PART I

PRIVACY

In the 1970s, Western countries began to grapple with the social implications of new information technologies. Mainframe computers enabled a very few large institutions to collect vast amounts of data about individuals. Many began to worry that these databases would inexorably erode our privacy and subject us to increasingly totalitarian methods of social control. As a corrective, American legal scholar Alan Westin articulated a set of fair information practices to give individuals some level of procedural control over their personal information.

Almost forty years later, these fair information practices have become the standard for privacy protection around the world. And yet, over that same time period, we have seen an exponential growth in the use of surveillance technologies, and our daily interactions are now routinely captured, recorded, and manipulated by small and large institutions alike.

This section begins with a critical examination of the crux of the fair information practices paradigm, the notion that individuals will be able to protect their privacy if their information can only be collected, used, and disclosed with their consent. Ian Kerr, jennifer barrigar, Jacquelyn Burkell, and Katie Black examine the ways in which the consent-gathering process is often engineered to skew individual decision-making, in effect creating an illusion of free choice that helps to legitimatize surveillance practices. Drawing on interdisciplinary work in psychology and decision theory, these contributors argue that the current threshold for consent with respect to the collection, use, and disclosure of personal information is not high enough to protect us from corporate initiatives that invade our privacy.

Philippa Lawson and Mary O'Donoghue examine the same question from a legal perspective, by canvassing the use of consent in Canadian privacy laws in both public sector and private sector contexts. Although private sector legislation provides more scope for negotiation between collectors and individuals, the authors caution that our current reliance on consent as the gold standard for privacy protection may be misplaced because the exercise of that consent is often more notional than real.

Alex Cameron looks at the unintended consequences of fair information practices in the context of digital rights management (DRM) software. He begins with the hypothesis that DRM impedes the individual's right to enjoy creative works in private. He then concludes that the consent provisions in data protection laws may be ineffective in constraining the surveillance capacities of DRM-protected works, in effect making it harder to create an appropriate balance between property rights and privacy rights in digitized spaces.

Rob Carey and Jacquelyn Burkell approach the consent question from a different perspective. They examine the privacy paradox: although people maintain that they are concerned about lack of privacy in digital social networks, they nevertheless reveal information about themselves to relative strangers. Through a heuristics-based analysis, they demonstrate that people are more likely to protect their privacy in the context of their personal relationships and less likely to

protect it when they interact with unknown others, because their assessment of risk in the latter scenario is stripped of the social markers upon which we rely in personal interactions. Accordingly, a heuristics approach helps to explain both aspects of the paradox and suggests that we should be cautious about assuming that the online disclosure of personal information serves as a proxy for consent to its collection, use, and disclosure.

Anne Uteck takes a similar look at the assumptions that are embedded in our enjoyment of spatial privacy. As we move to an age of ubiquitous computing, the signposts we use to negotiate our sense of space, visibility, subjectivity, and privacy are subtly reconstructed. She suggests that we need to develop a more nuanced understanding that can account for our everyday experience of privacy and the expectation that the spaces in which we interact will be protected from unwarranted intrusion.

In like vein, Jason Millar posits that we should revisit our assumptions about knowledge creation in the context of predictive data mining. He argues that the network society has given rise to new forms of knowledge about persons because it enables others to extract data about us from disparate sources and to use that data to create a representation of our beliefs, intentions, and desires even when we did not mean to disclose that information. Millar concludes that policymakers must go beyond mere procedural protections or fair information practices because the context of the original disclosure of the information is lost when it is matched for predictive purposes.

Jennifer Chandler also suggests that our notions of privacy must be reframed in the context of national security. She argues that the traditional juxtaposition of privacy versus security in a zero sum game closes down debate in favor of security before we can fully examine the impact that a given reduction of privacy will have. By accounting for the ways in which privacy enhances our security, she concludes, we will be better able to articulate an appropriate balance that will advance both security and privacy interests.

Daphne Gilbert suggests that part of the problem may be the narrow legal treatment of privacy in constitutional law as part of the legal right to be free of unreasonable search and seizure. She argues that seeking to protect privacy rights through substantive equality guarantees instead of through due process protections may create a foundation for the protection of privacy as an inherent element of human dignity. In doing so, she sets out a useful framework for addressing the original concerns of the 1970s and reconnecting the privacy debate to human rights discourses that seek to protect private life.

Jena McGill advances a similar approach through her examination of the experience of a specific equality-seeking community, abused women. Like Gilbert, she seeks to broaden the scope of the privacy debate by interrogating the feminist rejection of privacy as a means of shielding abusive men from legal sanctions. Grounding her analysis in a deep concern for the lived realities of abused women, she argues that women who are able to establish and defend

boundaries that reflect their needs and desires will be better able to achieve the privacy they require to protect themselves from a battering partner.

Marsha Hanen and Valerie Steeves apply a different lens to the privacy discourse by examining the relationship between privacy and identity. Hanen provides an overview of the ways in which new genetic technologies challenge our traditional understanding of these key concepts. She argues that genomics has the potential to redefine our sense of who we are. We accordingly need to think through the implications of new technologies from a more holistic perspective that accounts for the interaction between people's genomes, the environment, and human dignity.

Steeves returns to the starting point of fair information practices and revisits Westin's theory of privacy as informational control. Incorporating the insights of social theorists, she proposes a new model that defines privacy as a dynamic process of negotiating personal boundaries in intersubjective relations. This may potentially move the policy debate beyond the current impasse of fair information practices, by placing privacy at the heart of the social experience of identity. That experience of identity is the subject of the next section of the book.

1. SOFT SURVEILLANCE, HARD CONSENT
The Law and Psychology of Engineering Consent[+]

IAN KERR, JENNIFER BARRIGAR,
JACQUELYN BURKELL, AND KATIE BLACK

Most contemporary liberal democracies continue to pay lip service to John Stuart Mill's famous *harm principle,* which he articulated as follows:

> [T]he only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not sufficient warrant. He cannot rightfully be compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise, or even right . . . The only part of the conduct of anyone, for which he is amenable to society, is that which concerns others. In the part, which merely concerns him, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign.[1]

The harm principle privileges liberty over self-security. It is Mill's antidote against a state-induced paternalism that would protect people from themselves by treating them as though their personal safety mattered more than their individual liberty.[2] In this sense, one can understand Mill as saying that

> coercion can only be justified to prevent harm to unconsenting others, not to prevent harm to which the actors competently consent. The harm principle creates a 'zone of privacy' for consensual or 'self-regarding' acts, within which

[+] This chapter is adapted from the article "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information," *Canadian Business Law Journal* 40 (2006): 54.

1. John Stuart Mill, *On Liberty* (Boston: Collier and Son, 1909), 13.

2. Peter Suber, "Paternalism," in *Philosophy of Law: An Encyclopedia*, ed. Christopher B. Gray (Garland: Garland Pub. Co, 1999), 632, http://www.earlham.edu/~peters/writing/paternal.htm.

individuals may do what they wish and the state has no business interfering, even with the benevolent motive of a paternalist.[3]

Benevolent paternalism has spurred a number of social and educational programs in various jurisdictions. One well-known example is the increasingly aggressive anti-smoking campaigns across Europe and North America. No stranger to tobacco, one wonders how Mill might feel if he were living in the United Kingdom today and saw a picture of an impotent "cig" on his "pack o' smokes?"[4] While it is true that the British government is not forcing him to quit smoking outright, its paid consultants do provide a rather strong disincentive by suggesting that smoking will lead to undesirable conjugal consequences. If Mill were still kicking around, how long would it take him to sniff out this new brand of paternalism?[5]

Libertarian paternalism, as it has recently been labeled,[6] purports to have Mill's cake and eat it too. The oxymoron is this: while people are "free to choose," they are concurrently provided with cognitive escorts that lead them to do the right thing. *Soft* or *asymmetrical paternalism*,[7] as it is more often called, seeks to invoke self-conscious efforts of public or private institutions to steer peoples' choices in directions that will improve their own welfare. Does the government think its workers should save a portion of their earnings for retirement? No need to ram it down their throats with controversial legislation. Simply change the default rules for a pension program from non-enrollment to automatic enrolment.[8] Human nature (read: inertia) will do the rest. This rather new style of regulating citizens' behavior has emerged

---

3. *Ibid.*

4. "Impotence Warning for Cigarette Packs," *BBC News*, April 20, 2000, http://news.bbc.co.uk/1/hi/health/720359.stm.

5. Gerald Dworkin defines paternalism as "the interference of a state or an individual with another person, against their will, and justified by a claim that the person interfered with will be better off or protected from harm" in Gerald Dworkin, "Paternalism," *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, November 6, 2002 (Revised December 2005), http://plato.stanford.edu/entries/paternalism.

6. Cass Sunstein and Richard Thaler claim that libertarian paternalists should "steer people's choices in welfare promoting directions . . . and might select among the possible options and to assess how much choice is offered" in Cass Sunstein and Richard Thaler, "Libertarian Paternalism Is Not an Oxymoron," *The University of Chicago Law Review* 70, no. 4 (2003): 1159.

7. "The Rise of Soft Paternalism", *The Economist*, April 6, 2006, http://www.economist.com/opinion/displaystory.cfm?story_id=6772346; C. Camerer, et al., "Regulation for Conservatives: Behavioral Economics and the Case for 'Asymmetric Paternalism,'" *University of Pennsylvania Law Review* 1151, no.3 (2003): 1211–1254.

8. "The New Paternalism: The Avuncular State," *The Economist*, April 6 2006, http://www.economist.com/displaystory.cfm?story_id=6768159. Opt-out protocols (where consent is assumed unless explicitly withdrawn) lead to greater rates of consent than do opt-in protocols (where the default is no consent). See E. J. Johnson, S. Bellman, and G. L. Lohse, "Defaults, Framing, and Privacy: Why Opting in ≠ Opting Out," *Marketing Letters* 13, no. 1 (2002): 5. ("Defaults, Framing, and Privacy").

from decades of research suggesting that people are not quite as rational[9] as classical economists once hoped. According to many behavioral economists, people are only *boundedly rational*[10]—an academic term used to articulate and examine human limitations in decision making.

Claiming to know our fallibilities better than we do, soft paternalists do not bother with objectionable prohibitions. Instead, they seek to aid us in making "correct" decisions through persuasion; they guide us toward the alternatives that we would have chosen had we been exercising willpower and foresight.[11] Calling themselves *"choice architects,"* they merely organize "the context in which people make decisions."[12] Emphasizing the social benefits of soft paternalism, the supporters of this approach favor government initiatives that *engineer* peoples' decision making toward a particular outcome while, at the same time, preserving the possibility of choice for those supererogatory actors willing and able to buck the psychological norm.[13] They say this form of paternalism is justified (or at least "softened") by virtue of consent—or, at very least, *a lack of dissent*.

Soft paternalists are not the only ones to have learned from the behavioral sciences. Many businesses and governments involved in the information trade have recently recognized that a kinder and gentler approach to personal information collection works just as well as, if not better than, old-school surveillance. They too are exploiting people's cognitive tendencies in order to persuade them to willingly part with their personal information. Echoing the recent shift in popularity from hard to soft paternalism, both public and private sector surveillance are increasingly relying on what Gary Marx refers to as "soft" measures[14] which "nudge" people toward disclosure.

---

9. Richard Posner defines rationality as "choosing the best means to the chooser's ends" in Richard Posner "Rational Choice, Behavioral Economics, and the Law," *Stanford Law Review* 50 (1997–1998): 50; Edward Glaeser, "Paternalism and Psychology," *University of Chicago Law Review* 73 (2006): 133.

10. Herbert Simon wrote that "boundedly rational agents experience limits in formulating and solving complex problems and in processing (receiving, storing, retrieving, transmitting) information," cited in Oliver Williamson, "The Economies of Organization: The Transaction Cost Approach," *American Journal of Sociology* 87 (1988): 553; the 'bounded' nature of rationality, as per Simon, refers to the fact that people are working with limited time and limited cognitive resources. To be completely rational would require unlimited amounts of at least one of those, if not both. See Christine Jolls, Cass R.Sunstein, and Richard Thaler, "A Behavioral Approach to Law and Economics," *Stanford Law Review* 50 (2004): 1477–79, 1471.

11. "Soft Paternalism: The State Is Looking After You," *The Economist*, April 6 2006, http://www.economist.com/opinion/displaystory.cfm?story_id=6772346.

12. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New Haven: Yale University Press, 2008), 3.

13. *Ibid.*, 5.

14. Gary Marx defines traditional surveillance as "the close observation, especially of a suspected person" and new surveillance as the "scrutiny through the use of technical

This article investigates the nature of soft surveillance and the manner in which organizations are using certain cognitive tendencies to dissuade people from fully actualizing various rights otherwise afforded by data protection and privacy legislation that are based on fair information practice principles (FIPPs). Through an examination of recent interdisciplinary scholarship in the fields of psychology and decision theory, and using Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[15] as a model, we illustrate how the consent-gathering process is often engineered to quietly skew individual decision making while preserving the *illusion* of free choice. After contemplating the importance of setting a high legislative threshold for consent in the collection, use, and disclosure of personal information, we highlight the inadequacies of current privacy laws in dealing with the consequences of soft paternalism and soft surveillance. Through an analysis of the typical decision-making process that occurs when an individual trades personal information in exchange for "free" online services, we suggest that PIPEDA's perceived remedy—the "withdrawal of consent" provisions—will generally provide ineffective relief.[16] Consequently, we articulate the need for a much higher original threshold of consent in privacy law than in the law of contract.

I. SOFT SURVEILLANCE

When one considers the global uptake of the information trade, it is not unreasonable to expect that informational privacy will be to this century what liberty was in the time of John Stuart Mill. Our ability to control the communication of our personal information is globally recognized as an important aspect of personal liberty and self-determination.[17] Yet despite this fact, the data-gathering

---

means to extract or create personal or group data, whether from individuals or contexts" in Gary Marx, "Surveillance and Society", *Encyclopedia of Social Theory*, ed. George Ritzer (Thousand Oaks, CA: Sage Publications, 2005), 817 ("Soft Surveillance and Society"); Soft surveillance, Marx writes, is the use of "persuasion to gain voluntary compliance, universality, and... utilizing hidden or low visibility information collection techniques" in Gary Marx, "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—'Hey Buddy Can You Spare a DNA,'" *Surveillance and Security: Technological Politics and Power in Everyday Life*, ed. T. Monahan, (London, Routledge, 2006), 37. ("Soft Surveillance")

15. Personal Information Protection and Electronic Documents Act SC 2000 c.5 ("PIPEDA")

16. *Ibid.*

17. See, for example, Alan F. Westin, *Privacy and Freedom*, (New York: Athenaeum, 1970), 322; Privacy has historically been conceptualized as a right and has been linked with notions of dignity and autonomy. In 1948, for instance, the United Nations included privacy protections under Article 12 of the Universal Declaration of Human Rights,

process has nevertheless increasingly incorporated itself into people's daily routines, and has therefore become more obfuscated and harder to control.

One reason for this is the increasing engagement of governments and corporations in what Gary Marx has called *mandatory volunteerism*—"disingenuous communications that seek to create the impression that one is volunteering when that really isn't the case."[18] For example, Canadian airports announce:

> Notice: Security measures are being taken to observe and inspect persons. No passengers are obliged to submit to a search of persons or goods if they choose not to board our aircraft.[19]

Empowered by *self-determination*, the passengers can *choose* between volunteering to be searched and not taking their flight, which, in most cases, is not really an option. In other contexts, consumers are asked to "volunteer" their name, address, telephone number, e-mail, and postal code if they want access to online services. Other examples of typical soft surveillance include: recording help-line conversations for "quality assurance purposes"; creating free interactive online characters that play with or teach children by asking them questions about the products their families use;[20] seeking customers' phone numbers when they sign up for a new service in case there are any problems; offering downloads to anyone willing to click "I Agree" to an unending string of boilerplate legalese in an End User License Agreement.

The previous examples present the sharing of personal information as either necessary for improved customer services or as an opportunity to gain the positive feelings associated with "volunteering." Either way, information subjects are led to believe that they can only benefit by providing their data. This illustrates how the architects of soft surveillance, like the architects of other forms of soft paternalism, aim to steer people's choices. However, they do not

---

UNGA, Res 217 A (III) (December 10, 1948), http://www.un.org/Overview/rights.html. Similarly, Article 17 of the 1966 International Covenant on Civil and Political Rights refers to privacy, UNGA, Res. 2200A (XXI) (March 23, 1976), http://www.hrweb.org/legal/cpr.html. Specific data protection regimes include: Council of Europe Directive (EC) ETS No. 108, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981], http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm; Organisation for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html; and Council Directive (EC) 95/46 on the protection of personal data [1995] OJ L 23/31, http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

18. Marx, "Soft Surveillance," 37 (n. 14).

19. *Ibid.*, 37.

20. Ian Kerr and Valerie Steeves, "Virtual Playgrounds and BuddyBots: A Data-Minefield for Tinys and Tweenies," *Canadian Journal of Law and Technology* 4, no. 2 (2005): 91, http://cjlt.dal.ca/vol4_no2/pdfarticles/steeves.pdf.

necessarily do so with regard to improving general social welfare. In many instances, they do it merely as a means of improving their own ability to collect personal information.[21]

Compared to traditional Soviet watchtowers or London's omnipresent CCTV cameras, soft surveillance techniques often have relatively "low visibility, or are invisible."[22] As Marx notes, "With the trend towards ubiquitous computing, surveillance and sensors in one sense disappear into ordinary activities and objects [such as] cars, cell phones, toilets, buildings, clothes, and even bodies."[23] In-car GPS systems transmit information about a person's whereabouts and credit card companies collect data about type, time, and location of purchases via credit card purchases.[24] A person can "volunteer" his or her DNA via a mouth-swab in order to help solve a local crime.[25] These examples illustrate how the employment of universal and automated information collection strategies make it easier for people to "volunteer" comprehensive personal information. Corporations have made the conscious volunteering of personal information more palatable by universalizing the practice. Being asked by a cashier for your phone number is now a common shopping experience.

The universalization of such data collection processes tends to reduce the need for organizations to use coercive measures. Although people often say that they value privacy,[26] their actions seldom reflect this belief.[27] With increasing

21. Where surveillance is for purposes unrelated to increasing the welfare of those being monitored it cannot, strictly speaking, be understood as a form of paternalism (soft or otherwise), since the very justification offered by proponents of paternalism is that it is done for the good of those upon whom it is inflicted. Of course, there are many corporations and governments that try to claim that aggressive surveillance *is* a form of paternalism in that regard. Consider, for example, the following pronouncement by George W. Bush responding to questions about the NSA warrantless surveillance controversy:

> I can fully understand why members of Congress are expressing concerns about civil liberties. I know that. And it's—I share the same concerns. I want to make sure the American people understand, however, that we have an obligation to protect you, and we're doing that and, at the same time, protecting your civil liberties. George W. Bush, (press conference, Washington D.C., December 19, 2005), http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html.

22. Marx, "Soft Surveillance and Society," 817 (n. 14).

23. *Ibid.*

24. *Ibid.*, 818.

25. *Ibid.*, 37 (n. 14). For example, in 2004 male residents in Truro, Massachusetts, were asked in a "non-threatening" manner by police to provide a mouth swab of their genetic material in order to solve a local murder. Citing social responsibility as their main reason for complying, people voluntarily placed their genetic identification into the police dragnet.

26. For example, see Ekos Research Associates, *Privacy Revealed: The Canadian Privacy Survey* (Ottawa, ON, Ekos Research, 1993), 10.

27. According to a recent PEW survey, 60% of all Americans are "very concerned" about privacy, while at the same time 54% have shared personal information in order to

regularity, people are complacently parting with their personal information, readily consenting to its collection regardless of purpose.[28] As data gathering is increasingly incorporated into people's daily routine, it is becoming taken for granted.[29]

While the sway of soft surveillance is superficially innocuous, it is crucial to underscore that most people are oblivious to the influences that they are under, and those who are aware of these influences are easily made to forget them. Though people do in fact retain the freedom to reject the choice that is being *softly* promoted, psychological barriers predictably discourage them from doing so. As Edward Glaeser writes, "[t]he literature on self-control[30] and hyperbolic discounting[31] argues that people would want to refrain from certain actions if they only could. The bounded rationality literature argues that people face severe cognitive limitations and often make bad decisions."[32] The *magic* of soft surveillance (and soft paternalism) is in its *misdirection*: it encourages compliance by co-opting cognitive constraints, all the while maintaining the illusion of choice. While the prevalence of "hard" surveillance remains unchanged, the"culture and practice of social control is changing"[33] as these softer measures become more effective.

---

gain access to a Web site, and an additional 10% are willing to provide this information if asked, cited in: S. Fox, et al., "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," *The PEW Internet and American Life Project*, http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf. (Hereafter called PEW survey). As Oracle C.E.O. Larry Ellison famously said, "Well, this privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy." Larry Ellison, interview by Hank Plante, September 21, 2001, *KPIX-TV News, CBS*.

28. S. Fox, "PEW Survey," *ibid*.

29. Marx, "Soft Surveillance and Society," 817 (n. 14).

30. H.M. Shefrin and Richard Thaler, "An Economic Theory of Self-Control," *The Journal of Political Economy* 89, No. 2 (1981): 392–406, http://ideas.repec.org/a/ucp/jpolec/v89y1981i2p392-406.html.

31. The term *hyperbolic discounting* refers to empirical research demonstrating that people will choose smaller over larger rewards when the smaller reward comes sooner in time. People will choose the larger over the smaller reward when they are to be given in the distant future. For example, "when offered the choice between $50 now and $100 a year from now, most people will choose the immediate $50. However, given the choice between $50 in five years or $100 in six years most people will choose $100 in six years. In addition, given the choice between $50 today and $100 tomorrow, most people will choose $100 tomorrow." See A. Raineri and H. Rachlin, "The Effect of Temporal Constraints on the Value of Money and Other Commodities," *Journal of Behavioral Decision-Making* 6 (1993): 77–94, and David Laibson, "Golden Eggs and Hyperbolic Discounting," *Quarterly Journal of Economics* 112 (1997): 443, 445, and 446.

32. Glaeser, "Paternalism and Psychology," 136 (n. 9).

33. Marx, "Soft Surveillance," 37 (n. 14).

II. THE APPROPRIATE THRESHOLD FOR CONSENT IN PRIVACY LAW

If behaviorists are correct and human choice can indeed be so easily manipulated, the notion of consent becomes privacy's linchpin. Consent is a kind of nexus; it is the interface between human beings and our increasingly automated information-gathering systems. Except where it is unreasonable to require or otherwise inappropriate to obtain, privacy law requires the "knowledge and consent" of individuals for the collection, use, or disclosure of their personal information. Recognizing this, the current Privacy Commissioner of Canada, Jennifer Stoddart, has described consent as "the fundamental principle on which PIPEDA is based."[34]

Although data protection laws around the globe generally require consent prior to the collection, use, or disclosure of most personal information, it is our contention that FIPPs-based privacy laws must be understood as setting higher thresholds for obtaining consent than would otherwise be afforded by way of private ordering.[35] A number of the provisions of PIPEDA illustrate the legislative creation of this higher threshold. Principle 4.3 of Sch. I requires knowledge and consent; the data subject must be said to have *knowingly* consented to the collection, use, or disclosure of personal information, except where inappropriate.[36] This differs markedly from the private law where a party to a contract can be held to its terms even if it has neither read nor understood them. A further provision[37] requires consent to be "obtained in a *meaningful* way, generally requiring that organizations communicate the purposes for collection, so that the person will reasonably know and understand how the information will be collected, used, or disclosed."[38] PIPEDA also creates a higher threshold for consent

34. Jennifer Stoddart, Privacy Commissioner, "An Overview of Canada's New Private Sector Privacy Law: The *Personal Information Protection and Electronic Documents Act*," (speech, Ottawa, ON, April 1, 2004), http://www.privcom.gc.ca/speech/2004/vs/vs_sp-d_040331_e.asp; FIPPs-based law is equally founded upon the principle of consent.

35. For an elaboration of this claim, see generally Ian Kerr, "If Left to Their Own Devices," *In the Public Interest: The Future of Canadian Copyright Law*, ed. Michael Geist, (Toronto, Irwin Law, 2005), 167–211; Ian Kerr, "Hacking at Privacy," *Privacy Law Review*, ed. Michael Geist (Toronto: Butterworth's, 2005), 25–34.

36. PIPEDA, Sch. I, cl. 3 (n. 15).

37. *Ibid.*, cl. 3.2.

38. Kerr, "If Left to their Own Devices," *supra* note 36. See, for example, Case Summary #97, PIPEDA: Bank Adopts Sweeping Changes to Its Information Collection Practices, (2002), [September, 2002], Commissioner's Findings, http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020930_e.asp; It is crucial to note that a substantial number of limits on the high threshold of consent have been placed in s. 7 of PIPEDA. For example, s. 7(1)(b) states that an organization may collect personal information without the knowledge or consent of the individual if "the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province." This provision was cited in the *Eastmond v Canadian Pacific Railway*,

by contemplating different forms of consent depending on the nature of the information and its sensitivity.[39] Information said to be "sensitive" will generally require more detailed reasons justifying its collection and, in some instances, express consent.[40] Moreover, unlike the law of contracts, where consent is seen as a single transactional moment... typically signaling a 'state change' that cannot be 'undone', s. 4.3.8 of Sch. I of PIPEDA generally allows the information subject to withdraw consent at any time.[41] On the basis of these provisions, PIPEDA's consent model is best understood as providing *an ongoing act of agency* to the information subject, and is much more robust than the usual model for consent in private law, which treats consent as an isolated moment of contractual agreement during an information exchange.

Although the collection, use, and disclosure of personal information pursuant to PIPEDA generally require "knowledge and consent,"[42] the notion of consent is nowhere defined in the Act. In its broader common law context, consent is often characterized as "freely given agreement."[43] More specifically, consent is described as

> voluntary agreement by a person in the possession and exercise of sufficient mental capacity to make an intelligent choice to do something proposed by another. It supposes a physical power to act, a moral power of acting, and a serious, determined, and free use of these powers. Consent is implied in every agreement. It is an act unclouded by fraud, duress, or sometimes even mistake.[44]

Because the "voluntary agreement" aspect is so central, consent is often linked to the legal paradigm of contract. The notion of an agreement, contractual or otherwise, usually presupposes some particular aim or object. One never agrees in a vacuum; rather, one agrees *to* something, or *with* something. In private law, certainly in contract law, consent is understood as inherently transactional. It is a definable moment that occurs when the parties crystallize the terms and conditions upon which they agree. Contractual consent is determined at the moment parties

---

2004 F.C. 852 (Cda) 3 regarding Principle 3, where video surveillance was said to be appropriate by Lemieux, J. A factor in the decision was that the camera was minimally invasive and was only looked at if there was a triggering incident. The video was deleted after 96 hours. See paragraph 188.

39. PIPEDA, Sch. I, cl. 3 (n. 15).

40. *Ibid.*; Kerr, "If Left to their Own Devices," (n. 36).

41. "An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice." PIPEDA, (n. 15).

42. *Ibid.*, s. 7.

43. Daphne A. Dukelow and Betsy Nuse, *The Dictionary of Canadian Law*, 2nd ed. (Scarborough, ON, Carswell, 1995), 232.

44. *Black's Law Dictionary*, 5th ed. (Eagan, MN, West Publishing, 1979), 276, s.v. "Consent."

communicate their intention to be bound by that agreement.[45] Whether executed or executory,[46] contractual consent is expressed in an instant. Once the parties have achieved *consensus,* the contract is in place and the obligations become fixed.

Unlike the law of contracts, where consent is seen as a single transactional moment, PIPEDA generally allows the information subject to withdraw consent at any time.[47] PIPEDA is predicated on the notion that individuals have a *right* to control personal information about them. This ongoing right of control is reinforced in law by the corollary requirement of ongoing consent codified in Principle 4.3.8 of PIPEDA.[48] Consequently, unless they surrender it, individuals retain ultimate control over their personal information and can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. [49] Organizations wishing to use personal information must obtain the *ongoing consent* of the information subject for continued use. In other words, the *continued use* of personal information must be understood as a necessary consequence of the information subject's *continuing consent* to its use, and not merely as a consequence of the initial consent to collect the information.

Overall, the consent provisions in PIPEDA strongly suggest that consent acts like a "license" that permits some *limited* collection, use, or disclosure.[50] Thus, the consent given to an organization to use an individual's personal information is necessarily restricted and *does not* give the organization ultimate control over personal information in perpetuity. PIPEDA's Principle 4.5 buttresses this view by disallowing an organization from retaining personal information indefinitely.[51]

---

45. Gerald H. L. Fridman, *The Law of Contract in Canada,* 4th ed. (Scarborough, ON, Carswell, 1999), 16–17; Stephen Waddams, *The Law of Contracts,* 4th ed. (Toronto, Edmond Montgomery Publications, 1999), 66–67.

46. An executory contract is one that has not yet been completely fulfilled by one or more of the parties. Gerald H. L. Fridman, *The Law of Contract in Canada,* 3rd ed. (Scarborough, ON, Carswell, 1994), 108.

47. "An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice." PIPEDA, Sch. I s.4.3.8 (n. 15).

48. PIPEDA, *ibid.*

49. A question arises as to whether this right is alienable; see, for example, James Rule and Lawrence Hunter, "Towards Property Rights in Personal Data," *Visions of Privacy: Policy Choices for the Digital Age,* eds. Colin J. Bennett and Rebecca Grant, (Toronto, University of Toronto Press, 1999).

50. Under PIPEDA Principle 4.2.2, consent is only given for the purposes specified. Under Principle 4.4, these purposes must be appropriately limited, and under Principle 4.5, all uses or disclosures require consent and should be documented as *per* Principle 4.5.1. Almost any new purpose beyond those already specified requires new consent, as set out in Principle 4.2.4. PIPEDA. (n. 15).

51. *Ibid.* PIPEDA Principle 4.5.3 states that personal information that is no longer required to fulfill the identified purposes should not be retained, and requires organizations

This provision, in conjunction with others mentioned previously,[52] is meant to place the individual in control of his or her personal information at all times, signaling that his or her consent is an *ongoing act of agency*. PIPEDA's framework supports this contention as exemplified by the Sch. I Principles. Organizations are to be open about their information management practices,[53] presumably in order for individuals to make informed initial decisions and revisit those decisions when and if necessary.

The ability to withdraw consent is but one of the possible responses available to an individual managing his or her personal information. Individuals also have a right of access to their personal information,[54] and a corresponding right to challenge the accuracy or completeness of that information. Furthermore, individuals have the power to challenge an organization's compliance with the requirements of PIPEDA.[55] They can do this via a complaint to the Privacy Commissioner[56] and, if necessary, by proceeding to Federal Court after the Privacy Commissioner releases a report of her findings on the matter.[57]

III. PSYCHOLOGICAL BARRIERS TO MEANINGFUL CONSENT

Like Mill's harm principle, the theory of consent-as-ongoing-agency articulated above would seem to be a promising antidote to the erosion of individual privacy rights in the age of ubiquitous computing and soft surveillance. Certainly this is what former Privacy Commissioner of Canada Bruce Phillips thought when he proclaimed that Canada's private sector privacy law

> constitutes the first determined effort to place a check upon, and ultimately to reverse, the massive erosion of individual privacy rights brought about by the application of computer and communications technology in the commercial world.[58]

That said, the full potential of the consent model may be compromised in practice due to predictable psychological tendencies that prevent people from giving fully considered consent, and withdrawing it once given. As companies

---

to develop guidelines and implement procedures to govern the destruction of personal information.

52. *Ibid.*
53. PIPEDA, Principle 4.8 (n. 15).
54. *Ibid.*, Principle 4.9 and s. 8.
55. *Ibid.*, Principle 4.10.
56. *Ibid.*, s.12.
57. *Ibid.*, s. 14.
58. Bruce Phillips, "Foreword" in Stephanie Perrin, et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto, Irwin, 2001), ix.

and governments become increasingly adept at automating the consent process, it will be important to understand how psychological factors affect:

(i) A person's ability to consent to the release of his or her personal information
(ii) A company's ability to ensure ongoing consent
(iii) An individual's ability to meaningfully choose to withdraw consent.

Such an investigation, thus far absent in the Canadian privacy law and policy literature, is essential. It is important because a systemic failure in the consent process, not to mention the failure to provide a meaningful opportunity to exercise the right to withdraw consent, reduces the consent principle to little more than the transactional moment of private ordering, thereby rendering the interpretation and application of PIPEDA's new, robust, ongoing consent provisions practically useless.

To illustrate the kind of psychological constraints that people face, let's consider a hypothetical situation that addresses the following question:
Why do people consent to an organization's demand for personal information and then, generally, not review, revise, or withdraw their consent?
To answer this question, let's construct a hypothetical model citizen named Jijk. Jijk is representative of the majority of North Americans who are "very concerned about privacy."[59] Recently, Jijk's friend recommended that she follow a breaking story in the *Globe and Mail* by setting up a "keyword alert" on the *Globe* website that automatically sends her relevant stories by email.[60] The website offers this service for free—*with one catch*: Jijk has to register as a member by providing and consenting to the *Globe*'s use of her personal information. Jijk faces a common dilemma. In order to gain the immediate benefit of the alerting service, she must accept the loss of control over her informational privacy. Having a basic understanding of privacy law, Jijk knows that if she chooses to consent to the use of her personal information, she can, at any time, withdraw her consent. Presumably, Jijk will provide the required personal information and offer her consent if the perceived benefits of the alerting service outweigh the perceived costs. If Jijk later decides to reconsider her initial decision, she will undertake a new comparison of gains and losses, evaluated from her status as a *Globe and Mail* member.

Will Jijk provide her personal information and consent to its use in order to have the *Globe and Mail* alert her to relevant articles? If she does, will she ever withdraw her consent? Much will depend on various psychological factors influencing how Jijk makes these decisions. Our analysis suggests that in the context of privacy decisions such as this, psychological factors combine to increase

59. See Marx, "Soft Surveillance," (n. 14).
60. *Globe and Mail*, http://www.theglobeandmail.com. (Hereafter *Globe*)

the likelihood that consent will be offered initially, and reduce the likelihood that, once given, it will be withdrawn.[61]

In considering her initial consent, Jijk wants, and stands immediately to gain, the value associated with the alerting service. Against this benefit, she must weigh the subjective value of the loss of control over her personal information. Although the ramifications of this loss are significant, these consequences will occur only in the future. For example, Jijk is likely to receive targeted marketing materials as a result of her consent, but these materials will not arrive immediately upon consent, and they are likely only to *add* to the other materials that Jijk receives on a regular basis. In contrast, if Jijk is considering the withdrawal of consent, she knows that the result of this decision would be the immediate *loss* of the alerting service provided by the *Globe and Mail* and the temporally distant, ephemeral, and potentially partially illusory *gain* of control over her personal information.[62] The consequences of regaining control of personal information will be, for the most part, invisible to Jijk, manifesting in the future *absence* of some (obviously not all) of the targeted marketing materials that she regularly receives.

It is well known in decision theory that *subjective utility*—that is, the personal value of an outcome—changes depending on *when* the outcome will be experienced.[63] In particular, the subjective value of a benefit or loss that will be experienced today is *greater* than the subjective value of that same benefit or loss if we know that it will be experienced some time in the future. While the exact form of this discounting function is the subject of much debate,[64] the existence of discounting is universally accepted. Furthermore, and critically for the current discussion, the literature on decision making also suggests that although both gains and losses lose value as they are moved into the future, the *rate* of change is faster for gains than for losses: losses become less bad the further away they are in time, while gains become *much* less good.[65] In considering her initial consent, Jijk is evaluating an immediate gain against a temporally distant loss of privacy, rendered less negative precisely because it occurs in the future. As a result, she is *more* likely to offer her consent than if both outcomes occurred at the same time. In contrast, when considering withdrawal of consent, Jijk is

61. E. J. Johnson, S. Bellman, and G. L. Lohse, "Defaults, Framing, and Privacy," (n. 8).

62. The benefit could be partially illusory if her information has already been provided, with consent, to a third party.

63. See G. F. Loewenstein and J. Elster, *Choice Over Time*, (New York, Russell Sage Foundation, 1992).

64. U. Benzion, Y. Schachmurove, and J. Yagil, "Subjective Discount Functions: An Experimental Approach," *Applied Financial Economics*: 14, no. 5 (2004): 299.

65. See, for example, M. Ortendahl, and J. F. Fries, "Time-Related Issues with Application to Health Gains and Losses," *Journal of Clinical Epidemiology* 55 (2002): 843; R. H. Thaler, "Some empirical evidence on dynamic inconsistency," *Economic Letters* 8 (1981): 201.

weighing an immediate loss against a temporally distant gain whose value is *much* reduced because it occurs in the future. In this case, Jijk is *less* likely to withdraw her consent than she would be if loss and gain both occurred immediately.

Other aspects of the situation could have the similar effect of biasing Jijk's decisions *against* withdrawing consent. Bias arises from what is, essentially, a re-weighting of the gains and losses associated with consent after the initial decision has been made. It is a direct result of the decision itself. According to *prospect theory*,[66] decisions are made in a context where losses loom larger than gains, and outcomes are evaluated against an anchor point or implicit comparator. If the decision under consideration is whether to offer consent in the first place, Jijk's potential immediate outcome is a gain: currently, Jijk *does not* have benefit of the alerting service that she wants, and by consenting she gains that service. By contrast, if her decision is whether to withdraw consent, Jijk's potential immediate outcome is the loss of the alerting service that she currently enjoys. Prospect theory states that losses are weighted more heavily in decision making than are gains. By extension, the negative value of the loss of the alerting service if consent were withdrawn would be greater than the positive value of the service gained when consent was initially offered. Such an outcome is also known as the *endowment effect*. It is reflected in the tendency to value an object more when one owns it.[67] In Jijk's case, it results in an increased subjective value of the alerting service once she has activated it by becoming a *Globe* member. As the subjective value of the service increases, Jijk becomes more loathe to lose it by withdrawing her consent.

Another psychological factor known as *cognitive dissonance*[68] will also cause Jijk to re-weigh the gains and losses associated with her initial consent. This, in turn, will affect her decision whether to later withdraw her consent. According to the theory of cognitive dissonance, having inconsistent beliefs or acting in a way that is inconsistent with one's beliefs can give rise to an uncomfortable psychological state. Jijk likes to think of herself as a consistent person, making careful and considered choices based on her values. Yet, if she has consented to the sweeping use of her personal information in return for the alerting service offered by the *Globe* online, she has acted in a way that is inconsistent with her own values. She is not alone in this inconsistency. According to a recent PEW survey, 60% of all Americans are "very concerned" about privacy, while at the

66. D. Kahneman and A. Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47, no.2 (1979): 263.

67. Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler, "Experimental Tests of the Endowment Effect and the Coase Theorem," *Journal of Political Economy* 98, no. 6 (1990): 1325.

68. L. Festinger, *A Theory of Cognitive Dissonance* (Palo Alto, CA, Stanford University Press, 1957); L. Festinger, *Conflict, Decision, and Dissonance* (Stanford, CA, Stanford University Press, 1964).

same time 54% have shared personal information in order to get access to a web site, and an additional 10% are willing to provide this information if asked.[69] Therefore, at least one quarter of those surveyed have acted or are prepared to act with inconsistency similar to Jijk's.

Such inconsistency can be psychologically uncomfortable: people generally don't enjoy feeling like hypocrites. Moreover, Jijk finds herself in a situation that has all the hallmarks of one that is likely to cause this discomfort:[70]

(i) Jijk feels personally responsible for her own decision to consent, and thus cannot blame her actions on someone or something else.
(ii) Jijk understands that, as a direct result of her decision, her privacy, which is something she values, has been compromised.
(iii) The justification for her decision is relatively weak since she could, with little effort, have followed the breaking news story through other means.
(iv) She has clearly made a free choice to release her personal information.[71]

In the context of information privacy, cognitive dissonance becomes problematic in the way people seek to alleviate the discomfort they experience. Psychological research suggests that people resolve cognitive dissonance through one of three mechanisms.[72] Jijk might trivialize some of her competing cognitions by convincing herself that the privacy violation in this case is not important, or that privacy itself is overvalued.[73] Alternatively, Jijk could selectively seek information consistent with her decision.[74] In the current situation, this might mean that Jijk would selectively search for and attend to information suggesting that the collection and use of personal information by the *Globe* does *not* constitute a privacy violation, since the *Globe* has a privacy policy and therefore they *must* be privacy compliant.[75] As a third possibility, Jijk might decide to change her

69. See Ekos, *Privacy Revealed*, (n. 27).

70. J. Cooper and R. H. Fazio, "A New Look at Dissonance," *Advances in Experimental Social Psychology* 17 (2004): 227.

71. E. Harmon-Jones, J. W. Brehm, J. Greenberg, L. Simon, and D. E. Nelson, "Evidence That the Production of Aversive Consequences Is Not Necessary to Create Cognitive Dissonance," *Journal of Personality and Social Psychology* 70, no. 1 (1996): 5.

72. See J. W. Brehm and A. R. Cohen, *Explorations in Cognitive Dissonance* (New York: Wiley, 1962); L. Festinger, *A Theory of Cognitive Dissonance*, (Stanford, CA: Stanford University Press, 1957).

73. L. Simon, J. Greenberg, and J. Brehm, "Trivialization: The Forgotten Mode of Dissonance Reduction" *Journal of Personality and Social Psychology* 68 (1995): 247.

74. D. Ehrlich, I. Guttman, P. Schonbach, and J. Mills, "Post Decision Exposure to Relevant Information" *Journal of Abnormal and Social Psychology* 54 (1951): 98.

75. Jacquelyn Burkell and Valerie Steeves, "Privacy Policies on Kids' Favourite Web Sites," (paper, 6th Annual Privacy and Security Workshop, Privacy and

attitude, opinion, or behavior.[76] She could, for example, modify her attitude toward information privacy by considering privacy to be less important, or she could perhaps place less value on her privacy with regard to the particular information she disclosed to the *Globe*.

Each of these resolutions would mitigate the psychological discomfort associated with offering consent. At the same time, each reduces the likelihood that Jijk will later withdraw her consent. In fact, once she has successfully resolved the dissonance, there is little reason for her to go back and revisit her original decision: after all, she now perceives the initial consent as consistent with the only value that would lead her to revoke it (that is, her valuing of privacy). This is not to say that she *couldn't* withdraw her consent. She *could*. However, the principle of cognitive dissonance suggests that she may not be motivated to do so. It is safe to assume that the architects of soft surveillance are generally aware of this and exploit it.

IV. CONCLUSION

Cognitive dissonance, prospect theory, and discounted subjective utility have been shown to apply to decision making in a wide variety of contexts, and there is every reason to think that they are also applicable to decisions about giving or later withdrawing consent.[77] These theories predict a variety of decision biases that would facilitate the *social engineering of choice*: leading individuals in a particular direction when making an initial decision and encouraging them thereafter to maintain the status quo.[78] Together, these theories illustrate how psychological factors tend to *increase* the likelihood of initial consent and form cognitive barriers to the later withdrawal of consent.

Acquisti and Grossklags argue, "we need to incorporate more accurate models of users' behavior into the formulation of both policy and technology."[79] In the privacy

---

Security: Disclosure, University of Toronto, November 3, 2005), http://idtrail.org/content/blogcategory/21/72/.

76. A. Elliot and P. Devine, "On the Motivational Nature of Cognitive Dissonance as Psychological Discomfort," *Journal of Personality and Social Psychology* 67 (1994): 382.

77. C. Camerer, "Prospect Theory in the Wild," *Choices, Values and Frames*, eds. Kahneman and A. Tversky, (Cambridge, Cambridge University Press, 2000), 288–300.

78. This is reflected in the endowment effect.

79. A. Acquisti and J. Grossklags, "Privacy Attitudes and Privacy Behavior," *The Economics of Information Security: Advances in Information Security, vol. 12*, eds. J. Camp and S.R. Lewis, 12, (Massachusetts, Norwell, and Kluwer, Springer, 2004), 176; For an article which explores the wisdom of government attempts to debias people's decision making via the law, see Christine Jolls and Cass R. Sunstein, "Debiasing through Law," *Working Paper No. 225* (working paper, University of Chicago Law and Economics, November 2005), http://ssrn.com/abstract=590929.

context, this point cannot be overemphasized. Decision biases, created by the psychological factors discussed in this chapter, have obvious implications for any theory of meaningful consent and necessarily affect consent-based policy. If privacy legislation is aimed at providing people with meaningful control over their personal information, it must employ a model of consent formation that accurately reflects people's behavior. The following reasons illustrate why such legislation cannot force people to behave according to a theoretical model of consent. First, it is difficult to disabuse decision makers of the biases and heuristics that influence their decision making. Second, one cannot expect individuals who are unaware of the implications of consenting to the collection, use, or disclosure of personal information to recognize, let alone remedy, their tendency to "stick with" their initial consent. Third, many people currently share a general impression that consenting to the use of personal information is an all-or-nothing, take-it-or-leave-it, instantaneous transaction; an offer that they cannot refuse.

The consent model for PIPEDA and similar FIPPs-based legislation, properly understood, has some ability to respond to these concerns. Recognizing privacy law's higher threshold for consent provides the fulcrum for understanding data protection regimes as more than just default contracting rules in the information trade. By providing a regime premised on the notion of consent-as-ongoing-agency, FIPPs-based privacy laws require that organizations revise many of their current practices and policies. Unfortunately, most organizations continue to treat consent as a transactional moment, using standard-form, click-wrap agreements as a means of obtaining overarching "consent" (read: assent) to excessive collection, use, and disclosure of personal information. This archaic, nineteenth-century, laissez-faire, freedom-to-contract mentality fails to recognize the higher threshold assigned to consent in the privacy law context.[80] It also fails to recognize the unique role that consent is meant to play as the nexus between people and information technology.

Information-seeking institutions engaged in soft paternalism and soft surveillance will obviously prefer consent to be conceived of as a transactional moment. This approach allows them to engineer the consent-seeking process so that individuals are steered toward automatically offering up their consent to the collection, use, and disclosure of their personal information without further reflection. The increasing use of soft surveillance indicates that governments and corporations have begun to realize the behavioral consequences of the psychological tendencies discussed in this chapter. Whether soft paternalism is used to increase pension contributions or soft surveillance is employed in the interests of airport security, corporations and governments are becoming *psych-savvy*. They are increasingly adept at harnessing people's cognitive tendencies to further their own ends.

80. For an articulation of this thesis in the context of consent to the collection of personal information in digital rights management situations, see Kerr, "If Left to Their Own Devices" and Kerr, "Hacking at Privacy," (n. 36).

Although there have been a number of complaints about the limitations of PIPEDA resulting from the compromises that were made during its enactment,[81] the Act does inspire the possibility of a much more robust and meaningful threshold for consent. The Government of Canada's statutory review of PIPEDA[82] provided an important opportunity to examine what further improvements, and what additional institutions, are required to more fully articulate and enforce privacy law's higher threshold of consent so that it lives up to the Privacy Commissioner of Canada's claim that it is "the fundamental principle on which PIPEDA is based."[83]

---

81. The recognition of the need for PIPEDA sprang, in part, from concern about maintaining and facilitating Canada's international trading relationship. It was enacted under the federal trade and commerce power and focused primarily on commercial activities. The CSA Model Code for the Protection of Personal Information which forms Schedule 1 of the Act was the result of a process in which business was intimately involved. See Christopher Berzins, "Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building," *Queen's Law Journal* 27 (2002): 623 for a discussion of these tensions; Michael Geist, for example, criticizes the ombudsman's approach to the enforcement of PIPEDA. He argues that the Privacy Commissioner's inability to issue binding decisions means that there is insufficient incentive for companies to comply. See Michael Geist, "Canada's Privacy Wakeup Call," November 27, 2005, http://michaelgeist.ca/component/option.com_content/task,view/id,1025/Itemid,70; see also, Canadian Internet Policy and Public Interest Clinic, "Five Year Review: An Opportunity to be Grasped", July 2005, http://www.cippic.ca/en/action-items/pl_article_for_cplr_july_2005.pdf.

82. Mandated to be held five years after its introduction, as required by PIPEDA s.29, *supra* note 15 and completed in May 2007. In preparation for the review, the Commissioner released a PIPEDA Review Discussion Document that raised many questions about consent, including what she termed blanket consent where she addressed various understandings of consent`s duration and intent, including a reading of the Act that argues that "informed consent is a dynamic process that involves keeping individuals actively aware—on an ongoing basis, using understandable language, and in a transparent manner—of what an organization intends to do with their personal information and for what purpose. They may see consent as giving them the opportunity to receive further explanations and to ask questions or challenge assumptions—particularly in relationships of unequal bargaining power." Office of the Privacy Commissioner of Canada, "Protecting Privacy in an Intrusive World," section f, July 2006, http://www.privcom.gc.ca/parl/2006/pipeda_review_060718_e.asp#005. Although the Commissioner did indicate in her PIPEDA Review submission to Parliament that Blanket Consent was an area in which she was open to receiving guidance, neither the ETHI Committee Report "Standing Committee Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)," May 2007, http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04-e.html nor the consultation initiated in the "Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics," 2007, http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf have addressed this issue.

83 "An overview of Canada's new private sector privacy law: The *Personal Information Protection and Electronic Documents Act*," see note 35.