

SOFT SURVEILLANCE, HARD CONSENT ⁺

Ian Kerr, * Jennifer Barrigar, ** Jacquelyn Burkell, *** 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 himself, 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 individuals may do what they wish and the state has no business interfering, even with the benevolent motive of a paternalist.³

No stranger to tobacco, one wonders how Mill might feel if he were living in the UK 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*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 paternalism*, 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-enrolment to automatic enrolment.⁷ Human nature (read: inertia) will do the rest. This rather new style of regulating citizens' behaviour has emerged from

decades of research suggesting people are not quite as rational⁸ as classical economists once hoped. According to many behavioral economists, people are only *boundedly rational*⁹ -- 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; they guide us towards the alternatives that we would-have-chosen had we been exercising will-power and foresight.¹⁰ Emphasizing the social benefits of soft paternalism, the supporters of this approach favour 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.¹¹ 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 and 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.¹²

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 Canadian privacy law, with a special focus on the *Personal Information Protection and Electronic Documents Act (PIPEDA)* specifically.¹³ Through an examination of recent interdisciplinary scholarship in the fields of psychology and decision theory, we demonstrate that consent-gathering processes are often engineered to quietly skew individual decision-making while preserving the *illusion* of free choice. After contemplating the importance of setting a high 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. In our analysis of a typical decision-making process (trading personal information in exchange for “free” online services), we conclude that *PIPEDA*’s perceived remedy – the “withdrawal of consent” provisions – will not generally provide effective relief.¹⁴ Consequently, we articulate the need for a much higher original threshold of consent in privacy law than in contract law.

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 determine for ourselves when, how, and to what extent our personal information is communicated¹⁵ is globally recognized as an important aspect

of personal liberty and self-determination.¹⁶ Nevertheless, the data gathering process is increasingly incorporated 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.”¹⁷ 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.”¹⁸

Empowered by *self-determination*, the passenger can *choose* between volunteering to be searched and not taking their flight. (Yeah, right.) In other contexts, consumers are asked to “volunteer” their name, address, telephone number, email, and postal code, if they want access to online services. Other examples of typical soft surveillance include: recording help-line conversations for customers’ “quality assurance purposes;” creating free interactive online characters that play with or teach children by asking them questions about the products their families use;¹⁹ 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 above examples present the sharing of personal information as either necessary for improved customer services or an opportunity gain the positive feelings associated with “volunteering”: the informational subject can only benefit by providing their data. This illustrates how, like soft paternalists, the architects of soft surveillance also aim to steer people's choices. However, they do not 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.²⁰

Compared to traditional Soviet watchtowers or London's omnipresent CCTV cameras, soft surveillance techniques often have relatively “low visibility, or are invisible.”²¹ As Marx notes, “[w]ith 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.”²² 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.²³ A person can volunteer their D.N.A. via a mouth-swab in order to help solve a local crime.²⁴ These examples illustrate how the employment of universal and automated information collection strategies make it easier for people to “volunteer” very 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 data collection often reduces the need for organizations to use coercive measures. People often say that they value privacy,²⁵ yet their actions seldom reflect this belief.²⁶ With increasing regularity, people are complacently parting with their personal information, readily consenting to its collection, regardless of purpose.²⁷ As data gathering is increasingly incorporated into people's daily routine, it is becoming taken for granted.²⁸

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. 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-control²⁹ and hyperbolic discounting³⁰ 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.”³¹ 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”³² as these softer measures become more effective.

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 and dissemination tools. Consent purports to act as a kind of guardian of personal information. Except where it is unreasonable to require or otherwise inappropriate to obtain, privacy law requires the “knowledge and consent” of an individual for the collection, use, or disclosure of her personal information. Recognizing this, the current Privacy Commissioner of Canada, Jennifer Stoddart, has described consent as “the fundamental principle on which *PIPEDA* is based.”³³

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 privacy laws based on *Fair Information Practice Principles* (FIPPs) must be understood as setting higher thresholds for obtaining consent than would otherwise be afforded by way of private ordering.³⁴ 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* consent to the collection, use, or disclosure of personal information, except where inappropriate.³⁵ 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 provision³⁶ 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.”³⁷ *PIPEDA* also creates a higher threshold for consent by contemplating “different forms of consent depending on the

nature of the information and its sensitivity.³⁸ Information said to be “sensitive” will generally require more detailed” reasons justifying its collection and, in some instances, express consent.³⁹ 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.⁴⁰ On basis of these provisions, *PIPEDA*’s consent model is best understood as providing *an ongoing act of agency* to the information subject and is a 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,”⁴¹ the notion of consent is nowhere defined in the Act. In its broader common law context, consent is often characterized as “freely given agreement.”⁴² 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.⁴³

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 communicate their intention to be bound by that agreement.⁴⁴ Whether executed or executory,⁴⁵ 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.⁴⁶ *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*.⁴⁷ Consequently, unless they surrender it,⁴⁸ individuals retain ultimate control over their personal information and can withdraw consent at any time.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.

Taken altogether, 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. Principle 4.5 buttresses this view by disallowing an organization from retaining personal information indefinitely.⁵¹ This provision, in conjunction with others mentioned above,⁵² is meant to place the individual in control of her personal information at all times signaling that 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 her personal information. Individuals also have a right of access to their personal information⁵⁴ 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 Commissioner⁵⁶ and, if necessary, by proceeding to Federal Court after the Privacy Commissioner releases a report of her findings in 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 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 her personal information; (ii) a company’s ability to ensure ongoing-consent; and (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’s important because a systemic failure in the consent process, not to mention an 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?*

Jij is representative of the majority of North Americans who are "very concerned about privacy."⁵⁹ Recently, Jij's friend recommended that she read a series of articles posted on the *Globe and Mail* website which, from the articles' titles, looked interesting.⁶⁰ The website offers immediate access – *with two catches*: Jij has to pay 4.95\$ and register as a user by providing and consenting to the *Globe*'s use of her personal information. Jij faces a common dilemma. In order to gain the immediate benefit of reading the articles she must accept the loss of both a little money and control over her informational privacy. Having a basic understanding of privacy law, Jij knows that if she chooses to consent to the use of her personal information, she can, at any time, withdraw her consent.

Will Jij provide her personal information and consent to its use in order to read the article? If she does, will she ever withdraw her consent after the articles are read? Much will depend on various psychological factors influencing how Jij makes these decisions. Our analysis suggests that in the context of privacy decisions such as this, these factors combine to increase the likelihood that consent will be offered initially, and reduce the likelihood that, once given, it will be withdrawn.⁶¹

Typically, an individual considering initial consent weighs the subjective value of an immediate *gain* (e.g., of access to the *Globe and Mail*) against the subjective value of a less salient *loss* (e.g., control over personal information). Although the ramifications of the loss are significant, these consequences occur in the future and as a result have less impact on the decision. In contrast, withdrawing consent typically results in the immediate *loss* of access to the article and the relatively distant, ephemeral, and potentially partially illusory *gain* of control over her personal information.⁶² Consequently, it is important to consider *when*, and to some extent *whether*, Jij experiences the benefits and losses associated with her decisions about consent.

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 Jij experiences today is *greater* than the current subjective value of that same benefit or loss received some time in the future. While the exact form of this discounting function is subject of much debate,⁶⁴ the existence of discounting is universally accepted. So, when making her initial decision, in a sense Jij is weighing an immediate benefit (being able to read the articles) against a loss of information privacy whose effects are somewhat removed, both temporally and in terms of overall salience. The result is that the negative value of the privacy loss is reduced because it occurs in the future, and the value of this loss relative to the gain of

access to the article is reduced. This, in turn, makes it more likely that Jij to initially consent to the collection of her personal information.

In contrast, a decision to withdraw consent involves a comparison between an immediate loss of access and a distant and ephemeral benefit of regaining control of her information. She will no longer be able to access the articles.⁶⁵ In this case, discounting tends to discourage her from withdrawing her consent. The literature on decision theory 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.⁶⁶ When Jij considers the decision to withdraw consent, the loss associated with being denied access is tangibly immediate; the gain of regaining control of her information, however, is not. The value of the gain is reduced to the extent that she sees the privacy protection being realized in the future. This effect is magnified by the difference in the rate of change between losses and gains; because it is a *gain* that is distant in time, is it devalued at a faster rate than a *loss*.

Other aspects of the situation could have the similar effect of biasing Jij'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's a direct result of the decision itself. According to *prospect theory*,⁶⁷ 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, prospect theory predicts that the most salient effect is the immediate gain: currently, Jij *doesn't* have access to the information she wants and by consenting, she gains that access. By contrast, if her decision were to withdraw consent, it is likely that the most salient outcome would be the *loss* of access. Prospect theory states that losses are weighted more heavily in decision making than are gains. By extension, when consent is withdrawn, the negative value of the loss of access would be greater than the positive value of access 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.⁶⁸ In Jij's case, it results in her placing increased importance on the ability to access the *Globe's* online articles once she has gained the ability to do so.

Another psychological factor known as *cognitive dissonance*⁶⁹ will also cause Jij to re-weight the gains and losses associated with her initial consent. This, in turn, will effect 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. Jij 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 access to the *Globe* online, she has acted in a way that was 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 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.⁷⁰ Therefore, at least one quarter of those surveyed have acted or are prepared to act with inconsistency similar to Jij's.

Such inconsistency can be psychologically uncomfortable: people generally don't enjoy feeling like hypocrites. Moreover, Jij finds herself in a situation that has all the hallmarks of one that is likely to cause this discomfort:⁷¹ (i) Jij feels personally responsible for her own decision to consent and thus cannot blame her actions on someone or something else; (ii) Jij 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 relatively little effort, have accessed the article through other means; and (iv) she has clearly made a free choice to release her personal information.⁷²

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.⁷³ Jij 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.⁷⁴ Alternatively, Jij could selectively seek information consistent with her decision. In the realm of consumption, this translates into selective attention to positive product information regarding a chosen alternative.⁷⁵ In the current situation, this might mean that Jij 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.⁷⁶ As a third possibility, Jij might decide to change her attitude, opinion, or behaviour.⁷⁷ 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 Jij's current state of psychological discomfort; however, each reduces the likelihood that Jij 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 consent: after all, she now perceives the initial decision 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 to their own ends.

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 no reason to think that they are not also applicable to decisions about giving or later withdrawing consent.⁷⁸ 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.⁷⁹ 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 that “we need to incorporate more accurate models of users’ behavior into the formulation of both policy and technology.”⁸⁰ In the privacy context, this point cannot be overemphasized. Decision biases, created by the psychological factors discussed above, have obvious implications for any theory of meaningful consent and necessarily effect consent-based policy. If privacy legislation is to 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 can’t 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 legislations, properly understood, has some ability to respond to the above 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, clickwrap agreements as a means of obtaining overarching “consent” (read: assent) to excessive collection, use and disclosure of personal information. This archaic, 19th century, laissez-faire, freedom-to-contract mentality fails to recognize the higher threshold assigned to consent in the privacy law context.⁸¹ 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 towards 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 article. 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.

Although there have been a number of complaints about the limitations of *PIPEDA* resulting from the compromises that were made during its enactment,⁸² the Act does inspire the possibility of a much more robust and meaningful threshold for consent. As

the Government of Canada moves towards its statutory review of *PIPEDA*,⁸³ it is time to start thinking more deeply about 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."⁸⁴

⁺ This article is adapted from "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information," forthcoming in (2006) 40 *Canadian Business Law Journal*. The authors wish to extend gratitude to the Social Sciences and Humanities Research Council, the Canada Research Chairs program, Bell Canada and the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of the research project from which this article derives.

^{*} Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa (iankerr@uottawa.ca).

^{**} LL.M. (Law and Technology), University of Ottawa; Legal Counsel, Office of the Privacy Commissioner of Canada (jbarr072@uottawa.ca). The opinions expressed in this article are personal and do not represent those of the Office of the Privacy Commissioner of Canada nor bind that Office in any way.

^{***} Associate Professor, Faculty of Information and Media Studies, The University of Western Ontario (jburkell@uwo.ca).

^{****} LL.B. candidate, Faculty of Law, University of Ottawa (kblac044@uottawa.ca).

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

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

³ *Ibid.*

⁴ "Impotence warning for cigarette packs" *BBC News* (20 April 2000), online: *BBC News* <<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 Edward N. Zalta, ed., *The Stanford Encyclopedia of Philosophy*, Spring 2006 ed. (Stanford: Metaphysical Research Lab Stanford University, 2006) s.v. "paternalism", online: <<http://plato.stanford.edu/cgi-bin/webglimpse.cgi?ID=1&nonascii=on&maxfiles=50&maxlines=30&maxchars=10000&query=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 Sunstein and Richard Thaler, "Libertarian Paternalism Is Not an Oxymoron" (2003) 70(4) *The University of Chicago Law Review* 1159.

⁷ "The new paternalism: The avuncular state", *The Economist* (6 April 2006), online: *The Economist* <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, & G. L. Lohse "Defaults, Framing, and Privacy: Why Opting in ≠ Opting Out" (2002) 13(1) *Marketing Letters* 5.

⁸ Richard Posner defines rationality as "choosing the best means to the chooser's ends" in Richard Posner "Rational Choice, Behavioral Economics, and the Law" (1997-1998) 50 *Stan. L. Rev.* 1551; Edward Glaeser, "Paternalism and Psychology" (2006) 73 *University of Chicago Law Rev.* 133.

⁹ 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 Economics of Organization: The Transaction Cost Approach" (1988) 87 *American Journal of Sociology* 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.

¹⁰ "Soft Paternalism: The state is looking after you", *The Economist* (6 April 2006), online: *The Economist* <http://www.economist.com/opinion/displaystory.cfm?story_id=6772346>.

¹¹“The new paternalism: The avuncular state”, *supra* note 7; see also “Paternalism and Psychology”, *supra* note 8.

¹² Gary Marx defines traditional surveillance techniques as “the close observation, especially of a suspected person.” He further defines new surveillance as the “scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts” in George Ritzer, ed., *Encyclopedia of Social Theory* (London: Sage publications, forthcoming), s.v. “Surveillance and Society”; Marx gives the following examples of soft surveillance: “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’” in T. Monahan, (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*, 1st ed. [forthcoming in August 2006], online: Gary T. Marx <<http://web.mit.edu/gtmarx/www/softsurveillance.html>>.

¹³ Although this paper uses the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 [hereafter *PIPEDA*] as the model for Canadian privacy law, the reasoning is meant to apply to most legal privacy regimes based on fair information practice principles (FIPPs).

¹⁴ *PIPEDA*, *ibid.*

¹⁵ See, for example, Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 322.

¹⁶ 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 as Article 12 of the Universal Declaration of Human Rights, online: United Nations <<http://www.un.org/Overview/rights.html>>; Similarly, Article 17 of the 1966 International Covenant on Civil and Political Rights refers to privacy, online: United Nations <<http://www.hrweb.org/legal/cpr.html>>; Specific data protection regimes include: the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, online: <<http://conventions.coe.int/treaty/EN/cadreprincipal.htm>>; the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, online: OECD <http://www.oecd.org/document/18/0,2340,en_2649_37441_1815186_1_1_1_37441,00.html>; and “Directive 95/46 of the European Parliament”, (1995) No L. Official Journal of the European Communities of 23 November 31, online: <http://www.cdt.org/privacy/eudirective/EU_Directive_.html>.

¹⁷ “Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information- ‘Hey Buddy Can You Spare a DNA’”, *supra* note 12.

¹⁸ *Ibid.*

¹⁹ Ian Kerr and Valerie Steeves, “Virtual Playgrounds and BuddyBots: A Data-Minefield for Tinys and Tweenies” (2005) 4 *Canadian Journal of Law & Technology* 91, online: Ian Kerr <<http://iankerr.org/files/Kerr-Steeves-CJLT.pdf>>.

²⁰ Where surveillance is for purposes unrelated to increasing the welfare of those being monitored it cannot be understood as a form of paternalism, soft or otherwise. Of course, there are those who claim that aggressive state surveillance *is* a form of paternalism. 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 Bush, “Press Conference of the President”, (19 December 2005), online: The White House <<http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>>]

²¹ “Surveillance and Society”, *supra* note 12.

²² *Ibid.*

²³ *Ibid.*

²⁴ For example, in 2004 male residents in Truro, Mass. were asked non-threateningly by police to provide a mouth swab of their DNA 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's dragnet [*Ibid.*].

²⁵ See for example Ekos Research Associates *Privacy Revealed: The Canadian Privacy Survey* (1993) (Ottawa, Ontario) 10.

²⁶According 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 gain access to a Web site and an additional 10% are willing to provide this information if asked, cited in: S. Fox, L. Rainie, J. Horrigan, A. Lenhart, T. Spooner, & C. Carter, “Trust and privacy online: Why Americans want to rewrite the rules” (2000), online: The PEW Internet and American Life Project

<http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf>[hereafter 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.” [Interview with anchor Hank Plante of KPIX-TV, a San Francisco TV station, on September 21, 2001]

²⁷ PEW survey, *ibid*.

²⁸ “Surveillance and Society”, *supra* note 12.

²⁹ H.M. Shefrin & Richard Thaler, “An Economic Theory of Self-Control” (1981) NBER Working Paper No 208, online: NBER <<http://nber.org/papers/w0208>>.

³⁰ The term hyperbolic discounting refers to empirical research which finds that people will chose smaller over larger rewards when the smaller reward comes sooner in time. People will chose the larger over the small 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 or \$100 tomorrow, most people will choose \$100 tomorrow.” [Wikipedia, s.v. “hyperbolic discounting”, online: Wikipedia

<http://en.wikipedia.org/wiki/Hyperbolic_discounting>]; For further example see David Laibson, “Golden Eggs and Hyperbolic Discounting” (1997) 112 Q. J. Econ at 443, 445, & 446.

³¹ “Paternalism and Psychology”, *supra* note 8 at 136.

³² “Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information- ‘Hey Buddy Can You Spare a DNA’”, *supra* note 12.

³³ Jennifer Stoddart, “An overview of Canada’s new private sector privacy law:

The *Personal Information Protection and Electronic Documents Act*”, (1 April 2004), online: Office of the Privacy Commissioner of Canada, <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.

³⁴ For an elaboration of this claim, see Ian Kerr, “If Left to their Own Devices” in Michael Geist, ed., *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005); Ian Kerr, “Hacking at Privacy” in Michael Geist, ed., *Privacy Law Review* (Toronto: Butterworth’s, 2005).

³⁵ *PIPEDA*, *supra* note 13 at Sch. I, cl. .3.

³⁶ *Ibid* at Sch. I, cl. .3.2;

³⁷ “If Left to their Own Devices”, *supra* note 34; See, for example, *Bank adopts sweeping changes to its information collection practices*, (30 September 2002) *PIPED Act Case Summary #97*, online: Office of the Privacy Commissioner of Canada <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 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*, [2004] F.C.J. No.10 3, regarding Principle .3, where video surveillance was said to be appropriate by J. Lemieux. A factor in the decision was that the camera was minimally invasive, and was only looked at if there was a triggering incident. After 96 hours the video was deleted [*ibid* at para. 188).

³⁸ *PIPEDA*, *supra* note 13 at Sch. I, cl. .3.

³⁹ *Ibid*; “If Left to their Own Devices”, *supra* note 34.

⁴⁰ “An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.” [*PIPEDA*, *supra* note 13 at Sch. I s. 4.3.8]

⁴¹ *Ibid* at s. 7.

⁴² Daphne A. Dukelow & Betsy Nuse, *The Dictionary of Canadian Law*, 2nd ed. (Scarborough, Ont: Carswell, 1995) at 232.

⁴³ *Black’s Law Dictionary*, 5th ed., s.v. “consent” at 276.

⁴⁴ Gerald H. L. Fridman, *The Law of Contract in Canada*, 4th ed. (Scarborough, ON: Carswell, 1999) at 16-17; Stephen Waddams, *The Law of Contracts*, 4th ed. (Toronto: Edmond Montgomery

Publications, 1999) at 66-67.

⁴⁵ An executory contract is one which 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) at 108].

⁴⁶ “An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.” [PIPEDA, *supra* note 13 at Sch. I s.4.3.8]

⁴⁷ PIPEDA, *ibid.*

⁴⁸ A question arises as to whether this right is alienable; See, for example, James Rule & Lawrence Hunter “Towards Property Rights in Personal Data” in Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

⁴⁹ Subject to legal or contractual restrictions and reasonable notice.

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, *supra* note 13].

⁵¹ 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 to develop guidelines and implement procedures to govern the destruction of personal information [PIPEDA, *ibid.*].

⁵² *Ibid.*

⁵³ PIPEDA, *supra* note 13 at Principle 4.8

⁵⁴ *Ibid* at Principle 4.9 and s. 8.

⁵⁵ *Ibid* at Principle 4.10.

⁵⁶ *Ibid* at s.12.

⁵⁷ *Ibid* at s. 14.

⁵⁸ Bruce Phillips, “Foreword” in Stephanie Perrin, Heather H. Black, David H. Flaherty, & T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin, 2001) at ix.

⁵⁹ *Supra* note 13

⁶⁰ *Globe and Mail*, online: *Globe and Mail* <<http://www.theglobeandmail.com>> [hereafter *Globe*].

⁶¹ “Defaults, Framing, and Privacy: Why Opting in ≠ Opting Out”, *supra* note 7.

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

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

⁶⁴ U. Benzion, Y. Schachmurove, & J. Yagil, “Subjective discount functions: An experimental approach” (2004) 14(5) *Applied Financial Economics* 299.

⁶⁵ This assumes that Jij would want to read the articles at a latter date.

⁶⁶ See, for example, M. Ortendahl, & J. F. Fries, “Time-related issues with application to health gains and losses” (2002) 55 *Journal of Clinical Epidemiology* 843; R. H. Thaler, “Some empirical evidence on dynamic inconsistency” (1981), 8 *Economic Letters* 201.

⁶⁷ D. Kahneman & A. Tversky, “Prospect theory: An analysis of decision under risk” (1979) 47(2) *Econometrica* 263.

⁶⁸ Daniel Kahneman, Jack L. Knetsch, & Richard H. Thaler, “Experimental Tests of the Endowment Effect and the Coase Theorem” (1990) 98(6) *Journal of Political Economy* 1325.

⁶⁹ See 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).

⁷⁰ *Supra* note 26.

⁷¹ J. Cooper & R. H. Fazio, “A new look at dissonance” (2004) 17 *Advances in Experimental Social Psychology* 227.

⁷² E. Harmon-Jones, J. W. Brehm, J. Greenberg, L. Simon, & D. E. Nelson, “Evidence that the production of aversive consequences is not necessary to create cognitive dissonance” (1996) 70(1) *Journal of Personality and Social Psychology* 5.

⁷³ J. W. Brehm & A.R. Cohen, *Explorations in Cognitive Dissonance* (New York: Wiley, 1962); see also *A Theory of Cognitive Dissonance*, *supra* note 57.

⁷⁴ L. Simon, J. Greenberg, & J. Brehm, "Trivialization: The forgotten mode of dissonance reduction" (1995) 68 *Journal of Personality and Social Psychology* 247.

⁷⁵ D. Ehrlich, I. Guttman, P. Schonbach, & J. Mills, "Post decision exposure to relevant information" (1951) 54 *Journal of Abnormal and Social Psychology* 98.

⁷⁶ Jacquelyn Burkell & Valerie Steeves, "Privacy Policies on Kids' Favourite Web Sites", (Paper presented to the 6th Annual Privacy and Security Workshop, Privacy and Security: Disclosure, University of Toronto, 3 November 2005), online: On the Identity Trail <<http://idtrail.org/content/blogcategory/21/72/>>.

⁷⁷ A. Elliot & P. Devine, "On the motivational nature of cognitive dissonance as psychological discomfort" (1994) 67 *Journal of Personality and Social Psychology* 382.

⁷⁸ C. Camerer, "Prospect Theory in the Wild", in D. Kahneman & A. Tversky, eds., *Choices, Values and Frames* (Cambridge: Cambridge University Press, 2000) at 288-300.

⁷⁹ This is reflected in the endowment effect.

⁸⁰ A. Acquisti & J. Grossklags, "Privacy attitudes and privacy behavior" in J. Camp & S.R. Lewis, eds., *The Economics of Information Security: Advances in Information Security*, Vol. 12, (Massachusetts, Norwell, and Kluwer: Springer, 2004) at 176; For an article which explores the wisdom of government attempts to debias people's decision making via the law, see Christine Jolls & Cass R. Sunstein, "Debiasing through Law" (March 2005) Working Paper No. 225 U Chicago Law & Economics, online: Social Sciences Research Network <<http://ssrn.com/abstract=590929>>.

⁸¹ For an articulation of this thesis in the context of consent to the collection of personal information in digital rights management situations, see "If Left to their Own Devices", *supra* note 34 and "Hacking at Privacy", *supra* note 34.

⁸² The recognition of the need for *PIPEDA* sprung (at least in part) from concern about maintaining and facilitating Canada's international trading relationship. It was enacted under the federal trade and commerce power, and it focuses 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" (2002) 27 *Queen's L.J.* 609 at 623 for a discussion of these tensions; Michael Geist, for example, has criticized 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 [Michael Geist, "Canada's privacy wakeup call" online: Michael Geist <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", Report, online: CIPPIC <http://www.cippic.ca/en/action-items/pl_article_for_cplr_july_2005.pdf>.

⁸³ To be held early in 2006, five years after its introduction, as required by s.29. [*supra* note 13]

⁸⁴ "An overview of Canada's new private sector privacy law: The *Personal Information Protection and Electronic Documents Act*", *supra* note 33.