

ORAL TESTIMONY
STANDING COMMITTEE (PIPEDA REVIEW)
ian kerr

Mr. Chair, honorable members. Let me commence by expressing my gratitude for the invitation and the opportunity to appear before you today on a set of issues I care very deeply about. Like others who have appeared before you, I am concerned that there are a number of significant problems with the current legislation that require reform. I have provided written submissions to that effect and hope to illustrate a key problem in my brief time before you today.

I am a Professor at the University of Ottawa where I hold a three way appointment in the Faculty of Law, the Faculty of Medicine and the Department of Philosophy. In July 2001, I was appointed the *Canada Research Chair in Ethics, Law & Technology*, funded by the Government of Canada, to conduct research on a myriad of issues including many of those that all of you have been co-investigating these past few months.

In 2004, the Social Science and Humanities Research Council of Canada awarded me 3 million dollars to direct a 4 year interdisciplinary project with more than 50 researchers from across North America called *On the Identity Trail*. This project focuses on questions relating to the impact of information and authentication technologies on privacy, identity formation, and on our ability to be anonymous.

We live in an information age. The information trade, its services, and its technologies of irresistible convenience demand *quid pro quo*: In order to *get* information products, you must *give up* some personal information. Computers and other information technologies pose new threats to privacy. Former Privacy Commissioner of Canada, Bruce Phillips, described PIPEDA as a response to these threats:

This statute ... 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.

It perhaps goes without saying that computers, databases, networks, surveillance cameras, cookies, spyware, radio frequency identification and other automated means of collecting, using and disclosing personal information directly threaten our ability to control personal information. You have heard about this from many of your previous witnesses. I have significant expertise on these issues and am happy to provide you with more information on any of these, if you wish to ask me about them during your question period.

My testimony today, however, will be to suggest that the much bigger threat to privacy comes from a much more primitive and basic technology. It is a technology that all of you are familiar with, even those of you, like the honourable chair, who avoid computers, PDAs and the internet like the plague.

The threat that I am referring to is, in fact, a legal threat. En français il s'appelle le *contrat d'adhésion*. In English, we call it the *standard form contract*. While

computers, surveillance cameras and rfid chips *technologically enable* aggressive, voluminous and sometimes surreptitious collection, use and disclosure of personal information, it is standard form contracts that *legally enable* the so-called 'implied consent', 'deemed consent' and 'opt-out' consent-gathering processes said to justify the use of the surveillance technologies under our current privacy law. These means of using the law to DEEM CONSENT when in fact there is NONE are highly problematic.

Standard form contracts are mass-produced documents that prevent and preclude negotiation and agreement. They are drafted exclusively by parties in an economic position to offer certain terms on a *take-it-or-leave-it* basis. In an information age, where the business handshake has been replaced by mouseclicks, where bilateral negotiation is supplanted by global, one-to-many transactions, the standard form contract is regularly invoked by organizations to circumvent various privacy protections prescribed in PIPEDA and other data protection regimes.

Whether in the sale of goods or the licencing of services, many organizations use standard forms, clickwraps and end-user license agreements as a way to justify unreasonable and overarching so-called 'consents' to excessive collection, use and disclosure of personal information. Through their one-sided contracts, organizations are able to extend their personal information practices well beyond the bounds of what might otherwise be permitted by Canadian privacy law. They do this by compelling consumers, customers and citizens to "contract-out" of the protections that PIPEDA would otherwise provide.

In my written submissions, I offer you a series of detailed recommendations on how to amend PIPEDA to fix the enormous problems for obtaining genuine-consent that are generated by the contractual model. I am happy to answer any questions that you might have about those detailed recommendation. But let me first provide you with a two crunchy examples that hit close to home.

EXAMPLE #1

As a Member of Parliament, your job, like mine, requires you from time to time to stay at one of Canada's nearly 400,000 hotel rooms. Maybe you need to send some documents or check your email while you are there? To use a hotel's internet services, you will be required to agree to its terms of service. On a work related trip, I once stayed at a Hilton Hotel. While there, I needed to use the internet. Here is what I would have once been said to have 'consented to' when I plugged my computer into the Hilton's internet connection:

"We may automatically track, collect and compile User Information and Transaction Data ... when you utilize the Service.

You agree that HHC shall own all Information.

By using the Service, you voluntarily, expressly and knowingly acknowledge and agree with all of the foregoing and further agree to each and all of the following: (I) such Information belongs to HHC and is not personal or private proprietary information; (ii) such Information, wherever collected, may be processed, used, reproduced, modified, adapted, translated, used to create derivative works, shared, published and distributed by HHC in its sole and absolute discretion in

any media and manner irrevocably in perpetuity in any location throughout the universe without royalty or payment of any kind, without, however, any obligation by HHC to do so.”

So instead of me, lets imagine that the Honorable Member Mr. Tilson had stayed at the Hilton and sent email to Mr. Wallace, emails that contained some communication about these Committee deliberations. Or maybe they were about other personal stuff. Under the terms of service I referred to above, Hilton would have claimed that the personal information and private communications generated by these two honourable members is IN FACT NOT PERSONAL OR PRIVATE, that by way of their consent, it is therefore not subject to PIPEDA, and that in fact Hilton owned it, in perpetuity, ANYWHERE IN THE UNIVERSE (As David Bowie's *Major Tom* once sang, "Planet Earth is Blue and there's nothing I can do").

According to Canadian contract law, I suspect Hilton would likely have prevailed. Regardless, most individuals would be forced into submission during a lengthy and protracted litigation process in the courts about what is an unclear point of law. I recommend that we clarify the law on this.

EXAMPLE #2

Like me, everyone around this table consumes many intellectual products every day. You read the newspaper, specialty magazines or books, or maybe you watch tv, movies, or listen to music or talk radio. If you are like me, sometimes you don't care who knows what you are reading about or listening to, and sometimes you do.

But I'll bet that YOU WOULD CARE ALOT if you learned that someone was ALWAYS ABLE TO KNOW ABOUT EVERY SINGLE intellectual product that you consume: how often, where, when, etc. Everyone around this table, I suspect, cares about intellectual privacy: the ability to consume intellectual products free from public scrutiny and corporate or governmental surveillance.

So imagine that you go out and buy a CD or DVD (or maybe you borrow it from the library). You throw it into a device that you own to play it. You watch or listen.

All the while, and unbeknownst to you, a small software routine written into the code of that CD or DVD causes an automated communication via your wireless internet connection. The CD/DVD reports back to Sony (or whoever): who you are, where you are, what machine you use, which software you run, what you are watching or listening too, when you watched or listened, how often, etc.

By now in the course of these proceedings, these realities of the digital age are no longer surprising. But here is something that might surprise you. You decide to investigate whether Sony's practice infringes your privacy rights under Canadian law. You come to learn that it probably does not!! OR, at best, that the law is unclear about this.

In fact, you come to learn, you have probably legally 'consented' to letting the CD phone-home and rat-you-out to the mothership. In its more than 3000 word standard form contract (which is 700 words more than it took Edgar Allen Poe to tell the tale of "the thousand injuries of Fortunado"), 52 of those words provide your so-called 'consent' to the automatic installation of a "rootkit" -- what Sony called "a small proprietary software program." Because of this provision, the organization

collecting your personal information will claim that you have contracted-out of the protections otherwise afforded to you under PIPEDA. And, according to their agreement, you also supposedly 'consented' to allow them and their information-sharing partners to give that information to any member of the government who makes a request -- without a court order or any form of due process. And there is nothing you can do about it. In fact, according to the contract that you consented to the moment you put that CD/DVD into your player, the company owns that information.

The main point I want to impress upon this Committee today is that this form of legal maneuvering – something that each and every one of us around this table is subject to multiple times each and every day – is hugely problematic and not sufficiently addressed in PIPEDA.

Standard form contracts and other similar so-called 'consent gathering processes' can undermine the nature and value of genuine consent and fly in the face of what our privacy laws are actually trying to achieve.

I would submit that PIPEDA's attempt to balance individual privacy rights with the need of organizations to collect personal information is undermined if, irrespective of PIPEDA's many protective provisions, intrusive, unfair or unwanted collection, use or disclosure can be imposed on individuals with impunity through standard form contracts or other similar so-called 'consent-gathering processes' such as those formerly used by Sony, or the clause formerly used by Hilton, or other hotels, instant messaging services, mobile phone providers, other online service providers, health care providers, etc, etc.

I can assure you, this same strategy is used often and with great success in other sectors as well, all of which tells us that WE NEED A MUCH TIGHTER SET OF CONSENT PROVISIONS THAN THOSE CURRENTLY FOUND IN PIPEDA.

In my written submission, I offer concrete recommendations to fix this.

If I have one more minute, let me also add that I support some of the recommendations by other witnesses, in particular:

- the law should be amended to provide the federal privacy commissioner with order-making power
- the law should remove any lingering doubt about the power of the federal privacy commissioner to regularly name names in 'well-founded' findings
- the law should include a mandatory security breach disclosure requirement
- Ottawa must begin to address the growing concern in Canada over the outsourcing of personal information to non-Canadian organizations, particularly data flows to the United States

Although there is no time to address these points now, I am happy to respond to any questions that you might have.