Surveillance & Society

Review

In Defence of Privacy: The concept and the regime

Colin J. Bennett

University of Victoria, Canada. cjb@uvic.ca

The study of surveillance has now matured to the point where it embraces a wide diversity of disciplinary traditions. It is rich with contention over the roots of contemporary surveillance, over the relations between surveillance and power, over complex questions of structure and agency, over the place of new technologies, over the impacts on groups and individuals and over the appropriate means of resistance. Surveillance is a condition of modernity, integral to the development of disciplinary power and new forms of governance (Haggerty and Ericson 2006, 4). It has been essential to the development of the nation state, to global capitalism and to the decentred forms of disciplinary power and 'governmentalities' inherent within modern societies. It is *that* important, and consequently generates profoundly significant disputes over concepts, theory and method (Murakami Wood 2009).

However, there is one issue over which this broad and diverse community of surveillance scholars tends to agree: the concept of *privacy*, and the policies it generates, are inadequate. Indeed, this view has almost reached the level of a conventional wisdom. 'Privacy' and all that it entails is argued to be too narrow, too based on liberal assumptions about subjectivity, too implicated in rights-based theory and discourse, insufficiently sensitive to the social sorting and discriminatory aspects of surveillance, culturally relative, overly embroiled in spatial metaphors about 'invasion' and 'intrusion', and ultimately practically ineffective. As a concept, and as a way to frame the various global challenges encountered within 'surveillance societies', it is profoundly inadequate. It is not, and can never be, the 'antidote to surveillance' (Stalder 2002).

These critiques are clearly important, and to some extent, have set scholarly inquiry on new, exciting and broader trajectories than those offered by privacy scholarship, which still tends to be dominated by legal approaches and methods. Furthermore, these traditions overlap in multiple and complicated ways. Surveillance scholars do recognize the emotive potential of appealing to privacy as a powerful value (e.g. Lyon 2001, 150), and privacy scholars, advocates and regulators now frequently speak as if the social problems are far wider than individual privacy invasion, invoking broader questions of social control and warning of the dangers of the creeping 'surveillance society' (e.g. UK Information Commissioner). Nevertheless, the critique of privacy in the academic surveillance literature is widespread and insistent. Some of the more modern surveillance literature barely refers to the term (for example Aas et al. 2009).

On closer examination, however, I want to suggest that the critiques of privacy are quite diverse, and often based on some faulty assumptions about the contemporary framing of the privacy issue and about the implementation of privacy protection policy. Some critiques are pitched at a conceptual level; others focus on practice. There is a good deal of overstatement and a certain extent to which 'straw men' are

Bennett, C.J. 2011. In defence of privacy: The concept and the regime. *Surveillance & Society* 8(4): 485-496.
http://www.surveillance-and-society.org | ISSN: 1477-7487

constructed for later demolition. Moreover, the critiques tend to be included in texts en *passant*, dotted around numerous sources as ways to reinforce broader empirical or theoretical claims. The purpose of this paper, therefore, is to disentangle the various critiques and to subject each to a critical analysis.

I make no *a priori* assumption about the meaning of privacy at a conceptual level. I do tend to side with the conclusions of Solove (2008, 171-2), who argues that privacy is a convenient conceptual shorthand way to describe a cluster of problems that are 'not related by a common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element — they share family resemblances with each other'. I am, however, interested in what surveillance scholars think the concept means given that those understandings animate particular critiques and reformulations. As a *policy* problem, there has been an international convergence of understanding about the 'privacy paradigm' (Bennett and Raab 2006). As I hope to demonstrate, some of the critique from surveillance scholars is insufficiently sensitive to the ways in which the privacy value has been reframed at a governance level to meet the collective challenges posed by the broadening and deepening of surveillance.

The article is conceived, therefore, as a defence, of privacy as a way to frame the contemporary problem, as a regime of governance and as a set of practices. It is also an attempt at reconciliation. What areas of concern can appropriately be addressed under the rubric of 'privacy'? What are beyond its scope? What concerns, for privacy regulators and advocates, can better be addressed by framing the problem in terms of 'surveillance'?

Privacy is about Me, Me, Me…

At root, many surveillance scholars are troubled by the theoretical roots of modern privacy claims. Philosophically, privacy has its roots in liberal individualism, and notions of separation between the state and civil society. Privacy, in this conception, is about the protection of the self, from the state, from organizations and from other individuals. Privacy, therefore, tends to reinforce individuation, rather than community, sociability, trust and so on. It is about me, and nobody else.

Unfortunately the individualization of the issue is reinforced by some of the more prominent and influential definitions of privacy, which tend to proceed from a sort of state of nature assumption that there is a condition of perfect privacy which is violated when one enters into social relations (Gilliom 2001, 121). The frequency, for example, with which the Warren and Brandeis (1890) formulation of privacy as the 'right to be let alone' is cited has an unfortunate implication of reinforcing the notion that privacy is about seclusion and separation. Ruth Gavison's analysis, which posits a possible state of 'perfect privacy when he is completely inaccessible to others' (1980, 428), generates similar worries. By extension, privacy can only be restored once the whole panoply of public and private organizations stop monitoring and return what information they possess to the rightful owner — the individual.

One could argue that a formulation of privacy that has been the most more influential in the policy world is that of Alan Westin: 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (Westin 1967, 7). Charles Fried also defined the idea in terms of 'the control we have over information about ourselves' (Fried 1970, 140). Although these and other definitions do presume the importance of privacy within a set of social, economic and political relations, they still tend to be seen as a crucial component of democratic, and particularly liberal or pluralistic democratic, politics. Furthermore, these conceptual debates have largely taken place within the context of American attempts to draw some lines between privacy and other values in order to inform evolving constitutional and tort law (see Solove 2008). This whole debate does tend to reflect a broader American feature of the US rights discourse with its 'extraordinary homage to independence and self-sufficiency, based on an image of the rights-bearer as a self-determining, unencumbered, individual, a being connected to others only by choice' (Glendon 1991, 48).

The concept of privacy has therefore been open to attack on the same grounds on which liberalism more generally is critiqued. It reifies a problematic distinction between the realms of the public and the private – between other and self-regarding actions in John Stuart Mill's terms. It negates communitarian values such as trust and the common good (Etzioni 1999). It reinforces the patriarchal separation between a masculine public realm and a private female realm (Allen 1985, DeCew 1997). And it completely misses the point of some post-modern theorists who insist that the notion of the 'self' or the 'subject' mask far deeper ontological contradictions and complexities (Poster 1990).

These various critiques are picked up by surveillance scholars. For David Lyon, for instance, the issue is not about privacy but about 'where the human self is located if fragments of personal data constantly circulate within computer systems beyond any agent's personal control' (1994, 18). He has argued that 'privacy tends not to see surveillance as a social question or one that has to do with power' (2001, 150). It embodies a profound contradiction: 'privacy answers, consistently but paradoxically, to personal fears of invasion, violation and disturbance. Having successfully prised each of us from our neighbours so that we could be individuated social actors, amenable to classification and sorting and disembodied abstractions, privacy responses echo just such individuation' (2001, 150).

The individualistic conceptions of privacy, however, hardly constitute a paradigmatic understanding of the problem, and there have been a number of attempts to realign the issue in ways that perhaps hold more contemporary relevance. Most prominently, Priscilla Regan has argued that privacy should be seen as a common value, 'in that all individuals value some degree of privacy and have some common conceptions about privacy'. It is a public value, 'in that it has value not just to the individual…but also to the democratic political system'. And it is a collective value, 'in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy' (Regan 1995, 213). Her analysis suggests that privacy, framed in individualistic terms, is always on the defensive against arguments for the social benefits of surveillance. Privacy will always be in conflict with those social and collective issues, which tend to motivate mass publics and their representatives. We must, therefore, frame the question in social terms, because society is better off if individuals have greater levels of privacy.

In a similar vein, Valerie Steeves has recently attempted to reconceptualize privacy 'as a dynamic process of negotiating personal boundaries in intersubjective relations…By placing privacy in the social context of intersubjectivity, privacy can be more fully understood as a social construction that we create as we negotiate our relations with others on a daily basis' (Steeves 2008, 193). The critique also appears in analyses of particular surveillance practices. Jane Bailey and Ian Kerr, for instance, have analyzed the continuous archival and retrieval of personal experiences (CARPE) and concluded that the 'individualistic conception of privacy that predominates western thinking, is nevertheless inadequate in terms of recognizing the effect of individual uptake of these kinds of technologies on the level of privacy we are all collectively entitled to expect' (Bailey and Kerr 2007).

Moreover, recognition of the social value of privacy is increasingly observed in the legal and policy world. One of the earliest and most influential reports on privacy protection was produced in the mid-1970s in the United States. The Privacy Protection Study Commission was established under the 1974 Privacy Act, and had some influence on setting US privacy protection policy along a different track from that followed in Europe and other countries. It began, however, by pointing out that: 'A major theme of this report is that privacy, *both as a societal value* and as an individual interest, does not and cannot exist in a vacuum. Indeed, 'privacy' is a poor label for many of the issues the Commission addresses because, to many people, the concept connotes isolation and secrecy, whereas the relationships the Commission is concerned with are inherently social' (United States PPSC 1977, 21, my emphasis).

The doctrine of the 'right to be let alone' (Warren and Brandeis 1890) and subsequent jurisprudence has produced one very important tradition and legacy for privacy scholars. A different and more recent tradition, however, views privacy protection as a matter of regulatory policy. The various 'data protection' or 'privacy' statutes enacted since the 1970s are founded on an assumption that the processing of personal information by public, and latterly, private organizations was too important to be left to the private claims of the individual or to the decisions of the courts. As Spiros Simitis, the world's first data protection commissioner, argued in an influential article in 1978, 'privacy considerations no longer arise out of particular individual problems; rather they express conflicts affecting everyone' (Simitis 1978, 709).

As the issue has matured, both nationally and internationally, we have seen an increasing recognition that the work of this policy community is directed by the larger questions about the kind of society we are building. The trend is impossible to measure. However, a few contemporary examples illustrate the point that collective conceptions of privacy do appear in the discourse of regulators and motivate their actions. For example, the repeated comments by the former Information Commissioner of the UK that Britain is 'sleepwalking into a surveillance society' has gained a considerable purchase at the highest levels of British politics (The Times 2004). In 2006, the world's data protection and privacy commissioners released a closing statement to their annual conference acknowledging among other things that: **'**Privacy and data protection regulation is an important safeguard but not the sole answer. The effects of surveillance on individuals do not just reduce their privacy. They also can affect their opportunities, life chances and lifestyle. Excessive surveillance also impacts on the very nature of society. Privacy and data protection rules help to keep surveillance within legitimate limits and include safeguards. However, more sophisticated approaches to regulation need to be adopted' (International Data Commissioners Conference 2006)

The regulators and the discourse have moved on. Whether or not an individualistic conception of 'privacy' as conceived in the 'privacy literature' effectively describes the challenges of contemporary surveillance is largely beside the point. For a long time, privacy protection has been a matter of *public policy*.

Privacy and the 'Invasion' of Space

A related theme within the surveillance literature is a critique of the 'spatial' implications inherent in much privacy discourse. Felix Stalder (2002, 121) critiques the concept because it is typically framed as a 'kind of a bubble that surrounds each person, and the dimensions of this bubble are determined by one's ability to control who enters and who doesn't. Privacy is a personal space; space under the exclusive control of the individual. Privacy, in a way, is the informational equivalent to the (bourgeois if you will) notion of "my home is my castle."' Stalder has put his finger on a very important assumption within the privacy literature, that there should be a zone or a realm into which other individuals and organizations may not encroach.

This example inevitably leads to prominent metaphors about invasion, intrusion or violation, rhetoric that easily appeals to the popular imagination. Kevin Haggerty and Richard Ericson (2006, 12) believe that such metaphors distract from a central aspect of contemporary surveillance:

> In our day-to-day lives, privacy is not routinely 'invaded': it is not pried away from a resistant and apoplectic public. Instead, privacy is compromised by measured efforts to position individuals in contexts where they are apt to exchange various bits of personal data for a host of perks, efficiencies, and other benefits. Part of the ongoing politics of surveillance therefore does not involve efforts to 'capture' data, but to establish inducements and enticements at the precise threshold where individuals will willingly surrender their information. Surveillance becomes the cost of engaging in any number of desirable behaviours or participating in the institutions that make modern life possible.

Their point is a good one. It also leads to skepticism over the value of talking in measurable terms about whether 'we' have less privacy than in the past (Bennett and Raab 2006, 24-5).

Again, however, it can be argued that the governance of the issue has moved beyond the popular rhetoric. The privacy literature contains several attempts to add other dimensions, or forms, of privacy to provide intellectual foundations for the more complicated relationships between the individual and modern organizations. Westin disaggregated privacy into four states; anonymity, isolation, intimacy and reserve (Westin 1967). Applying Maslovian theory, Roger Clarke has distinguished between privacy of the person, privacy of personal behaviour, privacy of communications and privacy of data (Clarke 2006). Solove developed a complex taxonomy of socially recognized privacy violations surrounding information collection, information processing, information dissemination, and invasion (Solove 2008). Most recently, Helen Nissenbaum has argued that the public/private dichotomy tends to lead to a dead-end, and has fashioned a more nuanced theory of privacy as contextual integrity (Nissenbaum 2009). Conceptually, and practically, privacy protection has not just been about protecting the 'bubble' that surrounds the individual. It has been defined, redefined, disaggregated, sliced and diced (with varying success) to embrace the inherently social, relational, and contextual aspects of the value.

And at the governance level, only a fraction of privacy problems that reach the desks of the regulators really relate to the protection of a private realm from 'invasion'. Modern privacy issues only deal partially with the initial process of information collection, capture or relinquishment. They assume a relationship between the organization and the individual, and the regulatory problems then relate to how that relationship is managed in informational terms: how the personal information is kept secure; how access controls within the organization are managed; how disclosures are controlled; how notification and consent are communicated, and so on. Hence, the framing of the problem in terms of the conditions under which others might 'enter' one's personal space is unhelpful. The critique that privacy is about protecting the 'bubble' establishes a straw man. Academically and practically, the issue is more complex and relational, and most privacy scholars and professionals would realize that.

Privacy suffers as a human 'right'

A third and related set of objections rest on the notion that privacy is normally articulated as a 'right' and is therefore plagued with some of the same problems associated with the rights discourse more generally. Fundamentally, perceptions of privacy violation can be very subjective, and inseparable from wider attitudes about the institution, the program or the service: 'Translating this sense of subjective violation into a legal privacy claim is very difficult, especially given the legal tendency to avoid embracing subjective notions of victimization' (Haggerty and Ericson 2006, 9). Privacy battles also tend to pit vulnerable individuals, or poorly resourced civil liberties groups, against very powerful public or private organizations. Gilliom's study of welfare surveillance contends that the legalistic rights vocabulary, from which the privacy discourse is derived, means very little to the subjects of his study: 'there appears to be a strong possibility that the privacy rights language may serve to exclude a significant portion of the population for whom the idea of the private individual is just silly — people, many of them women and others who are deeply involved in family life, care giving, or other relations involving significant dependency and interdependency' (Gilliom 2006, 124).

The argument that the rights discourse tends, therefore, to push debate toward experts and authorities and fails to serve the people most at risk, is an important and generally valid one. Individuals do find it difficult to relate their experiences of surveillance to the possibilities of legal claim. We might ask, however, about just how much of this critique is prompted by observations of privacy violations in the United States, a country that uniquely relies on the self-assertion of claims of privacy violations, and litigation through the courts? In almost every other advanced industrial state, these claims can be mediated

through a privacy or data protection agency which receive and investigate complaints from individuals from all walks of life, and which attempt to act on behalf of the data subject in opposition to the large data controllers.

Furthermore, and perhaps predominantly, the actions of these authorities are often directed towards a more general, or policy, level. They do try to act on a larger canvass, consulting with organizations about the development of products and services, insisting on privacy impact assessments, advising governments about new legislative and regulatory measures, auditing information systems, educating citizens as to their rights and responsibilities, and negotiating codes of practice with industry associations (Bennett and Raab 2006, 135-143). Their effectiveness in these roles is, to be sure, limited and variable. But my point is that many of these actions are motivated by the public interest in controlling excessive surveillance, rather than by the private interests in privacy protection. And the fact that privacy claims, in the forms of complaints or litigation, are inherently limited and limiting is not necessarily a valid indictment of privacy law *per se*. Regulators can and do act in the absence of action by an injured party. Actions by the individual are not a necessary condition for triggering regulatory action.

Moreover, and in contrast to the arguments by Haggerty and Gilliom above, some scholars have contended that the 'rights' dimension needs to be reinstated into privacy discourse, objecting to the commodification and commercialization of the issue through mechanisms of exchange and certification (Davies 1997). Others have objected to the ways in which the more technocratic language of data protection has transplanted the human rights emphasis inherent in the history of privacy protection. These narrower conceptions have gradually displaced 'broader — and potentially more empowering — discourses rooted in a human rights model that seeks to protect human dignity and democratic freedoms in the surveillance society' (Steeves 2008, 192). So for some, privacy's definition as a human right is limiting and marginalizing. For others it is empowering.

The problem is discrimination, not privacy

A related tack is taken by those who contend that the concept and policies of privacy never challenge the larger questions of categorical discrimination. Individuals are arguably placed at risk because of their membership in, or assignment to, certain groups, rather than on the basis of their individual identities and the personal information it generates. According to Oscar Gandy, the problem is better articulated as 'the panoptic sort' — 'a difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technology that allocates options and opportunities on the basis of those measures and the administrative models they inform' (Gandy 1993, 15). For Gandy, the problem is not the invasion of privacy through the collection of *personal* information, but the classification and assessment of that information according to prior assumptions and standard operating procedures. The result is enormous power imbalances, and discrimination based on *classes* of persons, rather than on individual 'data subjects'. Similar arguments are presented in his more recent work on the application of probabilistic and statistical logic to an ever-widening number of life decisions that reinforce and widen social and racial inequalities (Gandy 2009).

These same themes were taken up by Lyon in 2003, who rearticulated the problem as 'surveillance as social sorting': 'Surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice' (Lyon 2003, 1). An important theme for Lyon and Gandy is that of routinization. Data are extracted from people in everyday circumstances as they engage in a variety of informational transactions. Data doubles, or 'digital personae' (Clarke 1994) are created which in themselves mutate: 'But the data doubles, created as they are from coded categories, are not innocent or innocuous virtual fictions. As they circulate, they serve to open and close doors of opportunity and access'

(Lyon 2003, 27). In this new reality, the insistence that individuals should have a right to control the circulation of information that relates to them goes nowhere to address the deeper discrimination.

While not rejecting these categorizations of contemporary surveillance, I do again come to a partial defence of the concept and practices of privacy protection. In my reading, there are two implications of the surveillance and social sorting argument that need to be analyzed. The first is that the panoptic sort necessarily operates in secret. It relies on a level of mystification and complexity. One of the main purposes of privacy protection policy, however, is to render such processes transparent. There are several mechanisms within the privacy regime designed to achieve that goal. Organizations are expected to be open about their policies and their practices, and to notify individuals of the purposes of collection, and the logic of the personal data processing. They must grant access to individuals for their personal information, and an ability to correct it if necessary. To be sure, many of these obligations are nothing more than hollow commitments — but not always. In 2010, there was a huge backlash against Google for its new social networking tool, Google Buzz. The resistance has been framed in terms of privacy, and the presumed lack of transparency to the dissemination of friends for those with Gmail accounts. Google revised its product. Of course, Google is watched, and most companies are not. But the implication of this analysis is that major corporations can, and do, get in trouble when they are perceived to be collecting and processing personal information surreptitiously in order to build their vast marketing databases and thus enhance advertising revenue. When companies are watched, the 'panoptic sort' can be revealed.

A second implication of social sorting relates to the argument that privacy addresses the problems of discrete individuals, rather than categories of people. It is argued to be somewhat oblivious to distributional questions. Who gets what privacy, or who gets what surveillance, are questions that the privacy regime tends not to address, let alone remedy. At a governance level, however, there is plenty of evidence that laws and other policy instruments are being designed with sensitivity to the particular invasions and problems experienced by categories of people and the data they generate. For example, laws do contain particular protections for 'sensitive' categories of data. The 1995 Data Protection Directive, upon which all European laws should be based, permits member states to impose more stringent rules on the processing of: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sexual preference. The explicit assumption behind these provisions is the fear of discrimination on the basis of race, ethnic origin, political affiliation, religion, trade union membership, health and/or sexual orientation.

Many regulators have attempted to target their advice and assistance to particularly vulnerable subpopulations within their jurisdictions, be it aboriginal groups in Australia and Canada or immigrant groups in Europe. Indeed, it is very difficult to determine any contemporary privacy issue that is not, in some way, implicated by issues of categorical discrimination and concern for the impact of surveillance on vulnerable groups. For example, one common complaint about the construction of databases without appropriate access controls, is the potential for stalking, particularly of young women. Cases have been documented with respect to airport surveillance practices, university records-systems, health databases, population registers, social-networking sites and many others. This one example, and many others could be cited, suggests that the realm of privacy law is not about protecting an undifferentiated population of 'data subjects'. Questions about the distribution of privacy risks are implicit, and often explicit, in almost every complaint received, investigation conducted, and report written by the world's data protection authorities.

Privacy is too 'narrow'

Implicit in each of the above critiques is the argument that privacy is, in fact, too narrow. Despite its conceptual confusion and vagueness, it still leaves aside a number of crucial questions that surveillance scholars take very seriously. At this level, however, the critique is more often pitched at the propensity of

privacy protection policy to reduce any issue to *informational* terms and to the definition of successful privacy governance in terms of the application of the 'fair information principles (FIPS)' doctrine (Bennett and Raab 2006, 12). Over time, national and international policy has converged around these principles, on the assumption that any surveillance must involve a moment of capture of personally identifiable data. The approach is arguably reductionist and over time a number of different critiques have emerged.

First, the problem of determining the point at which information becomes personal information is increasingly difficult to determine. Advances in 're-identification science' have exposed the faulty assumption that privacy can be protected so long as data are anonymized by 'stripping' known identifiers (Ohm 2010). Thus, individuals might have an interest in their personal data when it is identified, identifiable, partially identified, non-identified, or any at any point along that complex and multi-dimensional continuum. For Ohm, the theory of fair information principles, based on an assumption that there is a clear difference between personal information and non-personal information, requires a broader risk assessment approach which is sensitive to sector and context.

Secondly, the FIPS can be insensitive to the means of extraction and capture. More than a decade ago, Gary Marx attempted to reformulate the FIPS doctrine into a broader set of ethical principles for the new surveillance. He contended that the FIPS doctrine is 'almost three decades old and needs to be broadened to take account of new technologies for collecting personal information such as drug testing, video cameras, electronic location monitoring and the internet' (Marx 1999). Crucially, he argued that the ethics of a surveillance activity must be judged according to the means, the context and conditions of data collection and use. According to Marx, the FIPS doctrine is insensitive to the question of violations and trust, and the ethical dilemmas inherent in particular techniques of information extraction that might cross sensitive boundaries. Ian Kerr describes an 'Ick factor' associated with certain contemporary implant technologies (Kerr 2009).

This critique is particularly telling insofar as the body is concerned. Recent advances in biometric technologies have convinced some scholars that bodily boundaries are being redefined. Irma van de Ploeg, for instance, persuasively contends that dominant legal privacy frameworks tend to reduce the various intrusions to an informational dimension, whereas the real problem is better framed more fundamentally as bodily integrity. There is a forced integration of bodies and information systems and 'far less stringent criteria apply to what counts as a legitimate violation of privacy, compared to what is needed to justify a breach of bodily integrity'. She contends that these are profound ontological shifts over the demarcation of where the body itself stops, meaning that the 'moral and legal vocabularies will no longer suffice' (van der Ploeg 2003, 67). In a similar vein, Roger Clarke argues that 'biometric technologies don't just involve collection of information *about* the person, but rather information *of* the person, intrinsic to them. That alone makes the very idea of these technologies distasteful to people in many cultures, and of many religious persuasions' (Clarke 2001, emphasis in original).

Thirdly, power relations are present between the watcher and watched even when personal information is not captured. Take CCTV for example; cameras do not have to be monitored to change behaviour. They do not even have to be operational. The prospect or potential for surveillance is often enough to change behaviour. This, of course, is the crucial point about the panopticon, and its extension to modern forms of surveillance. 'Data subjects' might not be monitored at any one time, but they would be well advised to behave is if they were. Thus, privacy protection law and policy simply does not apply if the cameras are off or if the personal information is not collected. Similar dilemmas attend the capture of information by ubiquitous computing devices, remote sensors or drones. Yet each of these devices structure power relations and imbalances between individuals and between individuals and organizations.

It is in these examples that we find, I think, the crucial point at which privacy analysis ends and surveillance analysis begins. If some other structure simply does not collect personal information on the individual, it is difficult to contend that a 'privacy problem' *per se* arises. Yet power is, and can be exercised, without any capture of personally related data, anonymized or otherwise. No law or regulatory authority could possibly hold this form of surveillance to account under the guise of protecting privacy. And yet, if surveillance is a form of power, it is surely necessary 'to consider how that power is held to account and what limits are placed on its operation' (Norris and Armstrong 1999, 10).

Conclusion: Privacy is 'Cool' Too

Privacy is not the 'antidote to surveillance' nor was it ever meant to be. But privacy has come a long way — conceptually and politically. It has been disaggregated, refined and contextualized. Some formulations have been declared narrow or culturally specific. Others have been declared so broad that they are virtually indistinguishable from related concepts, such as liberty or autonomy. The concept has been expanded to a point where Solove declares that it is 'a concept in disarray' (Solove 2008, 1). Like 'surveillance' it is not clear what it means, and it is not clear what it does not mean. In the effort to fashion concepts that will travel and be relevant across cultures both ideas have been victim to what Sartori (1970) calls 'conceptual-stretching'. For both, it is becoming impossible to identify the range of empirical referents or observables that should fall within their scope.

Arguably, I have summarized and categorized a complex critique which does not do justice to the richness of these arguments. My overall impression, however, is that they address a conception of privacy which is dated, and a framing of the issue which is only partially related to what privacy protection means in practice, and what privacy regulators do in their day-to-day work. Thus, each critique is an important contribution, but none really challenges the concept and regime of privacy *in toto*. And none persuasively argues for a more effective way to redress the power imbalances between the hapless subject and the large organizations employing the latest information technologies.

Despite the slipperiness of the concept, 'privacy' does frame the contemporary political and social issue, both in the English-speaking world and elsewhere. It envelops a complicated network of private and public sector actors who engage in overlapping domestic and international regimes — privacy commissioners, chief privacy officers, privacy consultants, privacy advocates. It frames the many international, regulatory, self-regulatory and technological policy instruments all of which contribute to the 'governance of privacy' (Bennett and Raab 2006). It describes the policy tools: privacy impact assessments, privacy management tools, privacy accountability frameworks, privacy policies, privacy codes, privacy standards, and so on. It has also taken its place as a critical trade-related question to be resolved within the interplay of broader forces and interests in the international political economy (Newman 2008). It animates civil society activism and resistance (Bennett 2008). And it frames the scandals and conflicts in the public and media realm. As a concept, and as a regime, it has come a long way in forty years.

The most pressing challenge is clearly with enforcement and implementation. And here, I have considerable sympathy with the critics. Privacy protection policy is flawed. Laws are often weakened by broad exemptions, especially for law enforcement. The regulators generally have few resources, and many do not have the real independence from government or business, preventing them from acting as real privacy advocates. Self-regulatory schemes, such as privacy codes, policies, seals, standards, regularly suffer from the perception that the organizations responsible for compliance are also those with the greatest to gain from the uncontrolled processing and dissemination of personally related data. The governance of privacy is always under attack from powerful public and private interests eager to use the latest information technologies in the name of risk management or profit accumulation.

More broadly, contemporary information privacy legislation is often designed to manage the processing of personal data, rather than to limit it. From the perspective of those interested in understanding and curtailing excessive surveillance, the formulation of the privacy problem in terms of trying to strike the right 'balance' between privacy and organizational demands for personal information does not address the deeper issue and cannot halt surveillance. The privacy regime may produce a fairer and more efficient use and management of personal data, but it cannot control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information (Rule et al. 1980). According to Jim Rule, this has led to the paradoxical situation where there are more privacy rules — and less privacy (Rule 2008).

I do argue, however, that there is little wrong with the idea of forcing organizations to abide by the common set of fair information principles. Put it this way, *if* all organizations followed the OECD's 1981 Guidelines on the protection of privacy, with all their limitations, gaps, anachronisms, exemptions, there would be less surveillance in the world. The regime and the policy instruments it contains can plainly address many, though not all, of the social problems captured by the word surveillance, and there are sufficient examples where the more intrusive practices have been curtailed. Success is contingent, however, on a number of conditions: the content of law, the strength of the regulatory authority and its leader(s), the commitment of organizations, market incentives, the actions of a vigilant and concerned citizenry and the ability to design privacy into new systems (Bennett and Raab 2006, 264). It is also crucially contingent on the work and activism of the 'gatekeepers' — the privacy advocates and activists who can articulate the broader public interest in privacy protection and warn constantly of the drift into the surveillance society (Bennett 2008).

In this latter respect, there are unfortunate implications to the critique of privacy protection. The skepticism about privacy tends to promote a certain passivity and reluctance to engage in the messy debates over the rules, and the implementation and enforcement of those rules. Lyon sees a similar tendency: 'Legal measures do need overhaul from time to time, and everyone concerned about surveillance would do well to see this as an arena of "surveillance struggle"' (Lyon 2007, 176). If privacy is not the antidote to surveillance, then why bother trying to improve privacy laws, or attempting to hold government and business accountable using those rules? With such scepticism, there is a propensity for government and business to get away with practices that should be questioned and resisted. It is left to a few brave privacy advocates to do the really hard empirical work of comparing practice to norms, and of holding the processing of personal data to account.

Realistically, without privacy regimes, there would be few if any actual mechanisms of social redress for public and private wrongs. And sometimes, the policy regimes *do* have positive results. The recent complaint about Facebook, for example, by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) produced a largely critical finding by the Canadian Privacy Commissioner and forced the company to change its practices (Privacy Commissioner of Canada 2009). Detailed empirical work on self-regulatory privacy schemes *can* expose the obvious gaps and contradictions between wild claims about 'privacy friendliness' and the troubling details of privacy practices. Chris Connolly's work on privacy seal systems, such as Truste, as well as on the Safe Harbor regime, is an excellent example (Connolly 2008).

There are many legal and non-legal rules about privacy protection. Some are strong, and others are weak. Any public statement or commitment to privacy protection, however qualified, provides an opportunity to test whether words are supported by actions and practices; whether organizations say what they do, and do what they say. Experience from other issues also suggests that the broader the network, the easier it is to 'shop around' for opportunities to challenge surveillance practices. If a law in one country does not offer an opportunity to challenge the practices of a multi-national company, then the network might use actors located in another and broaden the opportunities for collective action (Keck and Sikkink 1997).

For younger scholars in particular, perhaps privacy simply is not 'cool'; surveillance is. Poring over laws, reports, guidelines, standards or privacy policies is not 'cool' either; interpreting the latest technologies and practices through the lens of post-modern social theory is. Responding to consultative exercises, or preparing for hearings, or registering complaints is not 'cool'; resistance is. Engaging with the crucially important contemporary debates about how, practically, to make consent meaningful on the internet is not 'cool'; deconstructing the ontological assumptions behind the very notion of consent, is. Coming to grips with cookies, deep-packet inspection, cryptography, spyware, protocols, and other opaque instruments of network management is not cool either; constructing metaphors about 'cyber-surveillance' is.

In conclusion, it is obvious that for all the academic critique, 'privacy', as a concept, as a regime, as a set of policy instruments, and as a way to frame advocacy and activism, is not going to disappear. On the contrary, it displays a remarkable resilience as a way to regulate the processing of personal information by public and private organizations, and as a way for 'privacy advocates' (Bennett 2008) to resist the excessive monitoring of human behaviour. Like it or not, privacy frames the ways that most ordinary people see the contemporary surveillance issues. Surveillance scholars have got to live with it.

References

Aas, K.F., H.O. Gundhus, and H.M. Lomel. 2008. *Technologies of Insecurity: The Surveillance of Everyday Life.* London: Routledge.

Allen, A. 1985. *Uneasy Access: Privacy for Women in a Free Society*. Totowa, NJ: Rowman and Littlefield.

Bailey, J. and I Kerr. 2007. Seizing Control: The Experience Capture Experiments of Ringley and Mann. *Ethics and Information Technology* 9(2): 129-139.

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

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

Clarke, R. 1994. The Digital Persona and its Application to Data Surveillance. http://www.rogerclarke.com/DV/DigPersona.html (accessed 11 March 2011).

Clarke, R. 2001. Biometrics and Privacy. http://www.rogerclarke.com/DV/Biometrics.html (accessed 11 March 2011).

Clarke, R. 2006. What's Privacy. http://www.rogerclarke.com/DV/Privacy.html 2006 (accessed 11 March 2011).

Connolly, C. 2008. *The US Safe Harbor: Fact of Fiction*, Galexia. http://www.galexia.com/public/research/articles/research_articles-pa08.html (accessed 11 March 2011).

Davies, S. 1997. Re-Engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity. In *Technology and Privacy: The New Landscape,* eds P. Agre and M. Rotenberg. Cambridge: MIT Press.

DeCew, J. 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology.* Ithaca: Cornell University Press.

Etzioni, A. 1999. *The Limits of Privacy.* New York: Basic Books.

EU Data Protection Directive. 1995. *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data,* Brussels, OJ no. L281, 24 October 1995.

Fried C. 1970. Privacy. *Yale Law Journal* 77: 475-493.

Gandy, O.H. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder: Westview.

Gandy, O.H. 2009. *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* Aldershot: Ashgate.

Gavison, R. 1980. Privacy and the Limits of the Law. *Yale Law Journal* 89: 421-471.

Gilliom, J. 2001. *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy.* Chicago: University of Chicago Press.

Gilliom, J. 2006. Struggling with Surveillance: Resistance, Consciousness and Identity. In *The New Politics of Surveillance and Visibility*, eds K. Haggerty and R. Ericson. Toronto: University of Toronto Press.

Glendon, M.A. 1993. *Rights Talk: The Impoverishment of Political Discourse.* New York: Free Press.

Haggerty, K.D. and R.V. Ericson, eds. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

International Conference of Privacy and Data Protection Commissioners. 2006. Closing Communique: http://www.privacy.org.nz/28th-international-conference-of-data-protection-and-privacy-commissioners (accessed 11 March 2011).

Keck M. and K. Sikkink 1998. *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Kerr, I. 2007. 'Still Feeling Icky', Presentation available at: http://www.idtrail.org/content/view/364 (accessed 11 March 2011).

Lyon, D. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.
Lyon, D., ed. 2003. *Surveillance and Social Sorting.* London: Routledge.
Lyon, D. 2007. *Surveillance Studies: An Overview.* London: Polity.
Marx G. 1999. 'The Ethics of the New Surveillance'. In *Visions of Privacy: Policy Choices for the Digital Age*, eds C. Bennett and R. Grant. Toronto: University of Toronto Press.
Murakami Wood, D. 2009. Situating Surveillance Studies. *Surveillance and Society* 19: 52-61.
Newman, A. 2008. *Protectors* of *Privacy*: *Regulating Personal Data in the Global Economy.* Ithaca: Cornell University Press.
Nissenbaum, H. 2009. *Privacy in Context.* Palo Alto: Stanford University Press.
Norris C. and G. Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.
Ohm P. 2010. 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' forthcoming, 57 UCLA Law Review 1701.
Organization for Economic Cooperation and Development (OECD) 1981. *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD.
Poster M. 1990. *The Mode of Information*. New York: Polity Press.
Privacy Commissioner of Canada. 2009. Facebook Agrees to Address Privacy Commissioner's Concerns. http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm (accessed 11 March 2011).
Regan, P. 1995. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.
Rule J. et al. 1980. *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. New York: Elsevier.
Rule, J. 2008. *Privacy in Peril*. Oxford: Oxford University Press.
Sartori G. 1970. Concept Misformation in Comparative Politics. *American Political Science Review* 64: 1033-53.
Simitis, S. 1978. Reviewing Privacy in the Information Society. *University of Pennsylvania Law Review*. 135: 707-746.
Solove, D. 2008. *Understanding Privacy.* Cambridge: Harvard University Press.
Stalder, F. 2002. Privacy is not the Antidote to Surveillance. *Surveillance and Society* 1: 120-124.
Steeves, V. 2008. Reclaiming the Social Value of Privacy. In *Lessons from the Identity Trail,* ed. I Kerr. Oxford: Oxford University Press.
UK Information Commissioners Office. 2006. *A Report on the Surveillance Society*. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.
UK, *The Times*. 2004. 'Beware Rise of Big Brother State', August 16th.
US. Privacy Protection Study Commission. 1977. *Protecting Privacy in an Information Society.* Washington DC: Government Printing Office.
Van de Ploeg, I. 2003. Biometrics and the Body as Information: Normative Issues of the Socio-technical coding of the Body. In *Surveillance as Social Sorting*, ed. D. Lyon. London: Routledge.
Warren, S. and L. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4:193-220.
Westin, A. 1970. *Privacy and Freedom*. New York: Atheneum.

Surveillance & Society

Debate

Response to Bennett: Also in defence of privacy

Priscilla M. Regan

George Mason University, USA. pregan@gmu.edu

Privacy has always been a messy, complicated, and rather vague concept. It has been in 'disarray' since earliest attempts at definition. But that's OK—and similar to a number of other powerfully important concepts, such as freedom, liberty, and justice. That alone should not dissuade us from its use and value. The question then is, does it still capture a meaning that is valuable to us in the 21st century and does its usage in public and philosophical discussions help us to understand and address important human and social issues. To this I simply answer yes and join Bennett in defending privacy. My defence, however, proceeds a bit differently, as might be expected, to help further the privacy and surveillance community's shared, but not new, conversations about this topic.

I believe that defining contemporary problems associated with governmental and nongovernmental activities of monitoring and recording peoples' actions, behaviours and communications is best done by speaking in terms of 'surveillance' not 'privacy invasion'. In this sense then I disagree with Bennett that privacy is an effective way to frame the contemporary problem. The scale and scope of the problems exist at a systemic level (institutions, social practices, fabric of modern life) not at the level of private space (invading one's house, taking pictures from a distance, over-hearing a conversation between two parties). The phrase 'privacy invasion', as it is commonly used and understood, is too limited to encompass what has become a distinguishing and disquieting feature of modern life. Surveillance as a concept, as an image, more accurately connotes the modern landscape.

Surveillance as a definition of, or frame for understanding, the policy problem is far more powerful than privacy because the way we define a problem affects what policy options are best for addressing the problem. Privacy definitions elicit policy options that focus primarily on giving individuals 'rights of control', based largely on the thinking of Warren and Brandeis (1890) and Alan Westin (1967) and developed in the mid 1960s at the time that society was moving from paper records to large computerized databases—not a time of decentralized data capturing literally every movement on mobile, wireless devices and putting that information up for grabs on the internet. As Bennett and others rightfully point out, the fair information practices, developed in response to privacy definitions of the problem, are generally weakly enforced, rely upon individual initiative, and narrowly cast the problem. Surveillance definitions elicit broader social, institutional practices and enforcement—ones that are more likely to effectively respond to the problem.

But although the problem is best defined in terms of surveillance, the social and individual value that is at risk from surveillance is still best captured by privacy. Surveillance is not just a problem because it involves monitoring and tracking of individuals but because surveillance practices affect the panoply of concerns that we have bunched together under the powerful concept of 'privacy'. Surveillance is an

Regan, P.M. 2011. Response to Bennett: Also in defence of privacy. *Surveillance & Society* 8(4): 497-499.
http://www.surveillance-and-society.org | ISSN: 1477-7487

activity or set of activities that are of concern to societies for reasons, and privacy provides, perhaps not the perfect, but the most robust and concise understanding of the reason we are, and should be, concerned. 'Everyday surveillance' (Lyon 2001) and the 'panoptic sort' (Gandy) have indeed created the 'digital person' (Solove 2004). We mediate most of our daily existence through digital, wireless, mobile systems. The surveillance activities accompanying these have fundamentally changed the relations of people and institutions, and increasingly of people and other people. So how do we understand that fundamental change? And I would argue that even in the 21st century our human, and perhaps predominantly liberal, understanding of that change has to do with some intuitive, conceivably innate, sense of the relationship of self within the larger society—an understanding that is generally understood as involving the value of privacy.

I agree, however, with Bennett and others (Lyon 2001; Haggerty and Ericson 2006; Allen 1985) who criticize an individualistic conception of privacy. As Bennett notes, I have argued that privacy is also a common value, a public value, and a collective value—and that when we are talking about privacy we are also talking about 'the larger questions about the kind of society we are building,' as Bennett states in his essay. Similarly Steeves refers to 'a social construction that we create as we negotiate our relations with others on a daily basis' (Steeves 2008, 193). These relationships between individuals and modern organizations are enormously complicated and now almost universally are mediated by, or occur within, socio-technical systems. Moreover, as Bennett and Nissenbaum (2009) point out, privacy is not simply about a 'bubble' around the self but about this social, relational, and contextual complexity.

And if we recognize that privacy encompasses more than the flow of information from the individual to others but also the relationships of which individuals partake, then the problem of monitoring and tracking individuals (surveillance) within those relationships entails a solution that targets these surveillance practices. This dovetails with Bennett's criticism of 'fair information practices' as the quintessential solution. Instead the solution becomes much more focused on the way these relationships are structured, understood, and most importantly held accountable. This means looking at these relationships as entailing power—as has also been recognized by those (such as Lyon 2001; Norris and Armstrong 1999) who start with a surveillance perspective. Privacy enters the discussion because it provides one of the key values available to hold power accountable. Privacy involves a constraint on the use of power—a rationale for setting limitations on its exercise. And, as has been noted since the beginning of our discussions of privacy and surveillance, information is a source of power. Within systems where accountability is expected and valued, justifications are required for uses of power and these justifications are necessary *ex ante*.

So, do we need a concise definition of privacy that conveys its larger social importance? Or is such a definition sufficiently recognized in our previous discussions of a social, collective and public value of privacy (Regan 1995; Simitis 1978), or of contextual integrity (Nissenbaum 2009), or of privacy as a social construction (Steeves 2008)? Where should surveillance and privacy scholars best spend their time —on framing the problem, on defining the concept or value to be protected, or on developing solutions? I recognize that this is all integrated but also recognize that finding a perfect conceptualization of the value may distract us from developing and analyzing options for responding to the problems involved.

However some attention to a more clear conceptualization of privacy in light of the current social and technical realities is essential and Bennett's piece nicely charts a path for our community. In my view, the need is for reinvigorating privacy not creating a new concept. Although I note the significance of a human rights basis for privacy, I would abandon the notion of an individual right to privacy—agreeing with Bennett's analysis, as this approach appears to have muddled the territory—and instead emphasize that the human rights justification supports a more social orientation for privacy. A human rights justification is entirely consistent with arguments for common, public and collective importance of privacy. Pitting the individual as citizen, consumer, friend or enemy against the organizational forces of society has become unhelpful and distracting.

Similarly, the public-private dichotomy is too simplistic to represent the range of relationships that individuals have with other people and organizations. Instead, the conceptual foundation for privacy in today's world should be its social, or societal, value. On the individual level, people may perceive they have different privacy preferences; but on the societal level, people require some measure of, and understanding of, how they can relate to others in a way that permits the development of a sense of self and connectedness to others within the society of which they are a part. This harkens back to a conception that Ferdinand Schoeman articulated in 1992 of privacy as protection against 'social overreaching,' limiting the control of others over our lives but also permitting us to participate in our social lives (1992, 1). The notion of overreaching well incorporates the importance of accountability, of privacy as a restraint on the use of power, and of the concerns that both privacy and surveillance scholars have been talking about for fifty-odd years.

References

Allen, A. 1985. *Uneasy Access: Privacy for Women in a Free Society.*Lanham, MD: Rowman and Littlefield.

Gandy, O.H. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Boulder: Westview Press.

Haggerty, K.D. and R.V. Ericson (eds). 2006. *The New Politics of Surveillance and Visibilit*y. Toronto: University of Toronto Press.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Palo Alto: Stanford University Press.

Norris C. and G. Armstrong. 1999. *The Maximum Surveillance Society: The Rise of CCTV.* Oxford: Berg.

Regan, P. 1995. *Legislating Privacy: Technology, Social Values and Public Policy.* Chapel Hill: University of North Carolina Press.

Schoeman, F. 1992. *Privacy and Social Freedom.* New York: Cambridge University Press.

Simitis, S. 1978. Reviewing Privacy in the Information Society, *University of Pennsylvania Law Review* 135: 707-746.

Solove, D. 2004. *The Digital Person: Technology and Privacy in the Information Age.* New York: New York University Press.

Steeves, V. 2008. Reclaiming the Social Value of Privacy, in I. Kerr (ed.) *Lessons from the Identity Trail.* Oxford: Oxford University Press.

Warren, S. and L. Brandeis. 1890. The Right to Privacy, *Harvard Law Review* 4: 193-220.

Westin, A. 1967. *Privacy and Freedom.* New York: Atheneum.

Surveillance & Society

Debate

A response to Bennett's 'In defence of privacy'

John Gilliom

Ohio University, USA. gilliom@ohio.edu

Introduction

Colin Bennett has written a thoughtful and enlightening article that is sensitive to both context and nuance; it advances valuable arguments in a balanced and engaged presentation that is sure to become a widely assigned and cited reference point in the field. Opening with the recognition that much contemporary surveillance scholarship has gone post-privacy, Bennett advances a 'defence of privacy as a way to frame the contemporary problems, as a regime of governance and as a set of practices'. What I read as his larger message is a case that privacy is actually more intellectually relevant to Surveillance Studies than it gets credit for and a plea for Surveillance Studies to stay relevant by maintaining its participation in the discourse of privacy. It advances, then, a request that Surveillance Studies comes home to privacy. To that, I must say, 'No, thank you'.

In the last two decades, the cohering field of Surveillance Studies has been shaping a vibrant paradigm for understanding and explaining surveillance. Surveillance Studies is now a robust interdisciplinary field that is, in many senses, defined by its movement away from the privacy/public law scholarship that defined the early phases of research and advocacy on surveillance issues. We are at a stunning confluence of rapid technological and social change, improving theoretical understandings, and self-consciously expanding scholarly networks. Much of our work has necessarily entailed going beyond and sometimes against the longstanding discourse of the privacy regime as new issues and intellectual framings come to the fore. We do not yet know how the journey will end, but one thing is sure: turning back to the privacy regime is the wrong way to go.

First, let me note that it is not 'privacy' that should be done away with, but the *regime* of privacy. By this, I mean, the *intellectual* regime which insists that privacy be the central theme or even the very terrain for every discussion of surveillance. Privacy is an important part of what we study, but we must and we are moving quickly away from an era in which it was the defining element of the field. The fact that we now have a leading scholar in the leading journal arguing for its salvation underscores the progress that has been made. But the mission of post-privacy scholars is not and really cannot reasonably be to remove privacy from the field of study—the mission has been (at least for me) to remove it from its position of intellectual and political monopoly. In the end, it is my belief that research-oriented participants in the field will do best to keep privacy in its proper place—as one part of the cultural politics of surveillance, but not as the organizing matrix for the field.

Space limitations prohibit a detailed engagement with this ambitious and far-reaching essay, so I here focus on three moments in the work: the conceptual defence of privacy as an intellectual tool; the realist

Gilliom, G. 2011. A response to Bennett's 'In defence of privacy'. *Surveillance & Society* 8(4): 500-504.
http://www.surveillance-and-society.org | ISSN: 1477-7487

defence of privacy as *the* way that people see surveillance; and the pragmatist defence that privacy is an effective tool for limiting the spread of surveillance.

1. The conceptual defence

Much of the Bennett's essay is a dialogue challenging several of the central critiques of privacy as an intellectual concept—the lead items are the arguments that privacy is hyper-individualistic, spatial, legalist, blind to discrimination, and, in the end, simply too narrow to catch the richness of the surveillance experience. The general sway of each section is to introduce the critique, acknowledge the validity of the concerns, point to some ways in which the critique misses the evolving nuances of contemporary scholarship and policy, and close with a defence of the privacy paradigm. Along the way, students of surveillance gain a well-explained tour of key points of contention in the privacy debate.

But even when I am persuaded that there is particular evidence that some contemporary privacy scholarship or policy has actually responded to and improved from the longstanding critiques, I remain unconvinced that the general sway and tenor of the privacy paradigm does not remain hyper-individualistic, spatial, legalistic, blind to discrimination, and, in the end, simply too narrow to catch the richness of the surveillance experience. These concerns cannot be solved with a few upgrades. The defence of the intellectual ground held by the privacy regime also tends to overlook that fact that there are many (some yet unimagined) dimensions to the impact and powers of surveillance that simply don't fit the privacy framework. At one point, Bennett recognizes this when he notes that privacy discourse is not helpful when we consider something like the social impact of non-operative but potential surveillance. With no viable privacy concerns raised, he finds a 'crucial point at which privacy analysis ends and surveillance analysis begins'. Maybe I just get to that point a lot earlier.

The conceptual section is summarized, in part, with the observation that 'each critique (of privacy) is an important contribution, but none really challenges the concept and regime of privacy *in toto*'. My response to the point-by-point defence is that each defence is an important contribution, but none really *salvages* the concept and regime of privacy *in toto*. This is, in large part, because the problem is not so much the specific points, but the impact of the regime *in toto*. This intellectual monopoly is the central problem and it cannot be argued away with examples of updates.

2. The realist defence

Bennett argues: 'Like it or not, privacy frames the ways that most ordinary people see the contemporary surveillance issues. Surveillance scholars have got to live with it'.

This is probably one of the most important dimensions of the argument for having surveillance scholars take a sober second look at the privacy regime. But, upon reflection, I do not think that even agreeing with this statement about popular culture means that one agrees with the necessary dominance of the *regime* of privacy in our work as intellectuals. As I have noted, privacy is certainly a relevant part of at least some of our work because it 'frames the ways that most ordinary people see' surveillance. Because of this, privacy is a part of our subject matter. But, here, it must be stressed that popular perceptions of surveillance issues are only one part of a field encompassing all sorts of work dealing with technology, policy, theory, ethnography, and other agenda in fields as diverse as Sociology, Political Science, Anthropology, Criminology, and Science and Technology Studies. The argument that all of the scholars in all of these fields should submit to the ways that most ordinary people see things is precisely the sort of intellectual domination that we attempt to shed when we enter the post-privacy period of Surveillance Studies.

From a different perspective, I am also not sure that either one of the sentences quoted at the opening of this section is correct. For the first claim, about 'how most ordinary people see the contemporary

surveillance issues', there are a number of reasons to raise questions. First, though privacy obviously has a lot of polling power and is the go-to term for journalists, empirical research has demonstrated that there are at least some people out there who do not turn to the privacy framework to voice their concerns about surveillance (Gilliom 2001). When we interviewed welfare clients about their interactions with a new computerized finance, benefits, and eligibility surveillance system, they only said a little about privacy—they spoke more of fear, degradation, need, and struggle. These are issues that are simply far more relevant and pressing in a life removed from relatively abstract concerns about privacy. What would happen if we expanded this sort of research to use open-ended interviews and other means to get a sense for how people 'see' surveillance away from the confines of a pre-formatted public opinion poll? We should also consider the possibility that a big part of the reason that Bennett and I have different takes on these questions has to do with the locations and people we study. His recent work has been about and among the privacy advocates and their struggle with surveillance; I have no doubt that in such a context, the idea of privacy seems vibrant, alive, useful, and nuanced. My research has been among everyday people and their struggles with surveillance as one dimension of their troubles. Here privacy has less going for it: privacy concerns don't stack up well when competing with the hunger, fear, and homelessness that are part of a broader system of inequality that is complicit with systems of surveillance.

Furthermore, we also need to ask if 'most ordinary people' actually 'see' surveillance—frequently, they seem to be simply unconscious of the fact that they live in a surveillance-intensive condition called 'modern life'. When I first tell my students that their cell phone is a *de facto* location and interaction monitor or that each of their credit card transactions records a merchant code revealing the nature of their business, they are authentically surprised. They do not, in short, 'see' the contemporary surveillance issue, let alone put it in the terms of the privacy framework. So how do we work to help people 'see' the contemporary surveillance issues? This is an important point within the terms of Bennett's essay because political relevance is one of his central touchstones. Here, I believe that the predominance of the privacy regime may actually interfere with effective public education about the practices and politics of surveillance. Part of the problem is tied to the fact that 'privacy discourse' has become something like background noise in a complex cultural environment. I recall a brief news story on National Public Radio that ended by stating that '*privacy advocates argue that the new technology poses a threat to privacy rights*.' Does anyone really even *hear* that? Is it not the socio-political equivalent of elevator music hovering in some strange space between silence and meaningless presence? Privacy frames may be in rampant circulation, but I am not sure people use them to *see* much at all.

I am even more sceptical on the second point: 'privacy scholars have got to live with it'. I actually think that we may be obliged to kill it! I begin my seminars on the politics of surveillance with an informal discussion about different surveillance practices and whether or not they are of concern to my students. As we go, I quietly make a rough count of how many times the word 'privacy' pops up. It's a lot. We then talk about this and discuss the fact that surveillance *is not, in fact, the ontological antithesis of privacy*.[1] We may be trained to think this way (up:down, in:out, surveillance:privacy), but, I explain to my students, our work as intellectuals demands that we move away from the inherited regimes of thought, which (as Dewey reminds us) are necessarily inappropriate because they are inevitably mired in times and situation which no longer exist. As class proceeds, we follow the lead of PeeWee's Playhouse: anytime someone says the secret word, ('Privacy' or, as we come to call it, the 'P-word,') we all yell and scream and wave our arms in the air. By thus disciplining ourselves (using surveillance, of course) to discuss surveillance without the stultifying intellectual crutch of the privacy regime, we can begin to think afresh about the startlingly new phenomena we're confronting. And, in my experience, this is when surveillance can truly capture my students' imaginations. Really, how many more lectures, debates, articles, or paperback books

[1] See Torin Monahan's discussion in the opening essay of his Surveillance and Security: Technological Politics and Power in Everyday Life (Routledge, 2006).

need to harangue us about the tradeoffs between surveillance and privacy? Isn't it more productive help people rethink what is, after all, an unprecedented new framework of social control?

3. The pragmatist defence

In 2001, I published *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*, which studied the ways in which impoverished Appalachian women cope with new forms of surveillance in welfare administration. Those few readers who made it all the way to the end of the book encountered a personal epilogue describing my family's experience when local sheriff's deputies searched our home under the (incorrect) suspicion that we were growing marijuana on public land adjacent to our small farm. In the epilogue, I described how the idea of 'privacy' was simply not up to the job of conveying all the senses of anger, fear, and frustration; the parental concern; the realities of local politics; the disbelief; the absurdity; and the physical toll. Our cherished rights to privacy were also—according to two specialist attorneys—not up to the job of doing anything to help us take legal action. Sure, we could sue, but it would just waste a lot of time and money and yield no tangible result.

In this sense, I argued, my own experience ran somewhat parallel to the women interviewed in the book itself—they were articulate in their critiques of welfare surveillance, but they very rarely used the P-word and they certainly didn't file a lawsuit or call Privacy International. There are a lot of important ideas that can be teased out of our shared recognitions of the limits of privacy, but I want to focus on one very important one here. It is a point that is particularly important as part of a response to Bennett's essay because he places so much emphasis on representing a realist's perspective—privacy failed us.

Neither my family nor the women studied in *Overseers* had any meaningful prospect of using the right of privacy as a credible vehicle for improving our situation. I think that there are many reasons for this (and Bennett's essay explains them well): privacy is a weak argument in the face of overwhelming arguments for public safety, drug-control, accountability and welfare fraud control; privacy has a cultural weakness as a NIMBY like, me-first sort of value; privacy has, for the most part, become a *procedural* order, not a substantive guarantee: if the rules are followed (consent forms, warrants, boilerplate notifications) then the objections are null. This list could go on, but if the crux of the argument for saving privacy is a realist assessment that it is a powerful tool in the anti-surveillance arsenal, I am not persuaded. There are, for sure, examples of limited policy successes for the privacy advocates. But, just as surely, we could point to myriad examples where privacy has failed to erect any meaningful barrier or limit to new surveillance initiatives. And success at limiting surveillance is not something we should expect to see. Surveillance is a central organizing principle of our times and no mere counter-arguments are going to slow the broad progress of its sweep. Why then, shackle a vibrant intellectual movement in a bid for very tentative political relevance?

Conclusion

The key points I have attempted to make in this brief response are that privacy is not the problem, but the privacy *regime*; that the regime's now-slipping monopoly has hindered our understanding of surveillance; that the weakening of the regime is a necessary part of the flourishing of the field; and that the path to continued flourishing is to keep questioning or even ignoring the regime.

These points are, I believe, supported by the fieldwork that I presented in *Overseers of the Poor* which was, at its heart, an effort to hear the ways that people talk about surveillance in their daily lives. As I wrote then:

> (B)y paying attention to what people are saying and doing about these important public policy issues, we can build better and more inclusive accounts and understandings of societal concerns. 'Privacy' is a very important and meaningful thing to lots of people. This study suggests that meeting needs and taking care of others is too. And so, it seems clear, is a sense of personal dignity. By moving away from the discursive monopoly of the privacy paradigm we might begin to hear about things like need and care, or religious objections, or fears of concentrated powers, and other unimagined claims as well. And we might, as we add these differently critical voices and ideas to the conversation, begin to learn more about the politics of surveillance.
>
> (Gilliom 2001, 125*)*

References

Gilliom, J. 2001. *Overseers of the Poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.

Surveillance & Society

Debate | Dear Voyeur, meet Flâneur… Sincerely, Social Media

danah boyd

Microsoft Research and Harvard University, USA. e-mail: dmb@microsoft.com web: http://www.danah.org/

There are times and places where people like being watched. And there are times and places when people like watching. Technology brings the flâneur and the voyeur together in new ways, constructing multibillion-dollar industries that profit off of their symbiotic relationship. From reality TV to Facebook, the flâneur and the voyeur come together to see and be seen. Yet, for all that people like being watched and for all that people like watching, there are limits to their comfort. Critical questions commonly emerge: who's watching? For what purposes? What are the potential benefits or consequences of watching or being watched? These are precisely the questions that Surveillance Studies bring to bear.

Implicit in any conversation about surveillance is the issue of structural power. Institutions and entities watch people. Challenges to surveillance also tend to focus on responses to structural power, as people interrogate institutions and entities. Yet, there are different forms of power at stake when we think about the watcher and the watched. Most importantly, there is situational power. People hold power over each other not simply through authority but through their interaction dynamic at any given point in time, watching and then being watched. Some situations enable people to maintain power when watching while others require people to make themselves vulnerable in order to watch. Likewise, technologies enable different configurations and with different outcomes. What Facebook enables is quite different than what is made possible by reality TV.

When critics think about the production of reality TV shows or the creation of Facebook, they typically focus on the institutions behind these entities and, thus, focus on the structural power that can be abused. But when people talk about invasions of privacy on sites like Facebook, they are not just talking about structural power; in fact, more often than not, they're talking about situational power. They're talking about how people—including and, especially, people that they know—can hold power over them in a particular moment. They feel violated when they are taken out of context against the social norms that regulate the situation.

In his seminal book, *Code and Other Laws of Cyberspace*, legal scholar Larry Lessig (2000) argued that systems are regulated by four different regulatory pressures: the market, the law, code (or architecture), and social norms. Most conversations about privacy and surveillance focus on the role that the law can—or should—play in curbing abuses of privacy by the market and the government because of available technology. Social norms are bandied about as a justification for nearly any approach with rhetoric like 'Privacy norms are changing' and 'People do (or don't) care about privacy'. Yet, social norms—when contextually understood—highlight how privacy and surveillance are both being challenged by an increasingly networked society.

boyd, danah. 2011. Dear Voyeur, meet Flâneur… Sincerely, Social Media. *Surveillance & Society* 8(4): 505-507.
http://www.surveillance-and-society.org | ISSN: 1477-7487

Bennett's essay, 'In defence of privacy', clearly articulates how unclear privacy is as a concept and why privacy, in its slippery state, fails to serve as an antidote to surveillance. At a regulatory level, his argument is persuasive—operationalizing a term that no one can agree upon is impossible. Likewise, he responsibly highlights a simple reality: people like to think about, talk about, and work towards defining privacy. In short, privacy is 'cool' and, pragmatically, leveraging privacy discourse has its advantages. While I agree with Bennett's assessments, I would argue that there is an additional reason that surveillance scholars should engage with privacy discourse: its messiness actually has value.

In trying to describe different facets of privacy, Bennett highlights that one of the greatest weaknesses of discourse about privacy is that it's individual-centric. He uses Valerie Steeves' (2008) critique to highlight how privacy is a dynamic, socially constructed process. Meanwhile, he argues that surveillance offers a better angle with which to think about violations that aren't well captured by privacy, in part because surveillance provides a framework for thinking about groups and categories. Of course, Steeves' critique also applies to a surveillance model that is group-centric. To resolve Steeves' challenge, it becomes critical to not only understand the role of social interactions but also the networks in which people inhabit. Helen Nissenbaum (2009) captures this as 'context', but it is important to highlight that context, in her sense, is more than just a definition of the situation; it's about the relationship people have to people, information, technology, space, and time. People's understandings of privacy and surveillance are very much driven by position in the various networks, and their interactions with others are shaped by these relationships. Technology only makes the networks more salient, both to those watching and those being watched.

People develop different strategies to manage realities in which they are observed. While there is little doubt that surveillance affects people's behaviour (Foucault 1975), people are also quite creative in finding ways to manage being watched so as to achieve privacy. Let me offer two examples in the form of case studies derived from my ethnographic work:

> Case #1: Carmen, a 17-year-old Latina girl living in Boston, was having a bad day. She and her boyfriend broke up and she wanted her friends to know that she was feeling sad. Her first instinct was to post a sappy song lyric to her Facebook, but she decided against doing so out of fear that her mother would take it seriously and think she was suicidal. Instead, she chose song lyrics from 'Always Look on the Bright Side of Life' knowing that her mother wouldn't recognize the song or the reference while her friends would immediately recognize that this song was sung in 'The Life of Brian' when the main character was about to be executed.
>
> Case #2: Shamika, a 17-year-old black girl living in DC, found that Facebook was often the source of social drama at her school. After a fight in which a girl had taken older posts of Shamika's out of context to justify her bullish actions, Shamika decided that status updates should be ephemeral. Each day, she 'white walls' her Facebook profile, deleting comments left by others after she reads them and removing status updates or wall posts that are more than a day old. In this way, Shamika keeps a living profile on Facebook but undermines the norm of persistence.

Both Shamika and Carmen have accepted that they're being watched. That's part of why they like Facebook in the first place—they want the attention of being watched by people that they know and like. But just because they like being watched does not mean that they inherently want people that they know to hold power over them. Shamika focuses on limiting access to older content. She is perfectly aware of the fact that anyone could save her profile content and that Facebook itself most likely has a record of the content, but that's not the point. She's intentionally making access harder to reduce the drama that can

ensue when it is too easy to access content and take it out of temporal context. She's trying to achieve control, not invisibility.

Carmen is taking a different approach. She's not trying to restrict access to content, but trying to limit access to interpretation. This can best be understood as a 'social steganography' technique; Carmen is hiding in plain sight, assuming that anyone can access what she is saying but that only some people understand the meaning. She relies on the fact that her mother doesn't recognize song lyrics let alone bother to look them up: she takes text at face value. Meanwhile, Carmen also assumes that anyone who knows the Monty Python movie but doesn't know her won't understand why she's posting the lyrics in the first place. In controlling the meaning, Carmen asserts agency over the social situation.

What is at stake in any conversation about privacy or surveillance is not simply power but agency. When and to what degree can individuals assert agency over a situation? Consider the position of celebrities who are under constant surveillance by paparazzi and others who demand that they have the right to access them as public figures. When Angelina Jolie married Billy Bob Thornton, the press frenzy around her was intense. She willingly exposed many aspects of her life, fuelling the fire. At one point, a journalist asked Angelina about her decision to be so public and reject any privacy that she might possibly have. Angelina responded by telling the reporter that the best way to achieve privacy was to appear to be so public that no one bothered looking into areas that she wanted to protect. Celebrities can't escape being watched, but they can divert attention.

Social technologies are undoing the private-by-default, public-through-effort norm that average people have when walking through this world. Participation in digital social media often means public-by-default, private-through-effort. Being watched is simply part and parcel with participating. Rather than opting out or going 'off the grid', many participants are developing techniques to manage the dynamics that celebrities have faced for a long time—life under a constant state of surveillance. What gives them power is not technology or legal regimes, but agency.

In focusing on agency, it is possible to recognize the role of networks. People aren't simply individuals or in groups; they are members of social networks, connected by information, time, and space, and they must navigate life as a series of relationships. When people understand their position in the constellation, they can then achieve the very essence of what privacy is all about. Furthermore, only when they have agency can people respond rationally and responsibly to surveillance.

References

Foucault, M. 1975. *Discipline and Punish: The Birth of the Prison*. Paris: Editions Gallimard.

Lessig, L. 2000. Code and Other Laws of Cyberspace. New York: Basic Books.

Nissenbaum, H. 2009. *Privacy in Context:* Palo Alto: Stanford University Press.

Steeves, V. 2008. 'Reclaiming the Social Value of Privacy', in I. Kerr (ed.) *Lessons from the Identity Trail.* Oxford: Oxford University Press.

Surveillance & Society

Debate

Autonomy beyond privacy?
A rejoinder to Bennett

Felix Stalder

Zurich University of the Arts, Switzerland. e-mail: felix@openflows.com web: http://felix.openflows.com

When debating 'privacy' we need to distinguish, as Bennett does, between the concept—that is, the framing of the issue—and the regime—that is, the concrete policies and their enforcement in particular contexts. However, the discussion is in danger of becoming self-referential. We fail to consider the changing nature of the practices by which people, acting under various constraints, make personal information accessible to others. In terms of the regime, it is easy to agree with Bennett that we have to work strategically with whatever resources we have at hand within the landscape of constraints in which we happen to find ourselves. It is not much use to wish for a different world. Presently, the privacy regime is capable of mobilizing a powerful set of resources to strengthen ever-threatened individual and collective self-determination against the encroachment of, or manipulation by, powerful institutional actors. These appeals can be relatively effective because that regime privacy is relatively well embedded institutionally, legally, and discursively. It comprises numerous established actors, private and public. They can rely on a patchwork of existing laws, regulations and guidelines to legitimate their agendas, and make widely understood and well-resonating claims on behalf of the public by invoking the right to privacy. It would be foolish to give up such resources in exchange for, well, what? The lack of clearly articulated and implementable alternative is the strongest argument in favour of current privacy regime, and one that also its critics readily acknowledge. There is nobody within this debate—except for the proverbial straw man—that would not favour expanding, or even advocate weakening, the privacy regime.

In terms of the concepts, the problem begins with the lack of even a working definition of what is meant by privacy. Indeed, it seems to be characteristic of the current state of the debate that definitions are not even attempted any more. Helen Nissenbaum, in a recent and innovative attempt to update the concept, states early on that she does not aim to 'carve a pathway through the conceptual quagmire to claim a definition— [my] definition—of privacy' (2010, 3). The same goes for Bennett, who, in place of a definition, refers to Solove, stating that

> privacy is a convenient conceptual shorthand way to describe a cluster of problems that are 'not related by a common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element—they share family resemblances with each other'.

However, it remains unclear which problems constitute this particular cluster, or what their family resemblance might be.

Stalder, Felix. 2011. Autonomy beyond privacy: A rejoinder to Bennett. *Surveillance & Society* 8(4): 508-512.
http://www.surveillance-and-society.org | ISSN: 1477-7487

Bennett then goes on to defend the undefined concept against a number of common critiques. I focus on two of them to explain why I find the defence not particularly convincing. The first critique taken up by Bennett is that privacy is all 'about me, me, me', based on liberal notions of (possessive) individualism. Rather than defend this core element of the liberal conception of politics and civil society, as many continental European privacy advocates do very eloquently (see, for example, Rössler 2002; Sofsky 2008), he claims that the debates have moved beyond this liberal foundation by stressing that privacy is a social, political and thus collective value, rather than an individual one. He paraphrases Regan on the point that we must 'frame the question in social terms, because society is better off if individuals have greater levels of privacy'. In this, however, I cannot find an indication that the concept is moved beyond its individualistic core. Rather, it is simply an acknowledgement that questions of individuality are to be understood as historically and socially mediated, rather than as essentialist. As such, they are, of course, embedded in social processes, but it is precisely these collective processes that constructed the notion of privacy centring around isolated individuals and their ability to engage in 'a dynamic process of negotiating personal boundaries', as Bennett quotes Steeves. Thus, the defence offered here is a shift from a philosophical to a sociological argumentation that does not fundamentally change the central role of the liberal conception of the individual—now rooted in society and history rather than in 'a sort of state of nature'—to the concept of privacy.

The second point I want to address is the claim that the 'panoptic sort' necessarily operates in secret and that the privacy regime allows to make this transparent, leading to the claim that, thus 'when companies are watched, the "panoptic sort" can be revealed'. While this is not necessarily wrong—there are, of course, plenty of examples where companies had to change their policies after a public outcry over them. The problem is not only that this approach doesn't scale—as Bennett acknowledges—but, more importantly, that social sorting is increasingly communicated to the public as a service, capable of rendering personal and individualized relationships to large institutions. It is precisely here, in the 'positive' forms of social discrimination based on institutional control over personal information, where the concept of privacy—even contextual privacy—reveals its most glaring inadequacies.

To understand this, we need to move beyond the concept and the regime and look at the practice, that is, we need to reassess why a majority of people, at least in Western countries, value privacy in theory—that is, when responding to surveys—but are willing today to surrender very private information in unprecedented quality and quantity to the most opaque of institutions. This valuing of privacy reflects, in my view, some more or less explicit shadows of the liberal political theory which established the connection between privacy and personal and collective freedom in the first place. From this perspective, privacy is not an end but a means to our ability to determine for ourselves how to engage with the world. This autonomy is valued both in its individual and collective, political dimensions. Without privacy personal freedom and democratic decision-making—relying on an informed, active, confident citizenry—would be severely weakened. The 'autonomy of the will' (to use Kant's expression) is the core of the liberal political theory that still dominates the collective imagination. Thus, when people value privacy, they value personal and political self-determination.

There are numerous instances where people have to provide personal information in situations where they have little bargaining power, and this is well explored in the literature.[1] This is bad enough, but why, then, are people also willingly and voluntarily providing so much personal information in contexts they most likely know they cannot fully control, for example, on social networking sites?[2] Is it that self-determination at the personal and social level are no longer valued? Or is it that people simply do not

1 See, for example, the recent study by Maurizio Lazzarato (2010) on the invasive new procedures that the unemployed are subjected to in France.

2 For a recent public opinion survey on privacy attitudes and social networking, see http://press-room.lawyers.com/Lawyerscom-2010-Social-Networking-Survey-Press-Release.html

understand the grave consequences of their actions until there is an 'Exxon Valdez of Privacy' (Felten 2006). We can rule out the former, as personal freedom is more than ever a core value across the political spectrum (collectivist approaches have all faded) and we should also not count on the latter, because assuming people have a false sense of their own day-to-day lives makes for a poor starting point to understanding their behaviour—not least since none of the many privacy incidents of the last decade has had the necessary transformative quality.

But how else can we understand the clear disconnect between what people say when asked about privacy and how they behave in everyday life? I propose to look at this everyday behaviour and see it as the basis for the contemporary construction of personal and collective self-determination, in the limited ways that such autonomy can usually be realized in complex day-to-day situations. This would indicate that, on some level, the link between privacy and autonomy is being transformed.

Self-determination in the network society

To understand this transformation and its particular connection to the notion of privacy, it is necessary to separate the processes at the 'front-end' of, say, social networking sites from those at the 'back-end'. By 'front-end', I mean the interfaces that user interact with, and the information that is made accessible through these interfaces. By 'back-end', I mean the servers and databases that support the activities of the users, but are only accessible to the owners of the infrastructures and can be used for purposes other than those of the front-end. At the front-end, providing personal information expands the user's autonomy in two regards. First, she makes herself available for networking with others by providing the raw material for social trust; that is, information about who she is, what she has done in the past, and what she cares about now. Because social collaboration increasingly takes place informally among individuals rather than among institutions, it is necessary to know who that person is, personally, rather than being able to rely on the formal dimensions that govern the relationships of individuals. Increasingly, social networking is becoming the condition through which to pursue individual goals, by connecting people with the resources (information, other people, opportunities, etc.) necessary to act autonomously—that is, to be able to follow their particular agenda for life. There are both a positive as well as a negative scenario driving people to make themselves, as individuals, publicly available. There is the promise to find people and resources to help one achieve ones goals—whatever these are—and there is the threat that if one is not visible and accessible, society will simply forget about you. Disconnected from the flows of information and resources, one is rendered powerless and invisible. If the implicit threat of disciplinary society was punishment (Foucault 1979), then the implicit threat of the network society is disconnection and redundancy. A node that does not actively contribute to the network's performance will be disconnected (Castells 2004).

However, it is not only the relationships between individuals being transformed; those between individuals and institutions are also changing. In a complex information environment, institutions have become adept in providing highly personalized services. Rather than treating all users/customers the same, it is their particular promise to treat everyone different, providing just what each of them needs. These institutions no longer appear as bureaucracies, but as personal, almost intimate, service providers. They do so, not only because they are good at spinning their public image,[3] but also because the quality of the services provided increases with the amount of personal information provided by the user. The institutions appear to get to know one very intimately. There are very tangible advantages to fine-tuning one's profile, both in terms of what other people see and what the service provider can offer. Of course, the service providers are actively nudging people into this direction, for example, by providing uniform log-in across the platform, so that users can be more easily tracked for purposes the user might not favour, but even then, there are direct, tangible benefits to the users for going along with it. Thus, there is an perceivable

3 Google still portrays itself as a group of creative individuals, even though it has more than 20,000 employees.

increase in personal autonomy—constructed within networks and communities of resource sharing, leading to a forms of 'networked individualism' (Wellmann 2002; Tseng and Li 2007) —that is directly related to giving up privacy, or at least, to making oneself visible to unknown others. What is being created in the process could be called multi-directional, horizontal visibility. People seeing each other, for the better or worse. The notion of 'contextual integrity' (Nissenbaum 2010) falls short here, because in many cases the context is extremely fuzzy. How bounded is the social space that comprises friends of friends of friends? Subsequently, at the front-end, there are powerful drivers that, on an everyday level, show that by providing personal information generously and without too much worrying about privacy, individual autonomy—and the ability to act in groups—can be increased.

The situation is very different at the back-end. Here, the relationship between autonomy and privacy is more traditional. Powerful, centralized institutions are amassing very large amounts of very detailed personal data, which is being used to further the interests of the owners of the infrastructures, which may, or may not, coincide with those of the users.[4] Rather than producing multi-directional, horizontal visibility, what is being created is traditional, bureaucratic one-way, vertical visibility and the power-differential that comes with it. Very few people can see great numbers of people, individually and aggregated, without being seen themselves. The resulting possibilities to use this power at the expense of the front-end users have been well-detailed by introducing the concept of 'social sorting', that is the ability to create 'classifications … designed to influence and to manage populations and persons thus directly and indirectly affecting the choices and chances of data subjects' (Lyon 2003, 13).

Yet even here, being sorted through classificatory schemes does not necessary need to be regarded negatively. The ability to treat people differently is formulated as personalized service to enhance the user's autonomy; in fact, it is the very core of personalized institutions. As a result of promoting one's own visibility and receiving personalized services, one can increase personal autonomy. Traditionally, when 'the iron cage of bureaucracy' was the primary danger, privacy was a useful means towards this end. But in the highly dynamic information environment, where we need to have some form of filtering in order not to be overwhelmed by the all the information and all the options, this is less and less the case.

The conclusion from this is not to argue that we do not need the privacy regime or that the concept should be abandoned in total. Rather, we should start from the understanding of what privacy is conventionally thought to achieve: individual and social self-determination. We need then to review the contemporary conditions under which this goal can be advanced and assess the role of privacy in advancing it. Today, it requires both the ability to make oneself visible to others in relatively open settings, as well as means of mitigating the resulting power-differentials between the users who provide personal and those institutions which collect, aggregate and act upon this information. The notion of privacy is of limited use in the context first dimension, but remains vital in relation to the second.

References

Castells, M. 2004. Informationalism, Networks, and the Network Society: A Theoretical Blueprint. In *The Network Society: A Cross-Cultural Perspective,* ed. M. Castells, 3-45. Northampton, MA: Edward Elgar.

Felten, E. 2006. *The Exxon Valdez of Privacy*. Freedom-to-Thinker.com (June 12). http://www.freedom-to-tinker.com/blog/felten/exxon-valdez-privacy (accessed 21/03/2011).

Foucault, M. 1979. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books

Lazzarato, M. 2010. 'Pastoral Power' Beyond Public and Private. *Cahier on Art and the Public Domain* Open 19. URL: http://www.skor.nl/artefact-4808-en.html (accessed 21/03/2011).

Lyon, D., ed. (2003) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London and New York: Routledge.

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press

[4] I detailed the scope of this information gathering in the case of Google elsewhere, see Stalder and Mayer 2009.

Rössler, B. 2002. *Der Wert des Privaten*. Frankfurt: Suhrkamp

Sofsky, W. 2008. *Privacy. A Manifesto* (trans: Steven Rendall). Princeton: Princeton University Press.

Stalder, F. and Mayer, C. 2009. The Second Index. Search Engines, Personalization and Surveillance. In *Deep Search. The Politics of Search beyond Google,* eds K. Becker and F. Stalder, 98-115. Studienverlag. Distributed by Transaction Publishers, NJ.

Tseng, S.-F. and Li, M.-H. 2007. A Sense of Community or Networked Individualism? In *Proceedings of the Annual Social Informatics SIG Research Symposium. Pre-conference Research Symposia at ASIST, Milwaukee Wisconsin, 2007*. Available at: http://arizona.openrepository.com/arizona/handle/10150/106381 (accessed 21/03/2011).

Wellmann, B. 2002. Little Boxes, Glocalization, and Networked Individualism? In: *Digital Cities II: Computational and Sociological Approaches*, eds M. Tanabe, P. van den Besselaar and T. Ishida, 10-25. Berlin and New York: Springer.

Surveillance & Society

Reply | In further defence of privacy…

Colin J. Bennett

University of Victoria, Canada. cjb@uvic.ca

I would like to thank David Murakami Wood for placing my 'defence of privacy' as the centrepiece of this issue of *Surveillance & Society*. I am also extremely grateful to Professors Gilliom, Regan, boyd and Stalder for their insightful responses. I have a high regard for their work and take very seriously their considered views on these important topics. I do not have the space to engage with their various arguments in sufficient depth and detail, but their responses allow me to crystallize my views more sharply and to clarify what I am, and am not, arguing with respect to the framing of the larger response to the troubling levels of surveillance in the world.

Gilliom is correct. Our views tend to be shaped by what we study. I have spent my professional career within the policy community of regulators, advocates, officials, and corporate and governmental privacy officers. That experience has certainly influenced my perspectives and judgments. No doubt, if I had researched and written an ethnographic study of poor women in Appalachia, I too would harbour a far more sceptical view of the value of the concept and regime of privacy protection. *Overseers of the Poor* is one of the best studies on the politics of privacy that I know, and is essential reading for any student of surveillance. As of course, is Regan's book *Legislating Privacy*, on the social, collective and public values of privacy protection, ideas that have continually influenced my work, and indeed underpin much of the reasoning within my essay.

Like Regan, however, I do consider myself one of the few scholars in this field who has consistently bridged the academic world of Surveillance Studies with an active and admittedly sympathetic concern for the work of the community engaged in the broad 'governance of privacy'. That experience has led me to observe something of a 'separate tables' phenomenon. As in the restaurant in Terence Rattingen's 1955 play of the same name, the participants sit at separate tables, have different interpretations of the menu, are vaguely familiar with the conversations of the other diners, but rarely actively engage in the same conversation. Each table is somewhat protective of its methods and discourses. I believe that phenomenon is observed within the privacy community, within the Surveillance Studies community, and certainly between the two. My essay is intended as one modest attempt to improve the conversation.

Or maybe these are separate vessels. boyd seems quite content in the 'privacy ship' though concedes that it needs some much needed repair to bring it into the era of social-networking. Regan likewise wants some repair, but she would also steer it towards the collective problems of surveillance, rather than the individualized problem of privacy. Stalder would continue to man the pumps, but at the same time examine the condition of the leaking vessel. And Gilliom perhaps wants to sink it and build a completely new craft. I suppose that my point is that the privacy ship (or ships) left port a long time ago and are laden down with a variety of weaponry that is only being used by a few brave advocates, and under-resourced regulators. I just want more people to 'man the pumps' by filing complaints with organizations and regulators, promoting the use of 'privacy by design', supporting educational campaigns, engaging in the

Bennett, C.J. 2011. In further defence of privacy… *Surveillance & Society* 8(4): 513-516.
http://www.surveillance-and-society.org | ISSN: 1477-7487

complex debates over laws, guidelines, codes, standards, privacy-enhancing technologies and so on—essentially using all the instruments in the 'privacy toolbox'.

Enough of metaphors, let me engage more directly with the respondents. Gilliom's excellent portrayal of my conceptual, realist and pragmatist defence of privacy captures my central point that privacy, as a concept and a regime, is more intellectually relevant and politically powerful than it gets credit for in the Surveillance Studies literature. But I am not contending that we should 'turn back to the privacy regime' as if the older formulations in the Warren and Brandeis and Westin 'rights of control' traditions have been correct all along. What I am saying is that a large proportion of the community of advocates and regulators have already woken up, 'smelt the coffee' and generally get the point about the need for broader conceptions of privacy that are sensitive to the larger social issues, and less obsessed with individual invasion and self-determination. Unlike Stalder, therefore, I see plenty of evidence at the governance level that the discourse has moved beyond privacy's 'individualistic core'. At a conceptual level, I would probably concede his point about the continued dominance of the liberal tradition and that 'when people value privacy, they value personal and political self-determination'. I would only add that the liberal tradition is broad and diverse, and rests upon various ontologies of freedom, liberty, and self-determination, which can mean different things for the protection of privacy in different contexts.

Gilliom is also concerned that privacy enjoys a 'position of intellectual and political monopoly' that is the 'organizing matrix for the field'. I think he is perhaps using the word *regime* in a different sense from myself, as a broader intellectual framework that frames the discourse, rather than just a set of governance arrangements; Stalder also supports this distinction. At the wider level, privacy is surely a very broad, fluid, vague, messy and dynamic paradigm that produces many discourses. I agree with boyd when she contends that messiness has its strengths. I have difficulty seeing that such a concept can produce such a hegemonic framework, however. It is also worth reinforcing the point that surveillance is a global problem that requires a concerted response. The problem gets defined in subtly different ways depending on particular historical experiences and cultural traditions. The North American conceptions of privacy do not, I would contend, barge their way into different national debates without some refinement and resistance. 'La vie privee' in France, 'integritet' in Sweden, 'datenschutz' in Germany, 'privacidad' in Spain, and so on, tend to frame the discourse in those languages and can mean subtly and contextually different things in relation to equally tricky concepts relating to society and community.

Nevertheless, I have argued that there has been an international convergence of ideas on what privacy (information privacy) means at a governance level, which has produced a common and powerful understanding about what it means for a public or private organization to process personal data responsibly. I am not contending that the privacy regime that has developed over the last thirty years can solve all the individual and collective problems associated with the capture, processing and dissemination of personally identifiable information (PII)—whatever PII is these days. There are, as Gilliom argues and I concede, certain power dynamics and dimensions that simply do not fit within this privacy framework. And I am certainly not contending that it has been broadly effective. I would just reinforce Stalder's argument that there is no 'clearly articulated and implementable alternative'. The regime needs to be made to work. I simply do not know what Gilliom means when he concludes, 'we may be obliged to kill it!'

Both boyd and Stalder address social networking as an illustration of the transformation of privacy. boyd's important ethnographic work on the activities, behaviours and attitudes of social networking users has effectively countered the contentions of those who claim that people do not care about privacy, and that we are therefore entering a new era of social transparency. Her response and her work focus on agency and context rather than structural power. While I am fascinated by evolving social attitudes towards privacy, and how they might vary across a host of social and cultural variables, as a political scientist, I am naturally more interested in structural rather than situational power and therefore in what social networking organizations are actually doing with personal information at the 'back-end' in Stalder's

terms. *Facebook* and other social networking sites are manipulating the personal information of their users in order to make money. And that is where the privacy regime comes into the equation. For all Mark Zuckerberg's superficial and self-serving generalizations about evolving social attitudes towards privacy, it is indeed that regime, through European and Canadian regulators, and US privacy advocates that has forced *Facebook* to think carefully about the norms of transparency, consent, notification and so on. Of course, companies like *Facebook* and *Google* are watched; most are not. Perhaps if more of us watched more organizations and subjected them to the same rules, there might just be less surveillance in the world.

boyd misreads my argument, however, when she states that I believe that 'privacy, in its slippery state, fails to serve as an antidote to surveillance' and that 'one of the greatest weaknesses of discourse about privacy is that it's individual-centric'. Rather, my purpose was to interrogate the critique of privacy, rather than to add my voice to the chorus of voices arguing that we are drifting towards a surveillance society, and that the privacy regime is incapable of doing much about it. I do not disagree with Gilliom's broader point that there are invariably many other values at stake when personal information is captured, controlled, manipulated, disseminated, profiled etc. without the individual's knowledge or consent. I just think that privacy protection can be instrumental in promoting those other values. The difficulty, as many have noted, is that most people tend not to interpret the denial of other rights and services in privacy terms, because often that processing of personal information is invisible. But that is why we need privacy regimes to render the surveillance more transparent. Thus, when Gilliom points out that his subjects in *Overseers of the Poor* would never contemplate filing a lawsuit or complaining to Privacy International I would suggest that this is, at some level, a bit of an American problem. In every other advanced industrial state, there would be recourse through a privacy or data protection commissioner, which can and do respond to complaints from welfare recipients, and try to regulate the conditions under which welfare files may be shared.

In conclusion, if not privacy, then what? A broad politics of anti-surveillance, perhaps? I read Regan's response as contending that the social problem should be defined in terms of surveillance because it more accurately frames the breadth and complexity of the social and political challenges. But privacy frames the risk because it is the most 'robust and concise understanding of the reason we are, and should be, concerned'. I think this formulation counters Gilliom's contention that 'surveillance is not, in fact, the ontological antithesis of privacy'. That argument is also implicit in my contention that privacy was never meant to be the 'antidote to surveillance'.

I would add a further reason as to why privacy continues to resonate very powerfully, and why surveillance may not be the better way to frame the social problem. One of the features of privacy advocacy is its broad ideological base. For example, recent campaigns in the US have drawn support from the libertarian right, Christian groups as well as those from the public interest and civil liberties traditions. If one were to try to reframe the discourse in terms of a politics of 'anti-surveillance' and to situate it within broader social antagonisms and struggles, these issues would tend to become associated with a politics of the left. One can challenge an ID card, or a video-surveillance system, or a genetic database, or a health identifier, or a host of other surveillance measures, without engaging in a broader social 'struggle'. Perhaps one of the strengths of the contemporary privacy advocacy network is that resistance can, and does, spring from a multitude of ideological sources at unpredictable moments.

A myriad of under-resourced privacy advocacy organizations are attempting to challenge the spread of surveillance. In October 2009, the Public Voice Coalition of privacy advocates launched the *Madrid Privacy Declaration* at the international conference of Privacy and Data Commissioners. It has been translated into ten different languages and has been endorsed to date by over 100 organizations, and around 200 international experts, from many countries including several in the developing world. Among other things, the declaration reaffirms support for the 'global framework of fair information practices', the

data protection authorities, privacy-enhancing technologies and calls for a 'new international framework for privacy protection'. More controversially, the Declaration calls for a 'moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate'.[1] Over forty official privacy and data protection agencies are receiving complaints, conducting investigations and audits, consulting with organizations, educating the public, and imposing sanctions. Increasingly they are trying to work in a concerted fashion. In 2009, for instance, ten commissioners sent a joint public letter to Google CEO, Eric Schmidt, expressing their strong concern that 'the privacy rights of the world's citizens are being forgotten as Google rolls out new technological applications'.[2] Some of these activities are effective; others less so. But I have difficulty seeing them as 'background noise'. Far from being a 'stultifying intellectual crutch', privacy *can* serve to engage, coalesce and resonate with many individuals and groups around the world.

The critique of privacy at conceptual and governance levels will and should continue. But that critique is diverse and sometimes contradictory, and I have tried in my essay to disentangle the various strands. At the same time, if that critique continues without reference to what regulators and advocates actually think and do in the name of privacy protection, then I fear that it will be misplaced and ultimately ineffective.

1 Madrid Privacy Declaration at: http://thepublicvoice.org/madrid-declaration/

2 Letter from privacy commissioners to Google CEO, Eric Schmidt at: http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm