c. Privacy advocates, privacy advocacy and the surveillance society

Colin J. Bennett

Introduction

Every day numerous stories appear in the print and online media about the latest attempts by governments and businesses to capture and process personal information in the name of better risk management, service delivery or profit accumulation. Some of these practices emerge without much comment or concern; others are debated and tolerated; and others are resisted strenuously, widely and continuously.

The literature on how surveillance is challenged has tended to focus on two distinct processes. On the one hand, there is an enormous variety of work on the institutional and legal responses in the name of protecting privacy, or advancing the cause of personal data protection. This literature has focused on the content of law and the powers and responsibilities of privacy and data protection authorities and has drawn important lessons about what works and what does not. In recent years, it has become obvious that other non-legal policy instruments, of a self-regulatory and technological nature, are also necessary (Bennett and Raab 2006). A second set of responses resides at the individual level. Gary Marx has categorized the range of inventive strategies that individuals use in their day-to-day lives to subvert, distort, block and avoid surveillance (Marx 2003). John Gilliom documents similar techniques, often not conceived in traditional privacy terms, which poor people have used to resist intrusions by an over-bearing state (Gilliom 2001). These strategies have proliferated in the online environment as individuals surf, e-mail, blog and network anonymously or pseudonymously.

Between, or beyond, formal institutional responses on the one hand, and individual resistance on the other, there is of course the possibility of collective action through pressure groups, non-governmental organizations and/or social movements. Until recently, however, there has been little written about this form of response in any of the literature. The prevailing view is that privacy protection laws have generally arisen as a result of pressure and bargaining among elites, and has downplayed the role of civil society organizations in the larger story about the development of privacy rights in advanced industrial states. Some even regard the ragbag collection of privacy advocates that has emerged over the years as a marginal and disorganized irritant, more intent on grabbing headlines than effecting lasting social change. That general perception has led to skepticism about whether a broader "politics" of privacy protection would ever be possible.

The Privacy Advocates (Bennett 2008) attempted to fill a gap in the literature, and convince readers that this general perception is inaccurate and unfair. The more I looked, the more privacy advocates I found

who, with courage, dedication, and ingenuity were pushing organizations to be more responsible and regulators to be more proactive. In every advanced industrial society, there exists one group or more whose self-defined mission is to advance the cause of personal privacy, and to campaign against excessively intrusive technologies and practices. Many privacy advocates work with few financial and human resources. At the same time, many of them have discovered creative ways to make a difference and to influence policy and practice.

Given the central importance of privacy protection, not only as a fundamental human right, but also as a prerequisite for securing citizen and consumer trust in international computer networks, the central role of privacy advocacy assumes a huge importance. Privacy advocates normally display a considerable technical sophistication and have therefore been prominent in the debates over the last decade about the future of the internet. In publicizing the problems associated with third-party cookies, spyware, key-escrow encryption schemes, or the personal information practices of a Microsoft, Google, or Facebook, their work has been important. The results of conflicts such as these have had significant implications for the future of digitally mediated communications (Bennett 2008: Ch. 5).

The Privacy Advocates was based on extensive documentary analysis and key informant interviews with some of the major privacy advocates in the world. The book allowed me to think through the same problems faced by advocates themselves, and thus to link my scholarship to their practical concerns. This entry updates and builds upon the analysis presented in that work. I begin by presenting a profile of the privacy advocacy network and suggesting a useful typology of both organizations and actors. Despite several dilemmas concerning the framing of the problem(s) in terms of "privacy," I contend that it matters deeply whether the issue is framed in terms of a civil liberty, a human right, a digital right, a consumer problem or in terms of a series of "single issues." These dilemmas are manifested in a deeper tension between the individualistic foundations of the right to privacy, and the collective prerequisites and grievances that tend to animate social movement politics. Nevertheless, while privacy may never mobilize a coherent social movement, it has certainly galvanized an important transnational activist network which engages in a combination of informational, symbolic, accountability and leverage politics (Keck and Sikkink 1998).

A profile of the privacy advocacy network

The opposition to excessive surveillance is generally framed in terms of "privacy advocacy", and those engaged in this critique and resistance are normally referred to as "privacy advocates" (Bennett 2008). The term is used widely, in the media and in the policy community. "Privacy" in the abstract is a cause that few people would wish to oppose, because we all have a subjective interest in the way our personal information is used. So there can be no self-declared counter-movement to the right for citizens to have control over their private space and their private information. There is no "anti-privacy" movement as there is an "anti-abortion" movement, for example.

In a broad sense, the term "privacy advocate" has emerged as shorthand to describe anybody that advances the cause in an official capacity, such as staff in data protection authorities, or chief privacy officers in government. However, there is also a sense that a privacy advocacy community exists as a relatively distinct network from those who are mandated to advance the cause within corporations or government agencies. There is a distinction between those who are paid to promote privacy protection, and those who emerge more spontaneously from civil society to promote the public interest, and act as the "gatekeepers" between a concerned but poorly informed citizenry and the organizations that process personal information. Governments and business also "reach out" to the privacy advocacy community by drawing them into consultative and advisory exercises (Bennett 2008: 169–97).

At an individual level, some self identify more as "activists" than advocates, focusing more on grassroots mobilization and a more uncompromising articulation of the value rather than a negotiation with

competing social interests (Davies 1999). Activism tends to be rooted in the belief that real change can only come from below, by challenging the conditions that give rise to the perceived threats in the first place. Most privacy advocates have to engage in other activities—research and teaching, hardware and software development, journalism or various forms of artistic expression. Particularly controversial is the relationship between the role of advocate and that of the consultant. Some privacy advocates find it difficult to resist the temptation to take money for advice, public speaking, research, training or education. Most self-identified privacy advocates wear a number of hats, and juggle several responsibilities, some of which can entail significant conflicts of interest.

There are no easy generalizations about what motivates individuals to become interested in advocating for this cause. They are: men and women, black and white, gay and straight, young and old, rich and poor, and so on. Some are active churchgoers; most are not. Most have higher levels of education, though their educational backgrounds are extremely diverse—humanities, sciences, medicine, business, social sciences, law, librarianship, computer science and others. A few have personal experience of damaging privacy intrusions; most do not. They also come from every wing of the ideological spectrum. It is probably the case that most advocates share a somewhat centre-left, civil-libertarian political perspective. Others would find sympathies with an anti-capitalist or anti-globalization agenda (Webb 2007). Some spring from a libertarian philosophy of minimal governmental intervention (Harper 2006). Yet others find favor with those on the Christian right (Albrecht and McIntyre 2006). Privacy advocacy has no conventional ideology; it can be promoted and opposed by those from all political and partisan positions.

From any review of the universe of groups who agitate against surveillance (see www.privacyadvocates.ca), it is immediately obvious that the modern policy issue, defined as privacy in the United States and data protection in Europe, has sustained few advocacy groups whose sole interests are in these issues. There are exceptions, such as Privacy International, the Privacy Rights Clearinghouse, the Electronic Privacy Information Center (EPIC) or the Australian Privacy Foundation. But in most countries, the privacy advocacy role is inextricably linked to broader civil liberties, human rights, consumer or digital freedom questions. Most groups have arisen, therefore, for reasons beyond those of advocating for privacy rights.

It therefore matters profoundly how the issue is perceived and articulated through some broader framework. Some groups, for instance, advocate for privacy as a civil liberty and focus on intrusions by the instruments of the state and (most especially) by law enforcement agencies. The claims of civil liberties advocates tend to be made with reference to specific national constitutional guarantees, such as the Bill of Rights in the United States. Many would insist that privacy is fundamentally a human right, and claim that it is far broader than one among many civil liberties. Claims about privacy as a "human right" tend to be made in more universalistic terms and derive from certain inherent human rights by virtue of our humanity, rather than our citizenship. There is evidence that many groups in developing countries see the close relationship between surveillance and other forms of repression and have embraced a pro-privacy agenda, though they may not frame their agendas in those terms. Privacy issues are often brought to the fore as a result of the practical and inherent problems of campaigning for human rights in repressive regimes.

National and international consumer protection groups have a long involvement with privacy issues. For them, the illegitimate capture, collection, use and disclosure of personal information are all issues of deceptive trading. They have assisted individuals with complaints about consumer credit, direct-marketing, and identity theft as well as with the various consumer services on the internet. Virtually every group mentioned so far has been involved in internet privacy questions. Some, however, have emerged solely as a result of the internet and desires to create an open medium based on sound democratic principles. The notion of a separate set of "digital rights" which are an extension of more fundamental civil rights and liberties underpins the work of a number of national and international organizations, of which the Electronic Frontier Foundation (EFF) is the most prominent example. A final category embraces a sprawling number of single-issue groups which have decided for various reasons to concentrate their efforts on a

particular technology or practice (such as RFID chips or video-surveillance), on a type of information (such as genetic information), on a set of vulnerable people (such as children) or on a particular business sector (such as direct marketing).

Traditional concepts do not adequately capture the dynamic, volatile, overlapping and fragmented nature of privacy advocacy. There is certainly no clear structure. Neither is there a social movement with an identifiable base. Perhaps the best label is the "advocacy network" which can be conceptualized as a series of concentric circles. At the centre are a number of privacy-centric groups, such as the Electronic Privacy Information Center (EPIC) in which other issues are peripheral and, if addressed, have to be entirely consistent with the core pro-privacy (or anti-surveillance) message. As we move out of the centre of the circle we encounter a number of privacy-explicit groups for whom privacy protection is one prominent goal among several; many of the civil liberties and digital rights organizations, such as the American Civil Liberties Union (ACLU) or the EFF fall into this category. Within the outer circle, there is an indefinite number of groups, for whom privacy is an implicit or potential goal. Their aims are defined in very different terms—such as defending the rights of women, gays and lesbians, the homeless, children, librarians, ethnic minorities, journalists and so on. Despite not explicitly focusing on privacy issues, the protection of personal information and the restriction of surveillance can be instrumental in promoting their chief aims. There is, therefore, a vast range of groups whose support could be mobilized given the right issue or correct case of intrusive governmental or corporate behavior (Bennett 2008: 57–61).

The privacy advocacy network therefore comprises multiple groups and individuals with varying commitment to the central value of privacy. It is non-hierarchical in the sense that no one group is considered more important than any other. There is no one person who can claim to speak for the network as a whole, any more than there is one group that is representative of the entire movement. It is an open network and has no defined limit, expanding and contracting depending on the issue and the opponent. The agents are consulted not as individuals, but as "privacy advocates" and are presumed to be articulating a public interest in this value. The term carries a significance and implication beyond the individual, and beyond the specific group to which he/she belongs, and often allows them to "punch beyond their weight."

Over the years, attempts to institutionalize that transnational cooperation have found expression in networks such as the European Digital Rights Initiative (EDRI), the Privacy Coalition or the Public Voice Coalition. These initiatives have been important. But the loose and open network of privacy-centric, privacy-explicit and privacy-marginal groups is apparent in many domestic contexts. Privacy advocacy springs from dedicated activists, but it also emerges out of existing civil libertarian, human rights, consumer and digital rights organizations. This pattern is evident in the United States, but in several other countries as well.

The politics of privacy advocacy

So what do privacy advocates do, exactly? The question is straightforward; the answer less so. Clearly any answer has to be framed in transnational terms. Surveillance is a global phenomenon; any challenge must be conceived similarly. In their study of advocacy politics in international politics, Margaret Keck and Katherine Sikkink (1998: 16) employ a fourfold typology of tactics used by international activist networks. Symbolic politics relates to the invocation of symbols, actions, narratives and other symbols to convey the implications and dangers of a particular practice within a particular culture. Accountability politics is about using legal and non-legal policy instruments to hold organizations responsible. Leverage politics implies that there is a threat or a sanction to non-compliance. Information politics relies on the ability to generate politically relevant information and to move it by the most effective means to the place where it will have the most impact.

Within the privacy advocacy network, there is plenty of symbolism on both sides of the debate. Verbal and non-verbal symbols generate attention and reduce the complexity of political problems for ordinary

citizens. Over the years, this advocacy network has used the full range of written, audio and visual techniques to advance their arguments. They have always invoked the specter of "Big Brother" to warn of the slippery slopes toward total surveillance. They also engage in a certain amount of lampooning, such as with the annual Big Brother Awards, now organized in several countries. Symbolic interpretation is part of a process by which they can raise awareness, solidify their networks and expand the constituency of believers. But symbolic politics only is effective when it connects to a broader set of cultural understandings, such as when current programs are equated with poignant historical memories.

There are also many opportunities for the privacy advocacy network to call organizations to account. Privacy advocates have occasionally been the authors of high-profile complaints to privacy commissioners. Because of the lack of resources, they more rarely engage in litigation. In most countries, privacy obligations are enshrined within data protection laws, which cover both public and private sectors. Other rules are embodied within international agreements, or in a range of self-regulatory measures, such as codes of practice and privacy seals. Thus, even where legal rules do not exist, privacy advocates can still try to ensure that organizations "live up to their own rules." Once governments and corporations have publicly committed to privacy standards, advocates can use these positions to expose discrepancies between discourse and practice, and possible deception. When that occurs, they have a tendency to want to take immediate and widespread advantage. The revelation, for example, that Google was inadvertently collecting personal Wifi data through its Street View operation immediately provoked complaints to privacy commissioners in Canada, Australia and Europe and to the FTC in the United States.

Leverage politics assumes that the group has some power and that it can get what it wants from those in authority by threatening some cost if there is no change in practice. Possessing resources is the essence of this form of politics, which can be withdrawn if the advocates do not get the reforms they want. Like other public interest groups promoting a public good, their constituency is broad and diffuse. Unlike professional associations or labor unions, they have no ability to mobilize a membership and threaten the withdrawal of electoral or financial support for elected politicians. Thus the leverage politics of privacy advocacy is almost entirely about the loss of reputation or the "mobilization of shame." And privacy advocates have used subtle, and not so subtle, ways to name and shame organizations and individuals, from standard media campaigns to outright boycotts, to efforts to sway the investment decisions of shareholders.

Symbolic, accountability and leverage politics are important elements of privacy advocacy, but they are not the dominant way in which the network tries to advance the arguments. The major resource that privacy advocates possess is information—or, more specifically, expert information about the causes and consequences of surveillance mechanisms, and about the various remedies—legal, self-regulatory and technological.

There is a long tradition within social movement politics of inducing those in power to do something that they would not otherwise do through the constant reporting of facts and testimony about abuses of power and the resulting harms. With few exceptions, however, the information politics of privacy advocacy has generally not been about adopting a "human rights methodology" and about documenting facts relentlessly about actual harms to real people. For the privacy advocate, the politics of information tends to rely upon argumentation about potential consequences. Sometimes the social and individual risks require expert analysis and explanation, and might depend on the confluence of a complex set of institutional motivations and technological development. Information about privacy invasiveness sometimes has to rely on hypothesis rather than fact. It must draw together certain assumptions about what could happen to personally identifiable information if certain worse case scenarios materialized.

At one level, privacy advocates engage in a constant fight to influence the discourse at the earliest stages of system and program developments. This often involves a process of going back to square one and of explaining in philosophical terms the nature of the problem, and perhaps challenging the myth that "If you have nothing to hide, you have nothing to fear." At another level, the argumentation involves extrapolations from the experiences of surveillance systems in other times and places. Increasingly it involves

considerable technical expertise, and sophisticated understandings of the operation of complex public and private organizations.

By and large, privacy advocates will try to enter the public debate about a particular practice earlier rather than later, and to generate relevant information about privacy implications in advance of the deployment of a product or service, or in anticipation of policy change. And they need to perform this role with respect to proposals which they support (such as a privacy protection bill), as well as those which they might oppose. Privacy advocates need to decide the appropriate institutional target given the constitutional framework and balance of institutional powers in individual countries. They also face vexing choices about whether to engage in sometimes perfunctory consultation exercises, and whether or not to sign non-disclosure agreements. Privacy advocates can, and do, spend enormous amounts of time injecting written and oral arguments into various stages of the policy cycle, and reacting to policy proposals developed by both executive and legislative agencies at the national level, as well as those by a myriad range of international organizations, including key technical standards bodies, such as the International Standardization Organization (ISO). Advocates have complained of a process of policy laundering, where national governments seek influence in international arenas to pursue controversial schemes, such as biometric passports, unattainable through domestic processes (www.policylaundering.org).

However, some are suspicious of the political process, or are not conveniently located to engage with decision-makers in the "corridors or power." They prefer to engage in public education. Others work well with reporters, are good at media interviews and have that ability to encapsulate the complex policy issue within the pithy one-liners that make good journalism. More rarely, other advocates will attempt to mobilize support on the streets. To the extent that this street-level politics has been encountered, it is entirely associated with high-profile governmental schemes in countries outside North America. In Germany, for instance, there were several early protests in the 1970s and 1980s against the national census, and more recent street activism against the data-retention directive mandating the surveillance of telecommunications traffic data. Identity card schemes have also sparked public protest, such as in Australia in the late 1980s, and more recently in the UK. When the Japanese government established its controversial "Juki Net" system, a national network of registration information on all Japanese residents, protestors shredded their identity cards on the steps of the Home Affairs Ministry.

The privacy advocacy network is therefore confronted with a series of choices and dilemmas within the frameworks of information, symbolic, accountability and leverage politics: whether to engage with governmental agencies and the private sector, to work out differences, establish compromises and advance pragmatic solutions, or to go public; whether to cast their net widely, and advocate for a broad range of privacy interests, or to focus on particular practices; whether to engage in broad and long-term research or to react more pragmatically to the events of the day; whether or not to build a broader constituency with a membership base; and whether or not to accept financial or other support from government and/or the private sector. As in any public interest advocacy network, these tensions create personal rivalries and jealousies, some of which have endured and cemented some entrenched and embittered views about who is true to the cause, and who has "sold out" (Bennett 2008: 129–32).

As an illustration, the recent introduction of "full-body scanners" into airports has been met with each of these forms of political activism. The symbolism of the naked scanned image has been reproduced many times to accentuate the level of intrusiveness. Privacy advocates have attempted to call governments to account by launching complaints to national privacy commissioners, or to the courts in the United States as an "unreasonable search and seizure" under the 4th Amendment. Analysis of the effectiveness and health risks of these scanners has been assembled and targeted to appropriate audiences. On 24 November 2010, activists planned a National Opt-Out Day to protest the use of full-body image scanners at American airports. The leverage stems from the choice of the day before Thanksgiving, and the hope that the consequent delays and line-ups could mobilize sufficient pressure against these new devices. Any contemporary privacy campaign ideally needs, therefore, a combination of information, accountability, leverage and

symbolic politics—clear presentation of facts and analysis, ideally backed up by research; a media strategy which presents those facts with symbols that resonate with the wider culture; the skilful use of official avenues of redress, both domestically and internationally; and the judicious use of opportunities to name and shame.

Conclusion: the globalization of privacy advocacy

The Privacy Advocates concluded that the privacy advocacy network is increasing in visibility and significance, and is worth further scholarly research. Interactions within the network are becoming more regular and frequent. There is now a broader recognition that a diverse set of interests can be attracted to particular causes, thus making the network appear more politically significant than in the past. Privacy advocates might thus become more cohesive and institutionalized over time, and result in less pragmatic methods for setting priorities and engaging in campaigns. Any such realization will undoubtedly grow as more horizontal connections are made between privacy advocates internationally.

This process took a further important step with the agreement and publication of the Madrid Privacy Declaration. Coordinated through the Public Voice Coalition, this Declaration was launched at the international conference of Privacy and Data Commissioners in Madrid in October 2009. To date, the Declaration has been signed 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" (http://thepublicvoice.org/madrid-declaration/).

It is instructive that this Declaration should be framed in terms of the language of "privacy," a concept that has been subject to so much criticism in the academic literature (Bennett 2011). "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 discriminatory aspects of surveillance, culturally relative, overly embroiled in spatial metaphors about "invasion" and "intrusion," and ultimately practically ineffective. The essential difficulty, therefore, is about how to "frame" the issue in ways that define a sense of collective grievance following from excessive surveillance. Can that sense of shared grievance grow when the issue is invariably articulated through the conceptual lens of "privacy"? There is perhaps a fundamental dilemma in trying to energize collective action around an emotive and powerful concept that is derived from a very subjective and individualistic right.

Yet, the term has been remarkably resilient. It attaches to a huge array of policy questions, to a sprawling policy community, to a transnational advocacy network, to an academic literature and to a host of polemical and journalistic commentary. Despite the fact that nobody can supply a precise and commonly accepted definition, privacy maintains an enormous and global appeal, in the English-speaking world and beyond. Witness the fact that the Madrid Privacy Declaration was translated into ten different languages, and was supported by organizations and individuals in every region of the world. Furthermore, and as noted above, it is a term that spans the ideological divide. 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 immediately become associated with a politics of the left. One can defeat 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, therefore, is that resistance can, and does, spring from a multitude of ideological sources at unpredictable moments.

This is not to say that the language of surveillance cannot be put to good use by the privacy advocacy network. But, with all its contradictions and vagueness, *privacy* is the concept around which this network has coalesced, and will probably evolve. It still carries a broad cultural and transnational appeal. For better or worse, "privacy advocates" have learned to live with it.

References

Albrecht, K. and McIntyre, L. (2006). *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance*, Nashville, TN: Nelson Current.

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

——(2011). "In Defence of Privacy: The Concept and the Regime," *Surveillance & Society*, 8(4): 485–96.

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

Davies, S. (1999). "Spanners in the Works: How the Privacy Movement is Adapting to the Challenge of Big Brother," in C. J. Bennett and R. Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age,* Toronto: University of Toronto Press.

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

Harper, J. (2006). *Identity Crisis: How Identification is Over-Used and Misunderstood*, Washington, DC: Cato Institute.

Keck, M. E. and Sikkink, K. (1998). *Activists Beyond Borders: Advocacy Networks in International Politics*, Ithaca, NY: Cornell University Press.

Marx, G. (2003). "A Tack in the Shoe: Resisting and Neutralizing the New Surveillance," *Journal of Social Issues*, 59(2): 369–90.

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