2008

The Sieve of Overspecialization

William (Bill) Bonner
University of Regina, bill.bonner@uregina.ca

THE SIEVE OF OVERSPECIALIZATION

William (Bill) Bonner
Paul J. Hill School of Business
University of Regina
bill.bonner@uregina.ca

ABSTRACT

Using Ulrich Beck's focus on experts as the source of unintended risks in society, this paper speculates on the consequences of linking the concepts of privacy and security too closely. The argument is made that this constructed linkage attracts separate and fairly narrow fields of technical expertise that focus on a very limited definition of the problem and hence the potential solutions derived. It is argued that this expertise focuses on small "p" privacy (data and rules about data) and that a failure to address privacy substantively understates the potential costs of security failures and that, paradoxically, a serious engagement with concept of the privacy may lead to more effective attention on data and its security.

Keywords

Privacy, security, experts, risks, overspecialization

INTRODUCTION

This paper explores for the potential of unintended risks emerging from the overspecialization of expertise on issues of privacy and security. The essence of the argument is that in phrasing the issue as a conjunctive phrase, "privacy and security", the efforts of narrowly focused technical experts limit the definition of the issues at stake and hence the range of solutions proposed. This is particularly true on the privacy side of the phrase and argued consequence is that it risks understating and undervaluing efforts devoted to security.

An important metaphor of IS privacy research is the notion of balancing privacy concerns against other interests, either explicitly cited (Culnan 1993; Culnan and Armstrong 1999; Culnan and Bries 2003) or implied in the suggestion of tradeoffs between individual privacy and other goals (Smith 1993). This appeal to balance is reflected in practice as organizations explicitly link their privacy policies to the act of achieving balance (Equifax Canada 2007; Royal Bank of Canada 2004a; The Canadian Marketing Association 2007) The Royal Bank of Canada states that Canadian private sector privacy legislation is "essentially about balance" (Royal Bank of Canada 2004b). This ties in to the discussion leading to the creation of fair information principles (FIP) on which most privacy legislation around the world is based (Raab and Bennett 1998; Slane 2000). The core issue to the developers of FIP was, "The need of balancing competing interests of privacy on the one hand and freedom of information on the other" (Organization for Economic Co-Operation and Development 1980, p. 16).

Yet, repeated studies using Actor-Network Theory (ANT) to reconstruct actual enactments of balance have led to a sense of unease and disquiet about enactments of balance in practice (Bonner 2006, 2007; Bonner and Chiasson 2005). For instance, the government of Alberta has opted to continue the sale of motor vehicle registration (MVR) data in its enactment of balance, with a vague appeal to "historical purposes and practices". Yet an investigation revealed that the history consisted of repeated questions about the propriety of the government selling this information. (Bonner, Chiasson and Gopal under review). In another instance the second largest school board in Canada disclosed the personal information of its almost 100,000 students to a company in California for access to email servers and a share of the revenue earned by the host company on student click through activities. An investigation into that enactment of balance revealed a lot of hype around the need for the education systems to respond to computer technology but little actual substance or the consideration of tradeoffs (Bonner 2007). Finally, an appeal body for a provincially run automobile insurance program posts detailed personal physical and mental health, financial and education information on its web page, under the individuals name, for anyone with internet access to view. In that enactment of balance transparency of the process was placed opposite privacy concerns and found to out weigh privacy (Bonner 2006). Yet, this same result could have been achieved by posting case numbers only, rather than individual names.

While the findings of these studies are enlightening they are labor intensive and too rare to be seen as anything more than interesting unrelated stories. Yet a theme that runs through each of these cases is that the outcomes and the production or

continuation of these practices are by-products of a host of decisions taken by different people for different reasons and that there appears to be little accountability or responsibility for decisions taken.

The unique nature of each circumstance makes it difficult to articulate links between such events enabling recognition of the patterns leading to their production and, with that, creating the possibility of limiting their likelihood. I believe that Beck's articulation of the source of risks and the use of ANT as a tool to identify, follow and understand action could provide insights into the production of these circumstances and hence a potential early warning system. This thought process will be applied to the privacy and security linkage. A few examples of the existence of this linkage follow.

In a recent case, a Canadian newsmagazine reported purchasing the cell phone records of the Canadian federal privacy commissioner from an organization in the United States (Gatehouse, 2005). Bell Canada, admitting that the records came from its system, issued a statement:

> "Bell wishes to assure its customers that protecting the privacy of customer information is a serious matter for the Company. To this end Bell has systems and procedures in place that are continually updated to better protect customer information…. As soon as the Company was made aware of this incident, it took additional steps to further tighten the safeguards in place to protect customer information" (Bell Canada, 2005).

Bell Canada's response focused on protecting information and updating procedures and safeguards to protect customer information.

In December 2004, Bank of America reported the loss of computer tapes containing information on 1.2 million credit cards (Nowell, 2005). In a statement regarding the loss of the tapes, a spokesperson said,

> "We deeply regret this unfortunate incident. The privacy of customer information receives the highest priority at Bank of America, and we take our responsibilities for safeguarding it very seriously" (Nowell, 2005).

Again the focus is on safeguarding or protecting. The link between privacy and security is even more explicit in the online privacy policy statements of Bank of America and LexisNexis. In both cases the privacy policy is accessed through a "Privacy and Security" link.[1]

Thus, there is a link between privacy and security in practice that it seems fairly natural. The examples above were easy to find. The question is what is being balanced in the privacy and security linkage?

The structure of the rest of the paper starts with theoretical lenses and then uses them to focus on the expertise drawn to privacy and security, followed by an articulation of risks that arise, and concluding comments.

THEORETICAL LENSES

Actor-Network Theory

Considerable in-depth case study research has been conducted on government and corporate uses of personal information and how issues of privacy play out in practice, using Actor-Network Theory (ANT) (Bonner 2006; Bonner and Chaisson 2005; Bonner and Gopal 2001). Essentially, actants (actors) act for local reasons and understandings and align with others who, also acting locally, see their interests being met in their self-enlistment and alignment in action (Latour 1987). If enough alignments take place then networks form and ideas transcend their local time and space. In order to enlist more and more actants in alignment, the idea or innovation attracting interest has to be malleable enough to appeal to an ever increasing variety of always local actant (Latour 1992).

The field of MIS provides a useful example for demonstration. In any given large general business conference many tents are set up for each of the disciplines (accounting, marketing, finance, MIS, etc.). These disciplines converge under the general heading of business, but usually remain within their separate tents. With respect to MIS many willingly gather under the MIS tent, but within the tent are groups with little in common. Qualitative researchers are unlikely to congregate with econometric researchers and econometric researchers are unlikely to associate with statistical researchers. The tent label, MIS, is vague

[1] http://law.lexisnexis.com/ and http://www.bankofamerica.com/. Both sites verified March 4, 2008.

enough to permit local actants to congregate seeing their own local interests being met even though they do so for very different reasons.[2]

What is of interest with the above for the current discussion is that the network does not have an independent goal, it is merely the umbrella under which local actants act and see enough of their interests represented to act and continue to act in alignment with others. It follows from this that outcomes produced by this sort of structure are not the product of an orchestrated or managed design. Instead they are consequences of diverse actions and understandings and the outcomes are often unintended (Latour 1999).

Beck's risk society

Beck's focus is on the source of risk in modern society. Essentially his argument is that risk emerges as a *fait accompli*, not as discussion points on future actions but rather the product of diverse past actions over which there was no broad discussion. Risks emerge over time from gaps between specializations through what he refers to as a division of labor, increasingly narrowly trained and focused experts, creating a "sieve of overspecialization" (Beck 1992, p. 70) with risks emerging through the unconsidered gaps between fields of expert knowledge and attention.

The basis of this argument is that experts translate issues into problems addressable by their expertise and will make decisions that focus on the aspects of the issue that are addressable this way (Beck 1992). Other facets of the issue beyond the skills and knowledge of the applied expertise are underplayed or ignored. The consequence is that if risks emerge later from actions taken no one is actually accountable as each expert has only limited responsibility for their very narrow area of expertise.

Beck argues that action taken with respect to technology is granted a *carte blanche* due to society's faith in progress. Society associates technical progress as equivalent to social progress and grants technology and actions taken with it a "blank check to be honored beyond consent and legitimation" (Beck 1992, p. 203). ANT theorists would argue against this as a source of motivation for action as "faith in progress" is not a reason local actants would cite for their actions. The philosophy underlying these two perspectives are largely incompatible in that Beck speaks about the outcomes from the structural perspective of a distant observer while ANT seeks to understand those outcomes from within, in terms of local actants and networks that produce outcomes through action. Nonetheless, an interesting overlap between the two perspectives lies in the production of unintended consequences with Beck's focus on experts as actants and ANT's conception of spokespersons as entities that claim to define reality through appeals to specialized knowledge and ways of knowing. Latour (1997) noted the linkage between his work and Beck's with specific reference to a general lack of responsibility of locally (narrowly) focused actants (experts) for unintended consequences that later emerge from actions already taken.

Continuing this line of argument, although tapering it with an ANT qualification as to the motivations for action, this sort of progress is "social change institutionalized into a position of non-responsibility" (Beck 1992, p 214). When risks eventually emerge, usually from the interaction of many past decisions made this way, problems appear as 'though from nowhere' and accountability and responsibility cannot be assigned (Beck 1992, p. 61).

This leaves governments to come up with legislation to address the negative consequences of prior decisions that others have taken.

> "The division of labor thus leaves the industries with the primary decision-making power but without responsibility for side-effects, while politics is assigned the task of democratically legitimating decisions it has not taken and of cushioning technology's side effects" (Beck 1992, p. 213)

THE ALIGNMENT OF EXPERTISE

In what follows, Beck's lens is used to exam the focus of actants that would gravitate towards a problem framed as one of privacy and security and then potential consequences are discussed.

Privacy experts

The term privacy has many potential meanings. Privacy could refer to privacy of communications and thoughts (Introna, 1997), privacy of knowledge of and access to one's body (Finestone, 1997), privacy of one's home and personal space

[2] To be careful with credit, the notion of tents and a tent for MIS specifically came up in a discussion after a presentation made by Burt Swanson at the University of Calgary in 2005 or 2006. I do not know if he uses the tent imagery in his publications. He is interested in how forces form around innovations, or not, although he does not to my knowledge use ANT (c.f. Swanson, 2002).

(Shapiro, 1998), the right to be let alone (Warren and Brandies 1890), or the right to be free from the amusement of others (Marcuse 1968).

In practice as well as research privacy has come to assume a very limited and narrow definition. In MIS research, privacy as a topic is narrowly defined as information privacy (Straub and Collins 1990; Stewart and Segars 2002). The same narrow definition of privacy is evident in the use of FIP as privacy's representative, by Canadian private sector organizations (Bell Canada 2007; Equifax Canada 2007; Royal Bank of Canada 2007; The Canadian Marketing Association 2007), US organizations (TRUSTe 2007[3]; Federal Trade Commission 2000) and research (Culnan, 1993; 1999; Smith, Milberg, Burke 1996, Culnan & Bries, 2003).

Yet a review of the eight FIP, developed by the Organization for Economic Cooperation and Development (OECD), reveals that seven contain the word data and none contain the word privacy (Organisation for Economic Co-Operation and Development, 1980). FIP deal exclusively with rules about personal data.

This confusion between big "P" privacy with a broad definition and small "p" privacy as it relates to rules about data is captured by David Flaherty, a respected North American historian who has studied issue of privacy for decades.

> "There is a failure in some cases to distinguish between the broad need for the protection of all aspects of personal privacy and the need for data protection. This situation primarily exists in North America, where data protection laws usually bear the misleading title of Privacy Acts" (Flaherty 1989, p. 377).

In terms of expertise I argue that experts evolve around small "p" privacy as it is the basis of legislation in many instances, but also because it is rule bound. That is, it presents a bounded topic that would attract lawyers, consultants, legislation interpreters, policy makers and others who make their livings being experts on interpreting rules and fashioning solutions that stay within the interpreted confines of those rules. Privacy, framed in terms of FIP translates the issue into one of expertise or rule adherence.

Thus, one of the alignments that form around privacy is a group of experts with a very limited focus on small "p" privacy. These are experts on data protection and the interpretation of rules around data protection. Their focus is not on privacy in any broad sense but on rule interpretation.

Security experts

Security is a broad largely technical field with a long history. Security can come in the form of physical devices such as doors, locks and safes to prevent access to unauthorized others. Less physical security can also be achieved through polices and procedures such as the separation of duties so that, for instance, people authorizing expenditures are not the same people that sign the cheques. Beyond physical and procedural security there are also measures to detect after the fact events, such as end of day cash audits in retail operations and computer logs that keep track of who accessed sensitive material.

Security of computer stored data can also take physical and procedural forms. Physical security could take the form of encryption of data where unauthorized access (deliberate or accidental) would still prevent the disclosure of personal information. Physical security could also include measures that disable the use of peripheral storage devices such as floppy disks or portable USB disk drives to prevent the copying of data. Other measures would include protecting the physical location of computer assets, firewalls, the creation of user accounts and instituting password controls over sensitive data.

Less physical security could include policies and procedures around computer and file access, particularly as it relates to access to and the subsequent use and dissemination of the personal data collected. This form of security would include the creation of logs of activity around data, policies and procedures around authorized access to data, the disposition of data and the handling of tapes and other backup copies of the data. The essential decision-making issue for both physical and procedurals types of security evolves around controlling access to the collected data; determining who is on the 'inside' and should be permitted access to the data and who is on the 'outside' and should be denied access..

This is fine as far as it goes. There is no question that security is important and that organization are legally, ethically and morally obligated to take steps to protect corporate information resources generally and personal information that it possesses about individuals specifically. But the old saying comes to mind, "To a man with a hammer everything looks like a nail". This is the nature of expertise; it is highly focused on a very narrow area. The question arises, "Is there something missing in the focus of experts?"

---

[3] This is evidenced in TRUSTe's web site where a search on "fair information" returned 37 hits, most of them advocating the use of FIP. Verified on March 16, 2007.

An example highlighting the point I am trying to make arose in a review of a version of this paper for a journal. The focus of the paper was similar to this one, raising concerns about the privacy and security conjunction. A reviewer offered the following in downplaying problems with a tight linkage between the terms privacy and security.

> "If we use a simple set theory notation we have one set P that represents all issues to do with privacy, another set S to do with security and an overlap P&S which focuses on the security of private data. Whilst there are clearly some limitations to a too strong focus on S in S&P, I don't think that anyone is really arguing that S covers all P, so any discussion on those aspects of P not covered by S are only meaningful in the context of this journal if they address the technological concerns."

According to this argument, the rest of P is irrelevant if it does not have technological concerns. It is clear in this example that the P in the privacy and security world represents small "p", the security of private data. This is the area of overlap, the area that privacy experts discussed earlier excel in. If big "P" privacy were to seriously be engaged then the Venn diagram would have to be subsumed by something else. It is that something else that I am trying to draw attention to in making these arguments.

RISKS FROM THE SIEVE OF OVERSPECIALIZATION

The concern is that the way that a question is understood or is translated determines the range of viable options considered in addressing it. Privacy as defined by FIP and security are actionable items by experts who are inclined, by the limits of their expertise, to frame and interpret the problem and range of appropriate actions in terms of the tools of their trades. The word privacy, as constituted by enlisted expertise, is replaceable with the expression "data protection" or "access restrictions". Since both alternative expressions can effectively be subsumed under the umbrella activity of security, then the focus of experts is on security. The argument is that if the problem of privacy and security is left to technical experts to address, their expertise will lead to a focus on data protection rules (FIP) and physical and procedural security measures.

Further to this narrowing of one of the central problems to be addressed (privacy reduced to data protection rules), there is a tendency on the part of experts to interpret rules as obstacles to be overcome; for experts to interpret the obligations implied by the rules in a minimal fashion. In a discussion on that point, with respect to privacy legislation, an individual with considerable experience (a former provincial cabinet minister, opposition party leader and privacy commissioner) offered the following comment:

> "That happens so often. The minimum becomes the maximum. … When you get bureaucrats wanting to do something or being asked to do something, they go and interpret the law. That's what they have to do. Any thought of more protection is pretty foreign. Quite often they're being pressured to 'How are we going to get around this?'"[4]

If privacy is seen as a potential obstacle to organizational goals the trick of expertise becomes one of interpreting those obligations as liberally as possible in order to minimize their interference with these goals. This creates the very real possibility that risks will ''fall through the sieve of over specialization" (Beck, 1992, p. 70).

The risks as considered by the organization's experts include the risk of loss of use of the data (it is destroyed), the risk of the loss of exclusive use of the data (it is copied), the exposure of collected data to others, public embarrassment over the handling of data and the resulting potential loss of share value. These are all good and valid concerns, but only one of them has anything to do with the absent others, the individuals supplying the information. That is the exposure of the data to others and the cost of that exposure to individuals.

The unconsidered risks arise from the question as to whether small "p" privacy (data protection) is a separable concept from broader notions of privacy in the lives of individuals. Essentially, "Can we practically sever privacy in the broader context from an exclusive focus on data?" An argument can be made that organizations only deal with personal data and that is all they can and should be concerned about. The problem with this argument lies in the possibility that, in accepting this argument, important threads connecting privacy generally and personal data specifically may be arbitrarily severed to the detriment of and cost to individuals. The essence of the concern is raised in Flaherty's earlier statement, "… There is a failure in some cases to distinguish between the broad need for the protection of all aspects of personal privacy and the need for data protection" (Flaherty 1989, p. 377).

If we consider privacy more broadly as involving the integrity and sanctity of personal spaces and places, of one's body, of one's thoughts, of one's correspondence and associations, of the right to let alone, then there is a direct connection between

[4] This statement was made in a recorded interview with the author.

personal data and these other spheres of the lives of individuals. For instance address information leads to the possibility of violation of one's space, physician name information leads to the possibility of violation of knowledge about one's body and affiliation information creates the potential to violate one's thoughts and associations. All of them and others lead to the possibility of the violation of the right to be let alone. These spheres of the lives of individual are not categorically separable; they are connected spheres. Can we pretend that personal data is categorically separable?

For example, being the subject of identity theft or living with the possibility of this occurring, due to losses or the misuse of personal data, impinges on other spheres of one's life through the time and effort necessary to reverse an identity or financial theft, or the time and concern consumed by monitoring against the possibility. In recent data breaches firms have offered free credit monitoring services to potential identify theft victims. This goes some way to assisting individuals in the monitoring process, but it places a burden of vigilance on individuals that affects other spheres of their lives.

A consequence of thinking about the issue of privacy more holistically is that it raises questions about the problem to be addressed and perhaps the locus of responsibility with respect to who should be involved in making decisions on matters involving personal data. Security experts will generate a range of considered options based on the tradeoffs between securing data and the costs and risks of having it exposed or misused. What they deem to be 'reasonable' will depend on assumptions made about the nature and value of the thing being protected and the resources made available, both financial and in terms of active support.

Referring to the Venn diagram mentioned earlier, its limits and the comments made by the reviewer reflect the narrowness of the focus of experts in defining the parameters of the problem to be addressed. The diagram omits an oversight body that should include organizational generalists (senior management) who define the problem and then identify the expertise required to address it. There is no question that senior management must rely on experts for advice. At the same time, senior management needs to be able to consider the existence of unacknowledged limits placed on the construction of the problem by these experts and therefore limits placed on the range of solutions considered. Stated differently, generalists must be aware of the potential for expert blind spots and answer the questions, "What was the question that needed to be addressed and what was actually addressed by experts?" A subsequent and related question would be, "Did experts translate the problem into one addressable by their expertise and propose solutions to a limited question?"

Admittedly the above is not unproblematic. It assumes that senior managers are generalists enough to be able to probe for the limits of the considerations of the experts. Their own narrowly focused training might make this difficult. An alternative would be to create oversight cross-function and perhaps cross-cultural work groups to independently assess and critique proposed actions, in order to uncover potential expert blindspots or oversights. These oversight groups could be formed from within organizations or by bringing in outsiders. The advantage of gathering other voices is that it provides the opportunity to hear and more importantly to listen to perspectives that might challenge limited conceptualizations and frame the issues differently. The automatic functional argument against these suggestions would centre on the implied assumption that this extension of effort to more fully understand issues of privacy is a distraction that does not serve the interests of shareholders. At the same time, failures in protecting consumer data have hijacked corporate and boardroom agendas and it would seem that questioning and listening before actions are taken might mitigate the potential for the sorts of public relations and financial damages that senior management has had to deal with, resulting from failings in the protection of personal information.

An advantage to thinking of big "P" privacy and including an oversight function around the Venn diagram is a clarification of the problem(s) delegated to experts and independent analysis of the proposed solutions. In addition to the issue of the limits of expertise, it may also be that organizational structure issues may force a limit on what can be considered. For instance, rationally one would expect that part of any data security effort should be an *apriori* or at the very least simultaneous rationalization of data, reducing what has to be protected and thus reducing potential exposure. As decisions about what data has value and what should be collected are operational issues, privacy and security experts on their own may not be able to address data rationalization. They might raise questions around certain data but without a corporate push for a data strategy, they will be left on their own to try and protect everything as best they can with a resulting diffusion of effort that ensures future missteps.

The weakness in this suggestion is recognized. Bringing another group of experts into the puzzle may only reduce the gaps between fields of expertise through which risks emerge. This may be true and if so has merit on that basis alone. In addition it has the potential to at least partially address a sense of unease and disquiet that continually crops up in studying enactments of balance, as discussed at the start of the paper. That is that the scale so easily tips away from privacy in favor of the particular programs of interest. To a considerable degree this occurs because privacy's representative, FIP, is fairly unsubstantial. But there is a potential organizational risk that emerges from this lack of substantial challenge posed by FIP. That is, that the substance of the program of interest has not been challenged and thoroughly examined for its own

substantive value. This leads to an exacerbation of organizational risk unaddressed in the Venn diagram, the time and effort consumed in protecting data of questionable value. The involvement of an oversight body may result in an organizational data strategy and rationalization that would reduce what has to be protected to the critical minimum and underscore the importance of protecting that information.

CONCLUSION

In the last section I tried to argue a position of organizational self-interest in having senior levels of the organization consider big "P" privacy for what it might offer organizations. I also suggest that considering big "P" privacy might help organizations understand how privacy issues might be viewed by a significant number of individuals and hence legislators. This cannot be done in a delegation of the problem to privacy and security experts.

At the end of the day accountability and responsibility for organizational actions rest at the top of the organization. Repeated missteps around personal data suggest that something is missing. It might be argued that big "P" privacy is not the concern of management, along the lines that it is outside management's field of responsibility and concern. Perhaps that is true. Perhaps management is just another form of narrowly focused expertise and there is no way around it.

If that is true, you reap what you sow. I have seen repeatedly in submissions and presentations by business to government committees, on questions of privacy, comments along the following lines, "We want to avoid avoid-heavy handed regulation with unintended consequences. Why use a vise grip when tweezers will do? (Wilder 2001). Why indeed, but you cannot have it both ways. Paraphrasing Beck's earlier comment, politics is left dealing with the consequence of the past actions and decisions of industry for which no responsibility was accepted. Past actions have created another form of risk, politics trying to cushion the side effects.

REFERENCES

1. Beck, U. (1992). Risk Society: Towards a New Modernity. Thousand Oaks, Sage.
2. Bell Canada, (2007). "Security & Privacy", http://www.bell.ca/support/PrsCSrvGnl_Privacy.page, last verified May 19, 2007.
3. Bell Canada (2005). Bell Canada statement on the protection of customer information, Montreal, media release, November 14, 2005.
4. Bonner, W. T. (2006). The Difficulty in Establishing Privacy Rights in the Face of Public Policy from Nowhere, Saskatchewan Institute of Public Policy, Policy Paper # 43, 35 pages.
5. Bonner, W. T. (2007). Locating a Space for Ethics to Appear in Decision-making: Privacy as an Exemplar. *Journal of Business Ethics*, 70, 3, 221-234.
6. Bonner, W. T., Chiasson, M. (2005). If Fair Information Principles are the Answer, what was the Question? An Actor-Network Theory Investigation of the Modern Constitution of Privacy, *Information & Organization* 15, 4, 267-293.
7. Bonner, W. T., Chiasson, M., Gopal, A. (under review). Questioning the practical substance of the concept of balance in privacy, under review (revise and re-submit), 23 pages.
8. Bonner, W. T., Gopal, A. (2001). The Technology Imperative in Education, in N. L. Russo, B. Fitzgerald and J. I. DeGross. (Eds.), *Realigning Research and Practice in Information Systems Development: The Social and Organizational Perspective*. IFIP WG 8.2, Kluwer Academic Publishers, Boston, 439-458.
9. Culnan, M. J. (1993). How Did They Get My Name? An Exploratory Investigation of Consumer
10. Attitudes Toward Secondary Information Use, *MIS Quarterly* 17, 3, 341-363.
11. Culnan, M. J., Armstrong, P. K., (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science*, 10, 1, 104-115.
12. Culnan, M. J., R. J. Bries (2003). Consumer Privacy: Balancing Economic and Justice Considerations, *Journal of Social Issues* 59, 2, 232-342.
13. Equifax (2007). Equifax Canada's Commitment to Privacy. http://www.equifax.com/EFX_Canada/welcome/privacy_full_e.html
14. Federal Trade Commission (2000). Privacy Online: Fair Information Practices in the Electronic Marketplace. Washington, DC.

15. Finestone, S. (1997). Privacy: Where do we Draw the Line? Ottawa, Standing Committee on Human Rights and the Status of Persons with Disabilities**:** Report to the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, Ottawa.
16. Flaherty, D. (1989). Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, The University of North Carolina Press, Chapel Hill.
17. Gatehouse, J. (2005). You are exposed. *MacLean's*, November 21, 2005.
18. Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy in the Information Society, *Metaphilosophy* 28, 3, 259 - 275.
19. Latour, B. (1987). Science in Action: How to Follow Scientists and Engineers Through Society, Harvard University Press, Cambridge.
20. Latour, B. (1992). Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, in W. E. Bijker and J. Law (Eds.) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, 225-259.
21. Latour, B. (1997). A Few Steps Toward an Anthropology of the Iconoclastic Gesture, *Science in Context*, 10, 1, 63-83.
22. Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Harvard University Press, Cambridge.
23. Marcuse, H. (1968). One-dimensional man: studies in the ideology of advanced industrial society, Beacon Press, Boston.
24. Nowell, P. (2005). Bank of America Loses Tapes With Federal Workers' Data. *Washington Post.* Washington**:** Saturday, February 26, 2005, p. E01.
25. Organisation for Economic Co-Operation and Development (1980). Guidelines: On the Protection of Privacy and Transborder of Personal Data. Organisation for Economic Co-Operation and Development, Paris.
26. Raab, C. D., J. Bennett (1998). The Distribution of Privacy Risks, *The Information Society* 14, 4, 263-274.
27. Royal Bank of Canada (2004a and b). The author has hard copies of these online policies.
28. Royal Bank of Canada (2007) "Our Privacy Policy: Ten Privacy Principles", http://www.rbcroyalbank.com/RBC:Rk96II71JsUAAfWeqVQ/privacy/priv_pri.html#two, last verified May 19, 2007.
29. Shapiro, S. (1998). Places and Spaces: The Historical Interaction of Technology, Home and Privacy, *The Information Society* 14, 4, 275-284.
30. Slane, B. H. (2000). Killing the Goose? Information Privacy Issues on the Web. Auckland, Office of the Privacy Commissioner**.**
31. Smith, H. J. (1993). Privacy Policies and Practices: Inside the Organizational Maze, *Communications of the ACM*, 36, 12, 105-122.
32. Smith, H. J., Milberg, S. J., Burke, S. J. (1996). Information Privacy: Measuring Individual Concerns About Organizational Practices, *MIS Quarterly*, 20, 2, 167-196.
33. Stewart, K. A., and Segars, A. H., (2002). An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, 13, 1, 36-49.
34. Straub, D.W., Collins, R.W., (1990). Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy, *MIS Quarterly*, 14, 2, 143-156.
35. Swanson, E. B. (2002). Talking the IS Innovation Walk, in E. H. Wynn, E. A. Whitley, M. D. Myers, J. I. DeGross (Eds.) *Proceedings of the IFIP WG8.2 Working Conference, Global and Organizational Discourse about Information Technology*, December 12-14, 2002, Barcelona, 15-31.
36. The Canadian Marketing Association, "Are You Privacy Compliant?"
    http://www.the-cma.org/public.asp?WCE=C=47|K=223469, last verified on May 19, 2007.
37. Warren, S. D. and L. D. Brandeis (1890). The Right to Privacy, *Harvard Law Review* 4, 5, 193-220.
38. Wilder, C. (2001). The Ethics of Data, *InformationWeek*, May 14, 2001. http://www.informationweek.com/837/prdataethics.htm