Journal of Comparative Policy Analysis: Research and Practice

ISSN: 1387-6988 (Print) 1572-5448 (Online) Journal homepage: http://www.tandfonline.com/loi/fcpa20

Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies

Colin J. Bennett

To cite this article: Colin J. Bennett (2011) Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies, Journal of Comparative Policy Analysis: Research and Practice, 13:2, 125-141, DOI: 10.1080/13876988.2011.555996

To link to this article: http://dx.doi.org/10.1080/13876988.2011.555996

Published online: 29 Apr 2011.

Journal of Comparative Policy Analysis,
Vol. 13, No. 2, 125–141, April 2011

Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies

COLIN J. BENNETT
Department of Political Science, University of Victoria, Canada

ABSTRACT *For the most part, privacy and data protection laws arose not through grassroots pressure but through interactions between governmental and business elites in the context of broader international harmonization efforts. Thus, civil society activists have rarely been seen as a client constituency with equivalent weight to governmental and business interests. There is evidence, however, that the privacy advocacy network is becoming more influential in comparative context. In most countries, a network of advocates has emerged with a relatively distinct profile from the "official" data protection authorities. Individual advocates play several conflicting roles and often exist within groups with wider civil liberties, human rights, digital rights, or consumer interests. Those at the center of the privacy advocacy network possess a set of core beliefs about the importance of privacy, and as one passes to the outer edges the issue becomes more and more peripheral. Privacy advocacy is beginning to occur from both the inside, and the outside, representing an important shift in the evolution of privacy protection policy both nationally and internationally, and producing difficult tensions between the two networks.*

Introduction

Historically, privacy protection has been viewed as a matter for individual claim and resolution, in which wrongs between individuals could be resolved through tort law. For many years, the doctrine of the "right to be let alone" (Warren and Brandeis 1890) and subsequent jurisprudence around "reasonable expectations of privacy" have produced one very important tradition and legacy for privacy scholars. A different and more recent tradition, however, is to view 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

Colin Bennett received his Bachelor's and Master's degrees from the University of Wales, and his PhD from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria, where he is now Professor. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels.
Correspondence Address: Colin J. Bennett, Department of Political Science, University of Victoria, Victoria, BC, Canada V8W 3R4. Email: CJB@UVIC.CA

ISSN 1387-6988 Print/1572-5448 Online/11/020125-17

DOI: 10.1080/13876988.2011.555996

important to be left to the private tort 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). It is now clearly a matter of *public policy*.

There is now a 40-year history of personal data protection policy. And most advanced industrial states now possess comprehensive statutes that regulate the collection, storage, processing, dissemination and retention of personally identifiable information by public and private organizations. To be sure, the content and implementation of these laws are deeply influenced by national administrative and legal traditions. Some, such as those in Canada, Australia and the United States, are titled "privacy laws". Others follow the European nomenclature – "data protection". These laws should also be understood within the context of different political cultures that accord varying levels of trust to the agencies of the state, given historical experiences. It is also obvious, however, that the transnational conditions that motivate a convergence of privacy protection policy, and particularly the influence of certain international regimes, have tended to overwhelm distinctive national traditions (Bennett 1992, Newman 2008). The overwhelming dynamic is one of policy convergence (Bennett 2010).

Privacy protection policy also now embraces far more than law. The environment now involves a complicated network of private and public sector actors who engage in overlapping domestic and international regimes. Many international, regulatory, self-regulatory and technological policy instruments contribute to the "governance of privacy" (Bennett and Raab 2006). Privacy protection is thus more than a civil liberties or human rights issue. It has 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).

Despite its growing importance, however, the attention of political scientists to the issue of privacy has been limited. The processing of personal information intersects with a number of the traditional concerns of political theory, constitutional law, comparative politics, public administration, international relations and political economy, and there is indeed a smattering of literature in each of these subfields (see Bennett 2001). However, only a few political scientists have written about privacy with a view to investigating the ways in which the issue can shed light upon wider theories of public policy-making in national, comparative or international perspective (Bennett 1992; Regan 1995; Bennett and Raab 2006; Newman 2008). Conversely, few in the field of privacy protection have drawn insights from political science to inform the development and implementation of privacy protection policy (van de Donk et al. 1996).

In most countries, there is still, therefore, a dominance of legal reasoning and scholarship within the literature. One reason, I suggest, is that policy instruments have spread, and the policy community expanded without significant intervention from mass publics, political parties or interest groups. As with other questions associated with the communications and information revolution, whether it be broadcasting, telecommunications regulation, freedom of information, or intellectual property, these issues tend to be seen as within the more specialized and technocratic realms of policy making and administration (Mueller et al. 2004).

For the most part they do not excite passions and adherence. They rarely appear in party platforms.[1] And they seldom affect the election or dismissal of elected officials.

This special issue challenges us to think more theoretically and critically about the transformation of privacy protection policy, and invites me to point to some current trends within the privacy policy community and to raise some searching questions about the continuation of this technocratic policy style. For while legal, self-regulatory, international and technological policy instruments have proliferated, a network of transnational activists has attempted to keep the broader human rights dimensions of privacy alive on the international agenda. Increasingly impatient with the technocratic and elitist character of contemporary policy making, some privacy advocates have contended that the progress of this issue will depend less on policy mechanisms devised and implemented by elites, and more on the extent to which resistance to privacy invasions can be more broadly mobilized. Some advocates wish to build a more coherent transnational activist network, which not only uses official means of advocacy and redress, but also engages in a broader "politics of privacy", publicly exposing overly intrusive practices and even "outing" the organizations that are responsible for them (Davies 1999).

This article advances the argument that a transnational privacy advocacy network is coalescing and increasing in visibility and significance. Interactions within the network are becoming more regular and frequent. There is also a broader recognition that a range of civil society organizations can be attracted to the privacy cause, thus making the network appear far wider and more politically significant than in the past (Bennett 2008: 182–184). There is, consequently, a growing tension between the "inside" and the "outside" privacy advocates – between the network of privacy commissioners, chief privacy officers and other "official" data protectors, and those who have emerged more spontaneously from civil society to challenge the particularly intrusive mechanisms, institutions and technological practices of contemporary networked societies.

This article explores the implications of this tension for the actors and instruments engaged in the protection of personal data. It is based on interview research conducted for *The Privacy Advocates: Resisting the Spread of Surveillance* (Bennett 2008), but extends that analysis by exploring in greater detail and depth the actual and potential relations between the "inside" and the "outside" privacy advocates, with illustrations from some recent key case studies of international data protection.[2] What roles does each set of actors play? What are the implications for the comparative and international protection of personal data and for the transformation of privacy protection policy?

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). There is a plausible argument that everybody is, or should be, a privacy advocate. Because personal information is collected, stored, processed and disseminated about each and every one of us, we all have a subjective interest in ensuring that the right people handle the right information for the right purposes. Furthermore, we may all declare that our information should not be provided to this or that organization, on the grounds that it is "none of their business". Hence, "privacy" in the abstract is a cause that few people would wish to oppose. There is no self-declared opposition movement to the right for citizens to have control over their private space and their private information. There is no countermovement on the issue of privacy (della Porta and Diani 2006) as there is an "anti-abortion" movement, for example.

A diverse number of individuals within the broad policy community might self-identify as privacy advocates. The issue is broad and amorphous and so is the community that identifies with it. Privacy advocates are found in government and in business. In another sense, therefore, the term 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 corporations. Advocacy implies expertise and is indistinguishable from the work of those professionals who challenge the processing of personal information by government or business.

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, either in their capacity as privacy and data protection commissioners, or as the chief privacy officers in corporations. In this sense of the word, advocates do what they do to promote a cause, a principle or a norm. The term "advocate" not only implies a normative commitment to a set of principles or values, but also a desire and ability to speak on the behalf of others, precisely because few of us have the time and energy to be our own "advocates".[3] Societies arguably need a set of informed and interested individuals to act as the "gatekeepers" between a concerned but poorly informed citizenry and the governments and corporations that process our information. Governments and business sometimes also "reach out" to the privacy advocacy community by drawing them into consultative and advisory exercises. It can therefore be argued that the privacy advocacy network has a relatively distinct profile and identity. It is something separate from the state and the market, even though it is very open and fluid (Bennett 2008: 169–197).

At an individual level, there are a number of overlapping types of privacy advocate. For example, some self-identify more as "activists" than advocates. The conventional perception is that advocates "advocate" whereas activists agitate, mobilize or resist. Privacy activists tend to take more radical or principled positions. They tend not to balance privacy against competing public interests, because they know that the opposing arguments will always be made with force by people with far more resources than they. For the activist, the privacy argument requires a less compromising articulation rather than a negotiation with competing social interests. The "balancer" is a "pragmatic advocate" (or "pragvocate"), according to Simon Davies of *Privacy International*.[4] Activism for some also entails educating the general public so that its membership is more sensitive to the dangers of certain technologies, more aware of their rights and more likely to put pressure on elected representatives. It is an activism rooted in the belief that real change can only come from below, by changing the conditions that give rise to the perceived threats in the first place. Activism implies a transformation of ideas and beliefs, over and above a reform of laws, policies and institutions. Thus "grassroots activism" is often contrasted with governmental "advocacy".[5]

Most privacy advocates need to play at least one other role in order to make a living. Though some privacy advocacy finds expression through traditional grassroots activism, most is combined with other activities – with research and teaching, with hardware and software development, with journalism and with various forms of artistic expression. Particularly controversial is the relationship between the role of advocate and that of consultant. Some privacy advocates find it difficult to resist the temptation to take money for advice, research, training or education, and through those processes continue to advocate the privacy cause.[6] There are few pure stereotypical cases. Most self-identified privacy advocates wear a number of hats and juggle several responsibilities, some of which can entail significant conflicts of interest.

The interviews conducted for this project have indicated that there are no easy generalizations about what makes a privacy advocate. 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 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 center-left, civil libertarian political perspective. Others would be positioned on the radical left, and 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.

An analysis of the individual privacy advocates exposes one dimension of the network. The groups or organizations within which they operate tell another story. The pattern of group formation tends to reflect the issue itself – constantly changing, very diverse and almost infinitely flexible. A definitive "mapping" of the landscape is impossible.[7]

The first point is 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 matters profoundly how the issue is perceived and articulated through some broader framework or discourse. Some groups, for instance, advocate for privacy as a civil liberty. Civil liberties are, however, traditionally thought of in terms of governmental, rather than corporate, power. For these groups, therefore, privacy advocacy tends to be focused on the protection of individuals from intrusions by the instruments of the state and (most especially) by law enforcement agencies. The political cultures of many countries do not readily embrace a "civil liberties tradition" that tends to be associated with countries, such as the United States, which have written constitutions and enumerated bills of rights. However defined, in most advanced industrial societies we find civil society groups which have long sought to protect individuals from abuses of power by the state. Privacy advocacy, while often not described as such, is a significant component of that tradition.

Many would insist that privacy is fundamentally a human right, and claim that it is far broader than one among many civil liberties. 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. Claims about privacy as a "human right" tend to be made in more universalistic terms and derived from certain inherent human rights by virtue of our humanity, rather than our citizenship. Thus the Universal Declaration of Human Rights (UDHR) states that "everyone has the right to life, liberty and security of person (Article 3)". It goes on (Article 12) to state that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations 1948).

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 do not term their agenda as such. 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. Human rights organizations, such as Amnesty International, face some agonizing dilemmas about the collection and confidentiality of extraordinarily sensitive information about rights abuses, dissidents, and so on. Their workers are themselves subjected to surveillance, the interception of communications and sometimes more brutal treatment. Other NGOs have arisen to assist human rights organizations to protect their databases and communications in the face of such threats.[8]

National and international consumer protection groups have a long involvement with privacy issues.[9] 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. These groups have lobbied for better privacy and data protection laws. They have researched and written reports on new and emerging consumer issues. For them, the illegitimate capture, collection, use and disclosure of personal information are all issues of deceptive trading. These groups associate good privacy protection with good business practices, and, even though privacy competes with other issues on the consumer protection agenda, many consumer advocates have no difficulty also being privacy advocates.

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 from desires to create an open medium based on sound democratic principles. The existence of a separate set of "digital rights" which are an extension of more fundamental civil rights and liberties is controversial. The belief, however, frames the work of a number of national and international organizations, of which the Electronic Frontier Foundation (EFF) is probably the most important.

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, on a type of information, on a set of vulnerable people (such as children) or on a particular business sector (such as consumer credit). A notable example is the Surveillance Camera Players who have been performing skits before the video-surveillance cameras in New York City for around ten years, and who have motivated similar groups in other cities and countries (New York Surveillance Camera Players 2006).

It is also not clear that the word "group" adequately captures all the advocacy behavior documented in this article. Some are indeed non-profit groups registered under their respective statutes with membership lists and subscription dues. But many have no membership base, even though they might operate with boards of advisors. Some groups can have grandiose titles which describe nothing more than a website and perhaps a bulletin board, blog or listserv. The Internet provides many false fronts, behind many of which are the same casts of characters. Neither is there a social movement with an identifiable base, or a shared collective identity.

Perhaps the closest descriptor is the "advocacy network" which can be conceptualized as a series of concentric circles. Those at the center possess a set of core beliefs about the importance of privacy, and as one passes to the outer edges, the issue becomes more and more peripheral. Policy change occurs, according to this hypothesis, when those on the periphery begin to share the core beliefs of those at the center (Sabatier 1988). With respect to privacy protection, at the center are a number of *privacy-centric* groups such as EPIC, Privacy International, the Australian Privacy Foundation, Privacy Rights Clearinghouse, and Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). Other issues are peripheral and, if addressed, have to be entirely consistent with a pro-privacy (anti-surveillance) message. As we move out of the center of the circle we encounter a number of *privacy-explicit* groups for which privacy protection is one prominent goal among several, and perhaps competing, goals. Many of the civil liberties and digital rights organizations, such as the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation, the Center for Democracy and Technology (CDT) and Statewatch, fall into this category.

Within the outer circle, there are an almost indefinite number of *privacy-marginal* groups, for whom privacy is a peripheral issue. Their goals are defined in very different terms – preventing torture, 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 government surveillance can, however, be central to these groups' purposes and instrumental in promoting their chief aims. There is, therefore, a vast range of groups for which privacy is a marginal purpose and for which it might become a central goal given the right issue or correct case of intrusive governmental or corporate behavior. Privacy is an implicit, or potential, goal for these groups (Bennett 2008: 57–61).

The contemporary privacy advocacy scene is best described as a transnational advocacy network, characterized by "voluntary, reciprocal, and horizontal patterns of communication and exchange" (Keck and Sikkink 1998: 8). The relations are similar to what scholars of social movements have found with respect to domestic movements. They are *segmentary*, insofar as they are "composed of many diverse groups which grow and die, divide and fuse, proliferate and contract" and *polycentric* because they have "multiple, often temporary, and sometimes competing leaders or centers of influence". Finally, they are *networked* given that they form "a loose, reticulate, integrated network with multiple linkages through travelers, overlapping membership, joint activities, common reading matter, and shared ideals and opponents'' (Gerlach 2001).

The privacy advocacy network is composed of 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. It expands and contracts depending on the issue and the opponent. This fluidity corresponds with the network's culture of improvisation, where priorities are never established in any coherent way and instead tend to emerge because one or two actors decide to do something, and ask around for support. The various privacy campaigns against major Internet companies, for example, have tended to exhibit this spontaneous quality (Bennett 2008: 151–163).

In many countries, not just the United States, a combination of privacy-centric, privacy-explicit and privacy-marginal groups have appeared on the landscape. The groups are different, and their character is certainly determined by distinctive institutional and cultural characteristics. The catalysts for their emergence are also often rooted in particular national conflicts. But in each major country, there are advocates with activist, consumer, digital rights, civil liberties and single-issue profiles. And on the outside, a range of potential groups exist that might be mobilized given the right motivation.

The network is therefore more than the sum of the individuals and groups that make it up. The term ''privacy advocates'' implies an identity as a separate community from government and the corporate sector. Thus, when a privacy advocate is consulted or quoted, s/he is presumed to be articulating a public interest in this value. The term carries a weight and implication beyond the individual, and beyond the specific group to which he/she belongs. Networks are not groups. They are not necessarily movements. And they are, according to Manuel Castells (1996), the dominant form of organizing in late capitalist, ''information'' societies.

Privacy Advocacy from the ''Inside''

The emergence of an outside network of civil society groups and activists is a relatively recent phenomenon. This ''outside'' network has developed in parallel with the more ''official'' and institutionalized data protection authorities in different countries. Most countries (with the notable exception of the United States) have set up small privacy or data protection authorities, independent from government, with varying oversight, advisory or regulatory powers. Abraham Newman's recent analysis of the international regulation of personal data contends that the data protection laws that have spread around the world in the last decade or so have resulted mainly from European leadership. Data protection authorities, according to Newman, have been key players in the development and implementation of these rules, thus contributing to the regional integration process. Collectively they constitute a robust and powerful trans-governmental network with significant regulatory capacity which ''constrains the ability of industry and government to exploit unchecked the processing of personal information'' (Newman 2008: 27).

In the 1970s and 1980s, it was possible to classify these instruments according to some clear regulatory models, depending on the enforcement powers of the agency in question (Flaherty 1989, Bennett 1992). It is now more difficult to draw such clear distinctions. One of the effects of the 1995 European Data Protection Directive has been to extend the process of policy convergence beyond the level of basic statutory principles. This Directive pushes for greater conformity in the ways in which these principles are enforced through a "supervisory authority". Moreover, the principle of independent oversight is also regarded as a test of the "adequacy" of data protection in non-European countries (EU 1995). We now see a convergence on principles, on the scope, and on the implementation mechanisms. These agencies have drawn lessons from one another about the best way to implement complex statutes (Bennett 1997), even though they are always constrained in their efforts by a lack of resources, and by powerful public and private interests eager to use the latest information technologies in the name of risk management or profit accumulation.

When we analyzed these agencies' functions at the turn of the millennium, therefore, it was apparent that a common set of roles appeared in virtually every data protection regime. The data protection agency plays the role of: ombudsman, auditor, educator, policy advisor, negotiator and enforcer (Bennett and Raab 2006: 133–144). This more functional approach recognizes that the letter of the law gives only partial guidance to the activities of data protection authorities in different societies. In addition, the agencies have developed very important relationships and activities amongst themselves on the international level and in smaller regional groupings. There is now a very well attended international annual conference. There are also regularized meetings in smaller regional or functionally specific contexts, such as telecommunications, as the articles by Newman and Raab in this issue demonstrate.

These agencies may also be "advocates" as their heads have sometimes expressly stated. One of the persistent criticisms of privacy commissioners is that they are too pragmatic and expedient. In his seminal study of data protection policy in six countries, David Flaherty (1989: 341) concluded that:

> The data protection agency should not be a mini-parliament that seeks to settle the appropriate balance internally, nor should it concentrate solely on presenting a balanced perspective of the competing interests to the external master, be it the government or the legislature. Its emphasis should be on the anti-surveillance side of the balance, since the forces allied against privacy, or at least in favor of efficient surveillance, are generally so powerful.

He continually asserted this role when he later took up the position of information and privacy commissioner of British Columbia from 1993 until 1999. Other commissioners have also self-identified as privacy advocates, such as the former Canadian Privacy Commissioner George Radwanski, who concluded one speech by stating that "a Privacy Commissioner's voice has to be raised in constant advocacy of privacy, reminding people of their rights and obligations, standing up for principle in the face of expediency and convenience, and strengthening one of the most critical elements of the social glue that binds us together – strengthening privacy" (Radwanski 2001).

These agencies, and the statutes which empower them, for the most part predated the emergence of privacy advocacy organizations. In Europe, Canada, Australia and other states, privacy and data protection authorities are regarded as the primary organizations expected to resist excessive surveillance and publicize pro-privacy arguments in the media. All commissioners, therefore, have to reconcile their public advocacy role with other responsibilities. The way that balance is struck depends in large measure on the style, personality and temperament of the individual commissioner (Flaherty 1989). Thus, a quite strident and public posture of privacy advocacy can be contrasted with a legislative reality and set of statutory responsibilities that inevitably require a more pragmatic stance.

These commissioners also, therefore, constitute a network. This is a network, however, with a deeper history and more established sets of rules and responsibilities. It is a network with a clearer sense of who belongs, and who does not, and one that steadfastly resists membership to countries which do not possess data protection authorities that are truly independent from government or the business sector (see Raab, this issue). The network jealously guards its important role as the guardian of privacy in the face of enormous institutional and technological pressures, and also defends its role in relation to the outside privacy advocates who operate within civil society.

Network Relations and Tensions

How, then, do these networks interact? How do the official privacy advocates within the community of privacy or data protection authorities relate to the transnational network of civil society advocates? For the most part, the privacy and data protection laws which give these bodies their authority did not arise because of grassroots pressure co-ordinated through civil society activists; most laws emanated through interactions between governmental and business elites, and were often prompted as much by the exigencies of international harmonization efforts as by the demands from public interest groups (Bennett 1992). Thus, in most states, the privacy advocacy network is rarely seen as a client constituency with weight equivalent to governmental and business interests. In many countries, privacy advocates exist in parallel, but often subordinate, domains.

Germany, as an example, has a lengthy history of data protection implementation and a coherent network of federal and state data protection authorities. From the point of view of the privacy advocacy network in Germany, the data protection authorities are bureaucratic agencies with limited tolerance for more radical forms of activism.[10] From the view of the data protection authorities, the activism of civil society advocates may seem marginal, perhaps silly, and of fringe importance to the legal and technological negotiations necessary for the implementation of data protection in complex societies.[11] In some cases, data protection authorities may not even be conscious of the extent of the privacy advocacy network, and insufficiently aware of the fact that privacy advocacy can emanate from a diversity of privacy-centric, civil liberties, consumer, digital rights or single issue groups.

The existence of institutionalized data protection authorities may also have the unintended effect of crowding the policy space. The authorities tend to be the first agencies to be consulted in legislative hearings, the first with which the media makes contacts, and the first to which the public goes for advice. The establishment of a national data protection authority can cause skepticism about the need for external privacy advocacy, making it difficult to raise funds, develop a distinctive voice and role, and be heard in the political arena. As an illustration, in the 1970s there was a very strong Dutch advocacy group (Privacy Alert) that atrophied as soon as the Netherlands data protection law was passed and the national authority (*Registratiekammer*) was established in the 1980s. Furthermore, it is surely no accident that the majority of privacy advocacy groups exist in the United States. The absence of a privacy commissioner in the United States perhaps allows privacy advocacy groups to bloom and to perform some of the roles played by the official data protection authorities elsewhere.

Whereas the relations in some countries are virtually non-existent, in others they can be tense, even abrasive. For example, there has been a long-running conflict between the London-based Privacy International, and the UK's information commissioner (ICO) over issues such as video-surveillance cameras, identity cards, fingerprinting in schools, data breaches and so on. Tensions and frustrations reached a culmination after the ICO rejected the complaint of Privacy International about the Google Street View application.[12] The group wanted Street View suspended pending an investigation into the methods and technologies used to blur faces and vehicle registration numbers. Simon Davies, Director-General of Privacy International, sharply criticized the ICO's rejection of the complaint and claimed that it had become

> official policy of the ICO not to stand in the face of business interests. ... The gloves are now off. After ten years of failed complaints and undermining by that office of the core data protection principles, we have decided that there is no further point in trying to educate the officials there.

Davies went on to blame the commissioner, Richard Thomas, for contributing to the surveillance society: "The Information Commissioner has clearly decided that pragmatism and commercial interest should triumph over principle. This is a dangerous trend and one that is clearly responsible for Britain's appalling surveillance culture" (Williams 2009).

Between benign neglect and outright warfare, there can, however, be more productive relations between inside and outside privacy advocates. For example, tensions can also be used to positive advantage by a strategic commissioner, allowing him or her to point to the more fundamentalist positions articulated by the outsiders and to accentuate the "reasonableness" of their recommendations and positions. Civil society advocates have more freedom to express the more radical privacy argument, unencumbered by the pragmatic need to reconcile that position with social, political and corporate interests. The articulation of the less pragmatic position from the outside permits the institutionalized privacy advocates within government and business to advance the cause, even if in a more compromising way.[13]

It is also the case that the non-governmental and non-corporate actors can push the limits of the discourse and bring new issues to the domestic and international agendas. They exist on the cutting edge, seeing the trends, warning of the dangers, pushing and cajoling in public arenas and private negotiation. They can act as an early warning, sounding the alarm about new technologies and trends. The US-based group CASPIAN (Albrecht and McIntyre 2005) advanced the earliest warnings about radio frequency identification device (RFID) technology. Much of the invasive potential of cookies and spyware was brought to light by the work of groups such as EPIC and Center for Democracy and Technology. In the UK, Privacy International and No2ID provided the early analysis of the implications of the government's identity card scheme (LSE 2005). The privacy advocacy network can often react more quickly. It also tends to possess more technical expertise, given the younger, perhaps "geekier" profile of some of its members. The assessments may sometimes be hasty and polemical, but they do serve to elevate specific issues to the national and international privacy agendas.

Privacy advocates can also sometimes act as complainants. Data protection authorities need informed and well-targeted complaints. Privacy advocates can sometimes offer that assistance. In Canada, Pippa Lawson, formerly of the Canadian Internet Public Policy Clinic (CIPPIC), has lodged a number of complaints under the Personal Information Protection and Electronic Documents Act (PIPEDA) with the privacy commissioner of Canada. For example, in 2004 she complained against Accusearch Inc., an American corporation based in Wyoming, that was routinely collecting, using and disclosing for a fee personal information about Canadians through its website for inappropriate purposes and without the knowledge and consent of the individuals in question.[14] CIPPIC has also lodged complaints under PIPEDA against Winners, Sony, Ticketmaster, InfoCanada, Mastercard, Canada.com, the Google-Doubleclick merger, and most recently Facebook.[15] These illustrations do reveal a possible tension because, in all cases, CIPPIC publicized the complaint from the outset on its website. The tension arises because the Canadian privacy commissioner is an ombudsman who is normally obliged to conduct a private investigation without revealing the identity of the complainant or the respondent. The summaries of any investigation finding appear on the commissioner's website with names de-identified, which is sometimes bizarre when those names are publicized earlier in the media.

In a few instances, advocacy groups have been able to lodge simultaneous complaints to a number of different data protection authorities. The best example occurred in June 2006, when Privacy International decided to lodge simultaneous complaints to data protection authorities in 33 countries concerning revelations of secret disclosures of millions of financial records from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to US Intelligence agencies. The matter became public when the *New York Times* and the *Los Angeles Times* published details of these private arrangements. The complaint alleged that the activity was undertaken without regard to the rights of citizens under data protection law, and that "the scale of the operation, involving millions of records, places this disclosure in the realm of fishing exercise rather than legally authorized investigation" (Privacy International 2006). Privacy International later lodged further complaints to six other authorities, filed a freedom of information request to the Bank of England, and published an open letter to the CEO of the company. Data protection authorities began investigating, individually and jointly. Ultimately, the Article 29 Working Group of European data protection authorities issued a finding that SWIFT was in breach of the European Data Protection Directive, and called for several remedial steps.

The complaint mechanism can be a two-edged sword, and from an advocates' point of view can be lengthy and frustrating. Often the potential of a public complaint against an organization is enough to effect a change in practices. Sometimes the company or agency concerned will see an interest in trying to resolve the issue informally. In the end, of course, it may not yield the anticipated result. Many advocacy groups, therefore, tend not to bother even initiating the process.

In their study of advocacy politics in international politics, Margaret Kekk and Katherine Sikkink (1998: 16) use a fourfold typology of tactics that international networks use in their efforts at persuasion, socialization and pressure. 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. Symbolic politics relies on the ability to call up symbols, actions, stories, that can interpret a situation in ways that make sense for a particular audience within a particular culture. Accountability politics is an attempt to hold powerful agents accountable to previously stated policies or commitments. Leverage politics is directed towards those who have power in public or private organizations and who can effect change, and involves a sanction or threat of some manner, typically "naming and shaming".

This typology is developed in the context of human rights and environmental advocacy networks, but it offers some interesting insights into privacy advocacy as well. And in each form of politics, the privacy advocacy network can work in tandem with official data protection authorities and contribute to the "governance of privacy". Advocates can engage in information politics by conducting research and injecting into the legal and policy process, the media and thereby assist with the education of the general public.[16] They can, and should, engage in more accountability politics, through formal complaints to any organization whose practices contradict their claims. They can exert leverage, through the judicious naming and shaming of privacy invasive practices. They also contribute to the larger debate by connecting the privacy issue to relevant symbols that resonate within the overall political culture.

Conclusion

One lesson from this analysis is that the formation and implementation of privacy protection or data protection policy can, and should be, situated within the broader literature of comparative policy analysis. There is still a tendency to view the issue in legal or technological, rather than political, terms. My argument here, as well as in other work, strongly suggests that broader patterns of governance evident in other policy sectors are manifested with respect to privacy as well. The governance of privacy involves a complicated and networked picture of enforcement, in which different policy instruments and actors play shifting roles. Successful privacy protection today does require a comprehensive law with an active and assertive regulatory authority. But data protection authorities do not, on their own, represent or embody a significant regulatory capacity. They are not even necessarily the central hub within national and international policy communities, but one of a network of technological, self-regulatory and international policy instruments (Bennett and Raab 2006). Data protection policy is, therefore, co-produced rather than enforced (Raab 1997).

This more open and networked model accords a greater opportunity for privacy advocates to exert political influence. This article has argued that there is evidence that the privacy advocacy network is taking advantage of these opportunities. It is increasing in visibility and significance, and assuming a greater responsibility within the larger policy community (Bennett 2008). Interactions within the network are becoming more regular and frequent. Campaigns are taken more seriously and there is also evidence of some success in thwarting the more intrusive and ambitious surveillance schemes of government and the private sector.[17]

There is also broader recognition that many related interests can be attracted to particular privacy causes that make the network appear far wider and more politically significant than would otherwise be the case. There is a component of privacy advocacy within a vast array of groups. But many extensions of the network are often only temporary; new groups may stay for one campaign and leave for the next, a typical feature of the "post-modern campaign" (Bennett 2003). Broad campaigns, such as that recently waged against the Real ID proposals in the US, take enormous amounts of time and effort and thus cannot be regular occurrences within a network with limited temporal and material resources.[18] Nevertheless, slow adjustment to the realities of the issue, and the potential of the Internet, have produced a broad realization that such broad-based campaigns are beneficial for the network and the issue.

Advocates are also discovering how to combine their cause with wider political or corporate interests. This often entails learning how better to marshal information to the debates, link the issues to symbolic events that resonate within the political culture, apply leverage where possible, and force organizations to live up to their own rules and those of the jurisdictions in which they are operating. There are many legal and non-legal rules about privacy protection, some strong and others weak. Any public statement or commitment to privacy protection, however weak and qualified, provides an opportunity to test whether words are supported by actions and practices. Experience from other issues, such as environmental protection, 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 "spotlight" the practices of a multinational company the network might use actors located in another (Spar 1998). The globalization of network activity not only permits mutual understanding and lesson-drawing, but it also broadens the opportunities for transnational collective action (Keck and Sikkink 1998).

The best example of international co-operation occurred in October 2009, when the Public Voice Coalition launched the *Madrid Privacy Declaration* at the international conference of privacy and data commissioners. It has been translated into ten different languages, and 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''.[19]

There is a fundamental dilemma in trying to energize collective action around a concept that is derived from a very subjective and individualistic right. As a proposition, it perhaps makes little sense to try and encourage people to engage in a social movement so that everyone can enjoy a private life. The concept has also been described as ''protean'' in that it tends to capture a family of problems that are not related by any common denominator or core element (Solove 2008: 171–172). The protean nature of privacy might be a conceptual problem, but it ironically also offers an opportunity for privacy advocacy groups strategically to highlight the aspects of the issue that have the best chances of bringing a wide variety of groups to a campaign – whether the campaign be about ID cards, video surveillance, data retention, air passenger data, biometric identification, spyware, behavioral advertising on the Internet, workplace monitoring, vehicle tracking, the measurement of heat emanation from homes, the interception of telecommunications, or whatever. The breadth and flexibility of the concept militates against a common cognitive frame, but it also perhaps presents some strategic advantages. Clearly these framing dilemmas are a matter for further empirical research.

In the face of enormous social, political and technological pressures, many privacy advocates have tried to advance a complex argument about the erosion of a fundamental human right. The opening and expansion of the policy community is one of the most significant recent transformations in privacy protection policy. The issue is no longer a matter for legal and technocratic discourse. There is sufficient initial evidence that a transnational advocacy network, attuned to the potential of cyber-activism, can inspire a range of responses to intrusions and abuses, and occasionally inspire social mobilization. The transformation of the issue in the years ahead will depend, in part, on whether the outside privacy advocacy network is accorded a less subordinate role in the larger policy community engaged in the politics of privacy.

Acknowledgements

I am grateful to Christopher Parsons for some of the research assistance upon which this article is based, as well as to two anonymous reviewers for Journal of Comparative Policy Analysis.

Notes

1. There is at least one exception. The ''Pirate Party'' in Sweden has placed privacy at the top of its reform agenda. See: http://www2.piratpartiet.se/international/english
2. The original project was based on a set of key informant interviews with over 30 privacy advocates in different countries. These interviews, in common with ''snowball-sampling'' then led to others in the network. The project also relied on the analysis of statements about privacy on the websites of privacy advocacy organizations.
3. That meaning is also implied in terms like ''animal rights advocates'' or ''child protection advocates''.
4. A term coined by Davies at the first Computer, Freedom, Privacy (CFP) conference in 1991. See the report on Risks Digest at: http://catless.ncl.ac.uk/Risks/11.39.html
5. A group called ''Privacy Activism'' was created for this very reason. http://www.privacyactivism.org

6. An example would be the small consulting company that was established by individuals within Privacy International. See: http://www.8020thinking.com/
7. A reasonably comprehensive listing is presented at: http://privacyadvocates.ca
8. Privaterra is a notable example: http://www.privaterra.org
9. The National Consumer Council in the UK and the Verbraucherzentrale Bundesverband (Federation of German Consumer Organizations) are examples.
10. Germany has, in fact, seen some quite important civic mobilization in protest against excessive surveillance. In September 2007, more than 15,000 took to the streets of Berlin to protest the new Data Retention Directive. EDRI Gram, September 26, 2007. These impressions were provided by German groups such as *Foebud* (Interview, June 27, 2006) and *Die Humanistische Union* (Interviews, June 22, 2006).
11. An example would be the common reaction to the "Big Brother Awards" organized in many countries, and often attended by attempts to ridicule and satirize prominent politicians and corporate actors to attract media attention.
12. See: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-564039
13. This point was made publicly by Canadian Privacy Commissioner, Jennifer Stoddart, at a forum for privacy advocates in Montreal, September 24, 2007.
14. At www.abika.com one can purchase background checks, personality profiles, search criminal records, tax records, vehicle license records, obtain DNA profiles and many others. She requested her own file from the company, was refused and filed a complaint with the Privacy Commissioner of Canada. She submitted that Accusearch Inc.'s activities were contrary to PIPEDA and called upon the Commissioner to investigate. The Commissioner refused, indicating that she did have not have jurisdiction to investigate a company residing in another country. Lawson appealed to the Federal Court, which determined that the Commissioner did have jurisdiction, and was therefore obliged to investigate the complaint.
15. See: http://www.cippic.ca/en/projects-cases/privacy/pipeda-complaints/
16. The most encouraging signs of co-operation perhaps exist in Canada through the explicit attempts by the Office of the Privacy Commissioner to fund non-profit research through its official "Contributions Program".
17. Examples from the various conflicts of census data, ID cards, and Internet monitoring are provided in Chapter 5 of *The Privacy Advocates*.
18. See, http://epic.org/privacy/id-cards/ EPIC has also co-ordinated a broad-based campaign against full-body imaging at airports. See: http://privacycoalition.org/stopwholebodyimaging
19. The Madrid Privacy Declaration is at: http://thepublicvoice.org/madrid-declaration/

References

Albrecht, Katherine and McIntyre, Liz, 2005, *Spychips: How Major Corporations and Government Plan to Track your every Move with RFID* (Nashville: Nelson Current).

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

Bennett, Colin J., 1992, *Regulating Privacy: Data Protection in the United States and Europe* (Ithaca, NY: Cornell University Press).

Bennett, Colin J., 1997, Convergence revisited: toward a global policy for the protection of personal data, in: Philip E. Agre and Marc Rotenberg (Eds) *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press), pp. 99–123.

Bennett, Colin J., 2001, *Privacy in the Political System: Perspectives from Political Science and Economics,* available from: http://www.colinbennett.ca/recent-publications/reports-2/

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

Bennett, Colin J., 2010, International privacy standards: a continuing convergence. *Privacy Laws and Business*, **105**, 13–14, available from: http://www.colinbennett.ca/recent-publications/journal-articles/

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

Bennett, Lance W., 2003, Communicating global activism. *Communication and Society*, **6**, 143–168.

Castells, Manuel, 1996, *The Rise of the Network Society* (Oxford: Blackwell).

Davies, Simon, 1999, Spanners in the works: how the privacy movement is adapting to the challenge of Big Brother, in: Colin J. Bennett and Rebecca Grant (Eds),*Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press), pp. 244–261.

Della Porta, Donatella and Diani, Mario, 2006, *Social Movements: An Introduction* (Oxford: Blackwell).

European Union, 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 (The EU Data Protection Directive).

Flaherty, David H., 1989, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press).

Gerlach, Luther P., 2001, The structure of social movements: environmental activism and its opponents, in: John Arquilla and David Ronfeldt (Eds) *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica: Rand), pp. 289–310.

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

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

London School of Economics (LSE), 2005, *The Identity Project: an Assessment of the UK Identity Cards Bill and its Implications* (London: London School of Economics).

Mueller, Milton, Page, Christiane and Kuerbris, Brandon, 2004, Civil society and the shaping of communications-information policy: four decades of advocacy. *Information Society*, **3**, 169–185.

Newman, Abraham, 2008, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca, NY: Cornell University Press).

New York Surveillance Camera Players, 2006, *We Know You Are Watching* (New York: Factory School).

Privacy International, 2006, PI launches campaign to suspend unlawful activities of finance giant. Press release, 28 June, available from: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-538985

Raab, Charles D., 1997, Co-producing data protection. *International Review of Law, Computers and Technology*, **11**, 11–42.

Radwanski, George, 2001, Protecting privacy in the 21st century: the Canadian approach to the protection of personal information. Paper presented at Conference of Privacy Laws and Business, Cambridge, UK, July 2, 2001, available from: http://www.priv.gc.ca/speech/02_05_a_010702_e.cfm

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

Sabatier, Paul, 1988, An advocacy coalition framework of policy change and the role of policy-oriented learning therein. *Policy Sciences*, **21**, 129–168.

Simitis, Spiros, 1978, Reviewing privacy in the information society. *University of Pennsylvania Law Review*, **135**, 707–746.

Solove, Daniel. 2008, *Understanding Privacy* (Cambridge, MA: Harvard University Press).

Spar, Deborah, 1998, The spotlight and the bottom-line: how multinationals export human rights. *Foreign Affairs*, **77**(2), 7–12.

United Nations, 1948, *Universal Declaration of Human Rights*, United Nations, available at http://www.un.org/Overview/rights.html

Van de Donk, Wim, Bennett, Colin J. and Raab, Charles D., 1996, The politics and policy of data protection. *International Review of Administrative Sciences*, **62**(4).

Warren, Samuel and Brandeis, Warren, 1890, The right to privacy. *Harvard Law Review*, **4**(5), 193–220.

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

Williams, Chris, 2009, Street view nod prompts call for privacy watchdog reform. *RINF News*, April 24, available from: http://rinf.com/alt-news/surveillance-big-brother/street-view-nod-prompts-call-for-privacy-watchdog-reform/5457/