust scientific method with which to capture empirically and analyse quantitatively the dominant social viewpoints with which individual can identify.

Research design: establishing the concourse and Q sample

Jeffares and Skelcher summarise the essence of Q methodology as follows: 'each participant in the sample (the P sample) sorts a series of statements (a Q sample) representative of the breadth of debate on an issue (the concourse) into a distribution of preference (a Q sort) from which statistically significant factors are derived and then interpreted' (Jeffares and Skelcher, 2011, p.1253).

The starting point for any Q study is the selection of statements to be ordered by participants. These statements need to be representative of the wider horizon of discourses – the concourse - on the chosen topic of inquiry; Stephenson (1988, p.9) appropriately describes this as the 'cultural heritage' forming 'the fertile soil from which new subjectivity grows'. The concourse reflects the volume of discussion on this topic (Brown, 1986, p.58; Watts and Stenner, 2012, p.34) that may include interviews with relevant participants (Jeffares, 2011, p.1257), focus groups, analysis of academic, media and other texts (Dryzek and Berijikian, 1993). Our concourse is

[2] Watts and Stenner (2012, 42) equates individual Q-sorts with expressions of subject positions. In our view, the factors extracted as a result of the analysis represent subject positions in the sense in which Foucault uses the term.

formed by the available representations of biometrics in institutional discourses, including governmental, industry, civil society and academic discourses – discussed above. We analysed government reports from the Department of Homeland Security, the UK Cabinet Office, the Home Office as well as committees from both Houses, EU commissioned documents and reports, industry promotional material and white papers, think tank reports, civil society reports on surveillance and privacy, press articles and finally academic literature on biometrics, surveillance, identity and privacy (see Appendix A). This allowed us to select statements capturing the specific language in which discourses on biometrics are articulated. The concourse consisted of 170 statements related to various uses of biometrics for digital identification. The next stage consisted in narrowing these statements down into our Q sample.

The use of classification matrices as heuristic devices for selecting statements is well established in Q studies (e.g. Jeffares and Skelcher, 2011; Sullivan, Williams, and Jeffares 2011). We adapted Dryzek and Berejkian's classification scheme, combining the types of argumentative claims made - definitive (concerning the meaning of terms), designative (concerning questions of fact), evaluative (concerning something's worth) or advocative (concerning what should or should not exist) - with the identified discourse elements (1993, 51). The discourse elements identified do not constitute categories defined in *a priori* fashion by the researcher; rather they are themes that emerged from the collected materials. The elements we identified are:

1. **Identity** refers to a focus on the use of the human body for identification. It also covers issues related to the assurance of individual identity through biometric technologies.

2. **Empowerment** captures issues relating to data usage and control of data. It also includes issues relating to the ease of use of biometric technologies, seen as a means to empower citizens.

3. **Security** contains statements on the use of biometrics for border control and policing. Issues revolve mainly around the safety of biometrics as digital records, their ability to irrevocably identify individuals and their effectiveness in battling identity fraud and terrorism.

4. **Accountability** explores the types of actors (e.g. government, industry) that should be held accountable of the various issues of biometrics. The possibility of function creep arising from the collection of biometric data is a key concern.

5. **Surveillance** focuses on the possibility to monitor public spaces without consent as well as the intrusiveness of biometric technologies in work settings and in private activities.

Once the matrix was created all the statements were classified into the various categories through an iterative process. Initially, each researcher classified the statements on her own. Classifications were compared until a consensus was reached. In selecting the 50 statements for the Q sample, we were mindful of obtaining a balance between the plurality of themes and types of argument, and avoiding duplication of meanings and issues.

Research design: the P-sample and sorting

In deciding on the number of participants, we followed the standard guideline of 40-60 participants. Our selection rationale focused on using individuals representing mobile respondents, in tune with current developments in technology, politics and society in general. Our P sample consisted of 60 student respondents, including 30

respondents from UK/EU and Overseas (non-EU) countries each, and an equal gender distribution. [3] For the sorting stage, an on-line tool POETQ, reflecting the card-based process, was used. This facilitated participation and increased responses making the sorting process less time consuming (Jeffares and Skelcher, 2011). Participants raked the 50 statements from +5 (most agree) to -5 (most disagree) using a forced ranked distribution (inverted pyramid shape). On completion of the Q-sorts, the participants were asked to comment on how they ranked the statements especially the ones at +/-5 and +/-4. These explanations contributed to selecting the factor solution but also to interpreting the subject positions represented by each factor.

Factor analysis

The responses (Q-sorts) were correlated and then analysed through a by-person factor analysis that reveals correlated groups of statement preferences. We used PQMethod 2.33 (Schmolck, 2014) to carry out the statistical analysis. Participants with a loading of 0.36 and above were flagged for a varimax rotation to maximize the loading in each factor. The choice of the varimax rotation ensured that the factors selected as the final solution only contained Q-sorts that were highly correlated with each other and

[3] The broad selection of participants also worked against an overly northern-hemisphere focus. As is common practice, respondents were offered an incentive to participate in the study. The Q sort was administered to participants in a PC lab, ensuring completion of the sort under similar conditions. The availability of specific technologies at the time (2013) are not particularly crucial, as the design of the study was not limited to a focus on existing technologies, but rather on the possibilities for empowerment, scrutiny etc. opened up in principle by biometric identification technologies.

that were uncorrelated with the remaining Q-sorts (Brown, 1993). We selected four factors as our final solution as this offered a nuanced view of citizens, favouring a context-driven assessment of the use of biometrics. (In a three factor solution this detail was lost offering instead indications of possible acceptance of biometrics according to circumstances.) All factors had eigenvalues greater than 1.0 and at least one Q sort loaded significantly on the factor. Table 1 presents the factor correlations, the number of Q sorts significantly loading on each factors and the level of variance explained by each factor.

Table 1 [here]

The four factors together explained 47% of the study variance.[4] They were selected as the best solution since they revealed views on the topic which showed how existing dilemmas (wholeheartedly rejecting vs uncritically accepting biometrics) in public discourse were overcome in practice. At this stage the task of the researcher is that of interpretation, of 'understanding the character of these synthesized factors based on the placing of statements' (Jeffares et al, 2011, p.1258). Table 2 below presents the resulting factor arrays: a single Q sort per factor is configured to represent the 'ideal' viewpoint expressed by the particular factor. The statements used to create these 'ideal' Q sorts are those that statistically distinguish the discourse from other factors at the P‹ 0.01 or 99% confidence level.

[4] Anything around 35-40% is considered a sound solution on the basis of common factors (Watts and Stenner, 2012, p.105).

Table 2 [here]

Results – The factors

The analysis of the Q sorts identified four distinctive discursive configurations or subject positions relating to the use of biometrics for managing digital identities. These viewpoints represent particular articulations of the elements present in the existing discursive horizon. Theoretically this reflects the relational conception of meaning underpinning PDA: each element does not have an inherent, essential meaning, but gains its meaning from the way in which it is combined with other elements (Howarth, 2009, p.311). This is particularly clear in our analysis that shows that while each of the four subject positions display a concern with privacy, they significantly diverge on other issues. There is only one statistically significant consensus statement (41) referring to the possibility of linking personal data from various databases through biometric identifiers. This shows a concern with the use of biometric data that is shared across all citizen viewpoints. The participants, depending on their understanding of biometrics, arranged the rest of the statements differently, revealing an interesting variety of views on the uses of biometrics. These views range from the overtly sceptical *Privacy Advocates* (Factor A) who express serious concerns about the use of biometrics for identification to *Casual Adopters* (Factor D) who espouse an easy-going instrumental use of biometrics, treating them as a technological solution to a variety of identity-related issues. Between these two viewpoints, there are *Conservative Techies* (Factor B) and *Safety Champions* (Factor C) who express more nuanced views on biometrics. *Conservative Techies* focus primarily on uses of biometrics that allow them to safeguard their personal devices (e.g. smartphones, laptops) while *Safety Champions* favour uses of biometrics for

access control to secure places. Below we outline each factor, representing a version of views on biometrics. Numbers in parentheses refer to the statements & their weightings.

Factor A: Privacy Advocates

With each new development in biometric technology, users have less control over their data, not knowing when, where and why it is used (31: +4). People can be identified without their consent, and quite often, without their knowledge (42: +4). Remote biometrics, like face and gait recognition (3: +2), intensify this lack of control on behalf of citizens raising concerns about bodily integrity too. Privacy, as we know it, is coming to an end (7: +5, 50: +1). People are caught in a world where nothing is forgotten as personal data can be linked irrevocably to individuals (38: +1). When it comes to the management of digital identities, the body should not be seen as a natural password (4: 0). On the contrary, people should be in control of how their data is collected, stored and used (37: +3). Most importantly, they must have the right to opt-out from services, preventing collection of personal information (1: +3). Intrusive uses like biometric time clocks in industry or face recognition in social media (5: -3, 19: -4) affecting individual freedom (44: +4) should be avoided. To counterbalance state surveillance, citizens need to be more active. They have the right to record police action on their smart phones and to circulate it on social media (32:+1). They should also use any device, such as privacy visors, that protect them from unauthorized identification while in public (30: 0). Finally, government arguments in favour of biometrics for efficiency and convenience need to be carefully scrutinized (35: -5). The promotion of more individualistic models of social life, as all devices

will be bound to their owner, undermines community (14: 0) and paves the way for increased monitoring of the population (28: -3, 26: -3).

Factor B: Conservative Techies

Our bodies are like natural passwords that we all carry with us at all times (4: +5), making biometrics a good alternative to the growing number of identification paraphernalia, such as PINs, that people need to memorise (6; +3). Biometrics seem to be a great way to safeguard personal devices (e.g. mobile phones) from loss or theft (12: +2). Moreover, they can be used in time clocks to allow companies to have better control of their labour force (5: 0). However, people should be wary of the possibility of extensive profiling. It is for this reason that biometrics should not be used in domestic settings (18: -3) since they have the potential to disclose sensitive information about their users' habits. The same applies to the use of face recognition software in mobile devices and social media (43: -3). However, biometrics are still seen as a particularly promising technology for security purposes. They are not infallible, since they involve a range of human decisions (23: +4), but, they do help governments to effectively lock foreign nationals into their identity (28: 0). Given this, citizens should be supportive of instead of jeopardizing biometric technologies by recording police action during demonstrations (32: -3) or altering their facial features with headwear (30: -5). Biometrics are not about state surveillance (45: -3). There is strong legislation against linking personal data from different databases (15: -1) for unrelated purposes. Finally, negative connotations accompanying certain biometrics (e.g. fingerprints) or concerns over community life (14: -5) should not become an obstacle to more efficient applications (8: -4).

Factor C: Safety Champions

Biometrics can be useful as long as personal data is well protected (49: +5). They strengthen safety and are convenient. Their use should be embraced instead of thinking that biometrics spell an end to individual privacy (50: -4). This is a widespread view that needs to be contested since it is highly inaccurate (48: -3). Securely identifying individuals is particularly important in border control. As a result, digital passports will need to include more biometric information (27: +3), and people should be willing to have their personal data shared internationally to speed up immigration processing in an increasingly globalised world (22: +2). Data sharing among governments does not mean that states lose control over citizens' data (16: -2) nor that the process is insecure (23: -4). However, people need to be alert to the possibility of having their personal data linked for unrelated purposes (15: +4). Governments need to be accountable too. For this reason, it is a good thing that protesters can record police action during demonstrations (32: +3) and post the videos on social network sites. It endows citizens with a sense of empowerment over state operations. Biometrics can also be used in domestic settings as they provide solutions to several safety concerns involving children and the elderly (18: 0). Crucially, biometrics facilitate improving authentication in social networking sites (19: 0) and increase safety on the Internet. To promote such uses of biometrics, fears over bodily integrity and loss of consent (3: -2) should be addressed. Biometrics should not be seen as tracking mechanisms (50: -4) reducing privacy (13: -5) and undermining community (14: -5) but as technologies for increasing security in a changing world.

Factor D: Casual Adopters

People worry more about convenience and security of transactions than issues of privacy (13: +5). This does not mean that biometrics jeopardize privacy (1: 0). This is quite an inaccurate view which is unfortunately widely held (48: +4). Biometrics are technological solutions to a number of identification problems; a swipe of the hand may provide faster and more secure identification procedures (25: +3) since asking people to remember multiple passwords rarely works. Biometrics help governments to securely identify mobile and versatile populations. Linking people irreversibly to their identities is crucial in a globalised world (26: +3). To this end, biometric resident permits can be an answer to immigration problems (26: +3). In tandem with border security, biometrics provide efficient solutions to problems pertaining to identity theft and fraud in financial transactions (10: +2). It follows that people should be willing to use their fingerprints or face to identify themselves in institutions such as banks. Finally, biometrics can be fun too. Face recognition software in mobile devices can be quite useful in several social settings (43: +2). People should embrace such innovations instead of worrying about their impact on their careers, credit held and families (46: -3). Biometrics is a reliable technology (9: -5) which endows people with more control over their personal data (31: -1). Contrary to popular understandings, it safeguards individual identity without undermining community (14: -5).

We now turn to a deeper analysis of these configurations so as to develop a clearer sense of the subject positions they encapsulate and what they mean in terms of our understanding of emerging contemporary conceptions of digital citizenship.

Citizens' voices: emerging viewpoints

> How people and institutions handle privacy and security concerns … will determine the new boundaries for citizens everywhere… What seems like defined debates today over privacy and security will broaden to questions of who controls and influences virtual identities and thus citizens themselves (Schmidt and Cohen, 2013, p.34 & p.81).

Digital citizenship is typically defined as the norms of appropriate, responsible behaviour with regard to technology use. In our view, digital citizenship above all relates to the ability of citizens to *give voice* to their concerns about this range of issues and to carve out distinctive positions on key topics. In a world where biometric forms of identification are used ever more extensively, policy-makers can no longer ignore public views on issues of accountability and empowerment, as well as the regulation of uses of personal data. Indeed, governments and industry are beginning to give attention to developing more user-centric tools of interaction. However, even here the role of the citizen is too narrowly circumscribed as 'users,' focusing almost exclusively on ease of use, rather than on more robust measures to enable citizen control over the collection and use of their data. The four discursive positions emerging from our research also suggest, contrary to expert views, that there is no simple zero sum trade-off between privacy and security. Our claim is that the four positions identified indeed encapsulate the wider held views of ordinary members of society, prefiguring the possible configurations around which different conceptions of digital citizenship may increasingly form.

Privacy Advocates understand their digital identities as a set of 'digital traces' (Schmidt and Cohen, 2013, pp.55- 6). They are conscious of the fact that digital interactions leave behind identifiable permanent markers of activity, and that the state

and corporations engage in extensive and potentially illegitimate collection and use of personal data. They are particularly concerned about the fact that they do not have control over this process and that there exists little by way of mechanisms of consent through which these interactions are managed. Ours is the first generation of humans to have an indelible record of our activities. Privacy Advocates are concerned about this 'data permanence' (Schmidt and Cohen, 2013, pp.55- 6). As a result, they are the citizens who 'have the self-awareness to closely manage their online identities and the virtual lives they lead' (Schmidt and Cohen, 2013, p.36). They are likely to insist on more user-centric designs, incorporating mechanisms of meaningful consent, so as to enable informed regulation of the collection and use of personal data. They are also the group most likely to demand 'the right to be forgotten', now inscribed in European and Californian law. As one respondent argues: 'I have the right to be forgotten, to be free, and unfollowed'.

These concerns are supplemented by an understanding of privacy as both an individual right and a societal good. Privacy Advocates are troubled by the linkage between specific biometric identifiers and particular individuals that may limit shared usage of goods (e.g. laptops and cars accessed by fingerprints) and undermine a sense of community.[5] This linkage also raises questions of bodily integrity given that contemporary biometrics are not simply neutral technologies that we can use without any further impact on our lives. Rather, Privacy Advocates recognise that they contribute to and redefine our senses of self. One respondent put it thus: 'This is a violation of human rights. It violates personal space and goes above and beyond the call of the state. If we start processes like this we will all eventually become robots.'

[5] Apple recently responded to this concern by allowing users of iPhones to register more than one fingerprint on a device, enabling multiple users of a single device.

This response echoes with public resistance to the use of full-body scanners at airports. In addition to expressing safety concerns, the public raised cultural and ethical concerns with regard to their use (Grabell, 2012). Digitized visualization dissecting the body and projecting 'fragmented and reduced elements of a person,' poses 'profound new questions of the political geographies of bodily boundaries' (Amoore and Hall, 2009, p.46).

Privacy advocates also problematise biometrics as intrusive. They reject most uses of biometrics since they consider them as forms of surveillance - by either the state or by private corporations - using fallible technologies. Privacy once lost cannot be recouped. Hence the urgent need to introduce mechanisms to safeguard control and accountability. While a considerable amount of progress has been made with regard to 'privacy by design' (Nissenbaum, 2004), work in this area is often based upon a narrow view of 'user' simply as 'consumers' of technology, rather than as citizens concerned with the reach of states and corporations into their lives. These wider concerns of Privacy Advocates resonate strongly with the positions advocated by many civil society organisations, such as the Electronic Frontier Foundation, that campaign to limit the collection of biometrics, as well as other organisations such as the Biometrics Institute that provides guidance on good practice in the collection, use and storage of biometric data (Lynch, 2012). While such specialised civil society organisations have long been critical of the way in which the state, industry and social media use biometrics, the wider public is now starting to engage with the range of new issues raised by biometrics. Artistic techniques – such as the use of face-painting to bedevil face recognition technologies (DIS Magazine, 2013) – are reasonably common and the public has begun to express annoyance with the use of new technologies such as google glass in public spaces. Privacy Advocates are most

strongly in favour of *sousveillance* - surveillance from below' (Mann, Nolan and Wellman, 2003) - as a legitimate strategy to counter excesses by authorities. Deploying technologies generally reserved for state use to call-out figures of authority abusing their power is now becoming commonplace, and are likely to be used more extensively, by marginalised groups, but also by those who are worried about the ever more extensive use of biometrics to record information about our public activities.

Conservative Techies also view the body as a way to identify oneself. In contrast to Privacy Advocates, their views are closer to that of the biometrics industry in positively framing the human body as a set of unique attributes for identification that people carry with them all the time. Central to the constitution of biometrics as the identification technology par excellence, especially in industry discourses, is the idea that body parts are unique and unchangeable. This property of biometrics is almost always stated in a 'factual' way in industry reports that propose biometrics as the logical solution to our increasing need to securely assert individual identity (Tistarelli, Li and Chellappa, 2009). Bodies are portrayed as 'natural passwords' as they contain information that is unique and cannot be removed from its bearer. Conservative Techies share the prevailing view in the biometrics industry that such technologies are privacy enhancing as they protect personal data from theft. An Ernest & Young (2011, p.2) report puts it thus: biometric technology can help guard against attempts to establish fraudulent multiple identities. As a Conservative Techie puts it: 'First technology, then security must be perfected – when this is done, then I would feel that the benefits would make it worth having a biometric ID.'

Conservative techies are also distinctive in that they are content that biometrics is used for security purposes and, in particular, for the state to use them 'to lock foreign nationals into their identities.' They also express the strongest view in

favour of iris recognition, as it does not have the criminal associations of fingerprinting. These views resonates strongly with widespread discourses that implicitly attribute the ills of society to the presence of 'foreigners' and 'immigrants,' as well as with state practices focusing on the control of immigration and refugees. Lynch (2012, p.3), for instance, argues that undocumented people living in the USA are 'uniquely affected by the expansion of biometrics collection programs'. Similarly, a key trigger in the adoption of biometric technologies in the EU includes the need to be able to identify individuals securely and efficiently to minimize security risks (in particular terrorism), illegal immigration, unwanted 'bogus' asylum seekers, 'overstayers' (European Commission, 2011, p.3) and 'benefit migrants', while also needing to ensure easier travel for 'trusted travellers' (US DHS), 'genuine visa applicants', citizens, as well as ease the movement of citizens and their benefits within the EU. These views reflect the UK Home Office (2013, p.5) argument that biometric residence permits 'make it easier for individuals to prove their identity, immigration status and entitlements', as well as industry suggestions that it is necessary to safeguard society through biometrics from 'cyberwolves' (Accenture, 2006).

Working with a strong public/private divide, Conservative Techies oppose the integration of biometrics into personal devices and utilities in the home (e.g. a fridge that records the eating habits of household inhabitants) since this is viewed as too intrusive into private life. They are, however, not opposed to it being deployed in the workplace (e.g. in time-clocks). Here the value of efficiency is placed alongside that of traditional security, with biometrics seen as technologies that could secure both. This strong divide between what is acceptable in private as opposed to in public is underwritten by an absence of scepticism about the potential misuses to which

biometric data collection are subject, and little awareness of the complexities of the potential trade-offs between security and privacy. Conservative Techies are not worried about data linkage. A 'having it all' attitude - 'securing' public spaces while protecting the home from intrusion - results from this trust in traditional authorities.

The third configuration, *Safety Champions*, entails a transactional view of identity. Identity here is seen as the information we use to identify ourselves in formal, institutional settings, and technologies are viewed as neutral instruments deployed in the service of identifying oneself. Like Conservative Techies, Safety Champions are content with biometrics at the border. Yet, their transactional understanding of identity is supplemented with a serious concern over safety in private spaces. To this end, they view biometrics primarily as a means to ensure access control over secure spaces such as the household or virtual spaces (e.g. accounts for on-line social networks). This echoes an argument prevalent in the biometrics industry where biometrics are promoted as tools enabling privacy and safeguarding individual identity. As Accenture (2006, p.3) suggests: 'Simply keying in some personal data - which can be stolen in a phishing scam … - is no longer enough to assure identity and deter fraud.' As the value of personal data increases, people become more aware of the need to safeguard information linked to their identity. Given this, biometric identifiers - 'something we are' and something we cannot 'leave behind' – are primary means for establishing digital safety. Safety Champions echo this view in their emphasis on digital safety in a wide range of spheres. It is particularly evident in their belief that the government should play a role in the reduction of fraud, an argument which forms one of the key drivers of developments in e-government. A report by the European Commission (Maghiros et al., 2005, p.7) suggests that: 'Modern economics require increasing levels of mobility

on the part of the workforce … physical identity is increasingly being replaced … by its digital equivalent… Biometric technologies seem to offer a solution for stronger identification.' However, Safety Champions are rather more sceptical of the potential consequences of commercial uses of existing biometric technologies and their implications for privacy, suggesting that under these circumstances, 'privacy as we know it would be a thing of the past'.

This healthy scepticism - in contrast to Conservative Techies - is also present in the position of Safety Champions on the possibilities of misuse of data once collected. Concerned about loss of privacy and bodily integrity as well as issues of consent and accountability, they are in many respects closer to Privacy Advocates than to Conservative Techies, advocating the use of *souveillance* and other mechanisms to keep governments accountable. They are less interested than Conservative Techies in the use of biometrics in personal devices, and hence do not share what we call the 'enjoyment factor', which is most prominent in those identifying as Causal Adopters. However, they positively engage with uses of biometrics to safeguard potentially vulnerable sectors of the population, such as children and the elderly. Far from being tools of surveillance, on this view, biometrics are regarded as technologies that increase security in a changing world.

Here an interesting shift is present in regard to trust in a progressively more complex world: as biometrics increasingly encompass personal uses, they become constitutive of how people build their relationships around technological devices and their ability to verify identity (Dardy, 1990). Trust, rather than being the outcome of reciprocal exchange of information between people, is technology-based, echoing the corporate slogan of a leading French biometric company Morpho (2013): 'Creating trust around the world'. The need to protect one's identity is also increasingly coupled

with the need for convenience valued by Safety Champions: 'I always forget the password that I set. It costs time to remember it while I can always bring my body with me. It's convenient in my point of view.' Biometrics, it is argued, solve this problem. This is a view that is taken to its extreme by Casual Adopters.

Casual Adopters hold the most encompassing view of digital identity. For them, it is the sum of all available information about an individual. Echoing a widely held view that 'privacy as we know it is a thing of the past' (Accentrure 2014) those who identify with this position believe that privacy is no longer is tenable, and positively celebrate the technologies with which we live today. Like Safety Champions, they believe that they can provide their personal data to governments, as long as there are appropriate safeguards in place. Uniquely, they also express trust in the technological infrastructures in place for handling personal data, echoing industry and governmental discourses that portray biometrics as 'merely' technical. As we have seen, governments and industry have developed an intricate web of discourses promoting biometrics through arguments around technological progress and neutrality; the idea of biometrics as value-neutral means to secure identified ends propelled the diffusion of biometrics to contexts far beyond border control. Equally constitutive of this development has been the emerging commitment by the biometrics industry to address privacy concerns accompanying biometrics. This has been done by seeking to develop applications that allow users to control their biometric data, and through adopting professional codes of conduct and privacy charters (IBIA, 2014). The latter occurred largely as a result of pressure by civil society organizations such as the Biometrics Institute (2013) that developed Privacy Guidelines 'to provide a universal guide for suppliers, end users, managers and purchasers of biometric systems'. The argument for neutrality supports the idea – core to the views espoused

by Casual Adopters - that once technical issues are addressed and privacy checks are done, all problems are solved. This, precisely, is what is assumed by those promoting their use: once the public is made aware of the need to use biometrics - through the deployment of justifications based on security, safety, efficiency, technological prowess and other reasons - they will appear to be neutral, even natural and above all, unproblematic technologies.

Conclusion

Given these distinctive views on digital identity and their relation to privacy and security, it is not the case, as widely argued, that the public is unable to form and express views on the complicated issues that arise in the wake of the ever more widespread use of biometrics in everyday life. It is also clear that everything depends on contextual articulations between biometrics and the other key factors identified: citizen views on security; on the use of biometrics in public, personal and domestic spaces; on whether individuals are concerned with data collection, usage and sharing; whether they think governments and industry should be held accountable and are responsible for the use of citizens' personal data. The results of our research provide a first snapshot of the distinctive positions that have crystallized thus far. Given the rapidity of change in the use and diffusion of biometrics, these distinctive positions as identified in our research are likely to become more prominent in public debate.

It is crucial that we remain cognizant of the fact that the processes of articulation giving rise to each of the discursive positions are deeply political in nature: they are not determined, even as they are shaped by ongoing developments in our contemporary world. The diffusion of biometrics will continue to challenge and complicate our conceptions of the boundaries between politics and bureaucracy, as

well as of our conceptions of accountability in an ever more highly digitized world. It is notable that there currently are relatively weak concerns about the uses of large-scale personal data for commercial use. This is likely to become an area of greater concern as the public becomes aware of the commercial value of 'big data' that trades largely on aggregation and analysis of data that is collected for different purposes and without consent. The uses of biometrics in personal devices are likely further to blur the divide between what is considered private and what is considered public, and thus available for scrutiny. Together, these will shape our conceptions of what it means to be a responsible citizen in a digital environment. It is crucial that citizens are consulted in the development of new regulations as well as in the development of novel technologies and mechanisms for such consultation.

Using a combination of Q-methodology and political discourse analysis, we have been able to show how distinctive viewpoints crystallise out of wider discourses on biometrics. These wider discourses - articulated by both governmental organisations and the biometrics industry - have tended to remain trapped in an apparent zero-sum trade-off between security and privacy. The viewpoints uncovered in our research shows how citizens have moved beyond a zero-sum game, taking up more complex positions that shape whether and in what contexts the use of biometrics are acceptable.

References

Aas, K. F. (2006) 'The body does not lie', *Crime, Media, Culture, 2*(2), 143-158.

Accenture (2006) The future of identity [online]. Available from: http://www.accenture.com/SiteCollectionDocuments/PDF/future_identity.pdf [Accessed 10 May 2014].

Accenture (2014) Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists [online]. Available from: http://newsroom.accenture.com/news/eighty-percent-of-consumers-believe-total-data-privacy-no-longer-exists-accenture-survey-finds.htm [Accessed 15 December 2014].

Agamben, G. (1998) *Homo Sacer* (D. Heller-Roazen, Trans.). Stanford: Stanford University Press.

Agamben, G. (2004) 'Bodies without words', *German Law Journal, 5* (2), 168-9.

Amoore, L. (2006) 'Biometric borders', *Political Geography, 25*, 336-51.

Amoore, L. and Alexandra Hall (2006) 'Taking people apart', *Environment and Planning D: Society and Space 27*(3), 444-64.

Aradau, C. (2008) 'Forget equality? Security and liberty in the 'War on Terror'', *Alternatives, 33* (3), 293–314.

Bennett, L. W. and A. Segerberg (2013) *The Logic of Connective Action.* Cambridge: Cambridge University Press.

Bigo, D. (1998) Frontiers and security in the European Union. Pp. 148-64. In M. Anderson & E. Bort (eds), *The Frontiers of Europe*. London: Pinter.

Bigo, D. (2005) 'La mondialisation de l'(in)sécurité', *Cultures et Conflits, 58*, 53-101.

Biometrics Institute (2013) Privacy Guidelines [online]. Available from: http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_V1.pdf [Accessed 29 October 2015].

Brown, S. R. (1980) *Political Subjectivity. Applications of Q Methodology in Political Science*. New Haven: Yale University Press.

Brown, S. R. (1993) 'A primer on Q methodology', *Operant Subjectivity, 16*(3/4), 91-138.

Callon, M.; Lescoumes, P. and Barthe, Y. (2009) *Acting in an Uncertain World.* Cambridge, MA.: MIT Press.

Caplan, J. (2001) 'Protocols of identification in nineteenth-century Europe'. Pp. 49-66. J. Caplan & J. Torpey (eds), *Documenting Individual Identity*. Princeton: Princeton University Press.

Caplan, J., & Torpey, J. eds. (2001) *Documenting Individual Identity.* Princeton: Princeton University Press.

Danielson, S., Tuler, S. P., Santos, S. L., Webler, T., & Chess, C. (2012) 'Three tools for evaluating participation', *Environmental Practice, 14*(2), 101-9.

Davies, B. and R. Harre, (1990) 'Positioning: the discursive production of selves', *Journal for the Theory of Social Behaviour*, 20(1), 43-63.

DIS Magazine (2013) How to hide from machines [online]. Available from: http://dismagazine.com/dystopia/evolved-lifestyles/8115/anti-surveillance-how-to-hide-from-machines/ [Accessed 25 January 2015].

Dryzek, J. S., & Berejikian, J. (1993) 'Reconstructive democratic theory', *American Political Science Review, 87*(1), 48-60.

Dryzek, J. S., and S. Niemeyer (2008) 'Discursive representation', *American Political Science Review, 102*(4), 481-93.

Erst & Young (2011) Biometrics [online]. October. Available from: http://www.planetbiometrics.com/creo_files/upload/article-files/Biometrics_-_time_to_evangelise_the_benefits.pdf [Accessed 16 February 2015].

European Commission (2011) Smart borders. Brussels, COM(2011) 680.

Fischer, F. (2009) *Democracy and Expertise*. New York: Oxford University Press.

Fisher, K.M. (2015) 'Spatial and temporal imaginaries in the securitisation of terrorism.' In Jarvis, L. and M. Lister (eds), *Critical Perspectives on Counter-Terrorism* (London: Routledge), pp.56-76.

Grabell, M. (2012) New report likely to fuel debate over TSA scanners [online]. *Propublica*, Available from: http://www.propublica.org/article/report-on-airport-backscatter-body-scanners [Accessed 13 July 2014].

Author (2014).

Author (2009).

Glynos, J. and D. Howarth (2007) *Logics of Critical Explanation*. London: Routledge.

Home Office (2006) Borders, Immigration and Identity Action Plan [online]. Available from: http://www.statewatch.org/news/2007/jan/uk-borders-id-card-plan.pdf [Accessed 29 January 2015].

Home Office (2013) Guidance Notes Biometric Residence Permits [online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261497/brp-information-leaflet.pdf [Accessed 29 January 2015].

Homeland Security & Defense Business Council (2011) Biometrics [online]. Available from: http://homelandcouncil.org/the-91011-project-biometrics.html#sthash.tCiHRig1.dpuf [Accessed 10 June 2013].

Howarth, D. (2009) 'Power, discourse, and policy', *Critical Policy Studies*, 3, 309-35.

IMPRINTS (2014) What do users want from their future means of identity management? [online]Available from: http://www.imprintsfutures.org/ [Accessed 19 February 2015].

International Biometrics and Identification Association (IBIA) (2013) Biometrics and Identity in the Digital World [online]. Available from: https://www.ibia.org/resources/whitepapers/ [Accessed 18 February 2015].

IBIA (2014) Privacy Best Practice Recommendations [online]. Available from: https://www.ibia.org/resources/whitepapers/ [Accessed 29 January 2015].

Jansanoff, S. (ed.) (2004) *States of Knowledge.* Routledge.

Jumb, Vijay, Martin, Jason, Figer, Phyllis, Rebello, Aniket (2015) 'Mobile Voting Using Finger Print Authentication', *International Journal of Engineering and Advanced Technology* 4(4), 141-6.

Jeffares, S., & C. Skelcher (2011) 'Democratic subjectivities in network governance', *Public Administration, 89* (4), 1253-73.

Laclau E. and C. Mouffe (1985) *Hegemony and Socialist Strategy*. London: Verso.

Lanier, J. (2014) *Who Owns the Future?* London: Penguin Books.

Liberty Global (2012) The value of our digital identity [online]. Available from: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf [Accessed 20 July 2014].

LSE Department of Information Systems (2005) The Identity Project [online]. Available from: http://identityproject.lse.ac.uk/identityreport.pdf [Accessed 16 February 2015].

Lynch, J. (2012) From Fingerprints to DNA [online]. Available from: https://www.eff.org/files/filenode/biometricsimmigration052112.pdf [Accessed 30 January 2015].

Madden, M. and Rainie, L. (2015) Americans' attitudes about privacy, security and surveillance [online]. Available from: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [Accessed 3 June 2015].

Maghiros, I., Y. Punie, S. Delaitre, E. Lignos, C. Rodríguez, M. Ulbrich, M. Cabbera, B. Clements, L. Beslay, and R. Van Bavel (2005) Biometrics at the Frontiers [online]. Available from: http://ftp.jrc.es/EURdoc/eur21585en.pdf [Accessed 10 May 2014].

Magnet, S. A. (2011) *When Biometrics Fail.* Durham: Duke University Press.

Mann, S., J. Nolan and B. Wellman (2003) 'Sousveillance', *Surveillance & Society* 1(3), 331-55

March, J.G. and Olsen, J.P. (1995) *Democratic Governance.* New York: Free Press.

Misuraca, G. & Lusoli, W. (2010) *Envisioning digital Europe 2030.*Technical Reports. EUR 24614 EN. Seville: Joint Research Centre.

Molokotos-Liederman, L. (2007) 'The Greek ID card controversy', *Journal of Contemporary Religion*, Vol. 22 (2),187-203.

Muller, B. J. (2004) '(Dis)qualified bodies', *Citizenship Studies, 8*(3), 279-94.

Nissembaum, H. (2004) 'Privacy as Contextual Integrity', *Washington Law Review, 79*(1), 119-58.

Noiriel, G. (2001) 'The identification of the citizen'. Pp. 28-48. In J. Caplan & J. Torpey (eds), *Documenting individual identity* Princeton: Princeton University Press.

Author (2000).

Author (2012).

Authors (2017).

Omand, D. (2010) *Securing the State*. London: Hurst.

Schmidt, E. and Jared Cohen (2013) *The New Digital Age*. London: John Murray.

Scott, J. C. (1998) *Seeing like a State.* New Haven: Yale University Press.

Schmolck, P. (2014) PQMethod Manual. (online) Available at: http://schmolck.userweb.mwn.de/qmethod/pqmanaul.htm [Accessed 10 May 20150].

Sullivan, H., P. Williams & S. Jeffares (2011) 'Leadership for collaboration', *Public Management Review, 14*(1), 41-66.

Tistarelli, M., S.Z. Li, and R. Chellappa, eds. (2009) *Handbook of Remote Biometrics.* London: Springer-Verlag.

Tully, J. (2008) *Public Philosophy in a New Key. Volume I.* Cambridge: Cambridge University Press.

Van der Ploeg, I. (1999) 'Written on the body', *Computers and Society, 29*(1), 37-44.

Vaughan-Williams, N. and D. Stevens (2015) 'Vernacular theories of everyday (in)security', *Security Dialogue*, 47(1), 40-58.

Watts, S., & P. Stenner (2005) 'Doing Q methodology', *Qualitative Research in Psychology, 2*(1), 67-91.

Watts, S., & Paul Stenner (2012) *Doing Q Methodological Research*. London: Sage.

Willis, M., & S. Jeffares (2011) 'Four viewpoints of whole area public partnerships', *Local Government Studies, 38*(5), 539-56.

Seeing like a citizen – Tables

Table 1

Discourse	A	B	C	D	Variance explained (%)	Number of coefficients >0.36
A	1.000	0.1962	-0.0209	-0.0429	25	30
B		1.000	0.4436	0.4226	9	8
C			1.000	0.3888	7	5
D				1.000	6	3

Table 2: Factor arrays: Factor q-sort values for each statement

	Statements	**Factors**			
		A	**B**	**C**	**D**
1.	As companies become better able to monitor our every move, consumers who want to maintain their privacy should be given the option to opt out.	+3	2	+1	0
2.	Biometrics, such as iris scans, can produce medical information, allowing people subsequently to be profiled according to their current and potential health status.	0	+4	-1	0
3.	Remote biometrics, using face or gait recognition, defies many of our deeply ingrained values concerning bodily integrity, freedom from arbitrary inspection, and requirements for consent.	+2	-1	-2	0
4.	Our bodies are like natural passwords or identity cards that we all carry with us at all times and that we can never leave at home.	0	+5	+1	+1
5.	Industry should embrace biometric time clocks – based on hand	-3	0	-2	-1

	geometry or finger printing - that can simply and accurately capture labour data.				
6.	We need to find a better alternative to all this traditional identification paraphernalia such as cards, passwords and PINs.	-1	+3	+2	+2
7.	In the wrong hands, biometrics have the potential to violate privacy.	+5	+5	+5	+3
8.	Iris scanning is more acceptable than fingerprint recognition, since it does not have criminal associations.	-1	-4	+1	-2
9.	Biometric identification relies on technology that is far from proven.	-1	+1	-3	-5
10.	Customers are likely to be willing to lodge two fingerprints and their facial image with their bank, if it means protection against banking fraud.	0	+1	0	+2
11.	If my phone had a secure palm recognition app to securely authenticate my identity, I'd be happy to use to connect with banks and other organisations.	-2	0	0	0
12.	Mobile phone owners should be prepared to download gait recognition software on their phones to prevent others accessing their information in the event of theft or loss.	-1	+2	+1	-2
13.	People worry more about convenience and security of transactions than issues of privacy.	-1	-2	-5	+5
14.	Using biometrics means that I can't lend my car, phone or laptop to a friend or relative nor can they lend me theirs. It undermines community.	0	-5	-5	-5

15.	We need to be wary of the possibilities of linking our personal data from one database to another for unrelated purposes.	+3	-1	+4	+3
16.	Decentralized global uses of biometric technologies mean that nation states no longer have exclusive control over citizens' data.	1	-1	-2	-1
17.	It would be nice to be able to carry my biometric credentials in a piece of personal jewellery.	-4	-2	-1	-1
18.	Biometric technologies supply simple solutions to domestic problems, from access control to secure use of kitchen appliances.	-1	-3	0	-2
19.	We urgently need improved authentication to social networking sites; biometrics can help here.	-4	-1	0	-1
20.	We need technologies that can prevent people holding fraudulent multiple identities.	0	+2	+4	+4
21.	The digital format of biometric records will make this information subject to serious security risks.	+2	+1	-3	-3
22.	As a trade-off for faster immigration processing, passengers should accept a system where more of their personal data is shared internationally.	-4	0	+2	1
23.	No biometric technology is fully secure since it involves a range of human decisions, especially in settings such as border control.	+2	+4	-4	+2
24.	Counter-terrorism officials cannot predict terrorism or identify terrorists by a biometric sample alone.	+2	-2	0	-2
25.	Asking people to remember multiple passwords rarely works. Whether we like it or not, a swipe of the hand may be the answer.	-2	+1	+2	+3
26.	In a globalised world, the state's task of giving stable identities to	-3	0	+1	+3

	mobile and versatile populations becomes extremely difficult. Biometric residence permits is thus part of the answer.				
27.	Digital passports of the future will need to include more biometric information to prove who we are.	-2	0	+3	+1
28.	Biometric identifiers need to be used to effectively and securely lock foreign nationals into one identity.	-3	0	-1	-4
29.	People suffering from Alzheimers should be implanted with RFID chips containing their biometric information to help their families track them in case they get lost.	-3	+3	+3	-3
30.	If CCTV can now identify us through face recognition, we should be allowed to use headwear, such as glasses called "privacy visors", to maintain our privacy.	0	-5	-3	-3
31.	With each new development in biometric technologies, users are getting less control over their data, in terms of knowing when, where, and why it is used.	+4	+2	0	-1
32.	It is a good thing that protesters can use their smartphones to record police action during demonstrations.	+1	-3	+3	0
33.	It is worrying that all this extra information generated by biometric systems can potentially be further used for unintended, unauthorized, purposes.	+5	+3	+1	+1
34.	Facial recognition technology reduces the consumer's ability to thwart unwanted tracking since it doesn't require any personal devices.	0	-1	-2	-1
35.	Government needs to adopt biometrics in order to reduce fraud,	-5	+3	+4	+4

	cut costs and enable them to offer faster, more convenient services.				
36.	Biometrics information stored on travel documents and the processing of such information should respect national data protection laws, human rights and cultural practices.	+3	+1	+3	+2
37.	It is worrying that all this central storage is seemingly irreversible; the owner of biometric data should be able to control his/her data.	+3	-1	0	-1
38.	I don't like the fact that biometrics links my personal data irrevocably to me. I feel I won't have the right to be forgotten.	+1	-4	+2	-4
39.	If advertising boards have face recognition technology it is important that notices are used to alert consumers.	+1	-1	+1	+1
40.	Border control should take into account objections of passengers who find whole-body scanning a humiliating experience.	0	-2	-1	0
41.	Multiple searches of databases with the unique biometric identifiers can result in an excessive collection of personal information pointing to an individual.	+1	+1	+2	+1
42.	The idea that there may be new biometric technologies that can identify me without me ever knowing, makes me uncomfortable.	+4	0	-4	0
43.	It is an exciting time for facial recognition! It is now easily available through handheld consumer devices and free software packages.	-1	-3	-1	+2
44.	It needs to be acknowledged that biometrics provides a powerful weapon to corporations and governments; these are surveillance technologies affecting the freedom of individuals and of societies.	+4	+2	0	+1

45.	Biometric ID systems enable greater surveillance without providing increased protection or security for citizens.	+1	-3	-1	-2
46.	The ability of emerging technologies to put "a name to face", so to speak, is going to impact on our careers, credit, health, and families.	+2	+1	-1	-3
47.	There's a need for commercial products that combine tracking and location data with individual profile histories from social media to monitor people.	-5	-4	-2	-4
48.	The idea that biometrics equals privacy violation, is probably the most inaccurate and yet also most widely held view of biometrics.	-2	0	-3	+4
49.	As long as data is well protected, then I think there's no harm in having a biometric ID card.	-2	+4	+5	+5
50.	If we as a society accept biometric technology in the commercial form now being marketed, it spells an end to individual privacy as we now know it.	+1	-2	-4	0