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

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 as 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 Ringier 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 Communiqué: <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.