The Personal Information Protection and Electronic Documents Act

Christine ELLIOTT*

* Sollicitor, Vancouver (BC).

If you learn only one thing out of the following it is this: under the common law, you, as an individual do not "own" your personal information.

By "own" I mean the ability to control when and why your personal information is collected, whom it is given to, and lastly the ability to correct when it is in error.

The purpose of the federal *Personal Information and Electronic Documents Act*,[1] is to level the playing field between individuals and federally governed non-governmental bodies, such as banks, by giving individuals a say in who collects what information for what purpose.

I. WHY DEFEND PRIVACY?

In other words, how to counter the following arguments:

- If you have nothing to hide, why do you not want to disclose your personal information?
- The only reason for collecting the information is to know you better and tailor merchandising to your personal individual needs.
- Capitalism supports this lowering of cost of provision of products.
- I find the arguments in favour of preserving privacy of information more compelling:

> "The common law secures to each individual the right of determining ordinarily to what extent his thoughts, sentiments, and communications shall be communicated to others. The right to be let alone, the most

---

[1] S.C. 2000, c. 5 [hereinafter, Act].

> comprehensive of rights and the right most valued by civilized men."[2]
>
> "A man has a right to pass through this world, if he wills, without having his picture published, his business enterprises commented upon, whether in handbills, circulars, catalogues, newspapers or periodicals."[3]
>
> "Privacy is related entirely to the degree to which we respect each other as unique individuals, each with our own sets of values, which we are entitled to make known or not as we see fit … Respecting one another's privacy means the difference between a life of liberty, autonomy and dignity, and a hollow and intimidating existence under a cloud of constant oppressive surveillance."[4]

– At some point, what amounts to consumer service turns into consumer stalking.

I had always assumed that capitalism would protect privacy—on the theory that privacy was valuable to individuals. Regrettably, privacy is more valuable to those collecting aggregate information for sale than it is for individuals.

The first inkling that I might be wrong came when I saw the film *The Insider*. In the film, on the weekly news show "60 Minutes", Dr Wygand "blew the whistle" on the top seven tobacco companies, who had been saying that nicotine was not carcinogenic. At the time, the sale of CBS to one of the top seven tobacco companies was proceeding and there was pressure from the *éminence grise* to stop Dr Wygand's story being broadcast.

So, instead now, I would say capitalism is diametrically opposed to privacy. As the federal Privacy Commissioner has pointed out, at the heart of our apprehension is the loss of control: who has the information, how do they use it to influence events and decisions which affect our lives. With a universal identity card, it would amount to an "internal passport."

---

2 U.S. Supreme Court Associate Justice Louis Brandeis (1928).

3 New York State Court of Appeals Chief Justice Alton B. Parker (1901).

4 Bruce Phillips, Privacy Commissioner of Canada.

II. WHAT WAS THE SITUATION IMMEDIATELY PRIOR TO PROCLAMATION OF THE ACT

One hundred years ago, before the advent of computerization and the resulting ability to collect much personal information at low cost, there was little to protect privacy and little privacy to be protected. This has resulted in very little common law development on rights to privacy.

1. Federal *Privacy Act*:[5] to permit individuals to ask federal government institutions to provide to the individual his/her personal information. The Privacy Commissioner has a budget of $60,000,000 a year to carry out his mandate.
2. BC *Freedom of Information and Protection of Privacy Act*:[6] to permit individuals to ask provincial governments institutions to provide to the individual his/her personal information.
3. The BC *Privacy Act*:[7] makes it a tort to breach a person's privacy. The classic situation is where the man with the video has the toupé blown off and that clip is then used in the TV evening news. The difficulty with making breach of privacy a tort is that it is virtually impossible to prove damages. Thus there have been few cases under this Act.
4. Under the common law, individuals do not own their personal information. It is virtually impossible to obtain your personal information from a firm, such as Dun & Bradstreet, even where you consent to the search of your information being done by a bank which proposes to lend money to you. Under the terms of its search request, a bank agrees not to disclose the search request to the consumer searched.

---

5 R.S.C. 1985, c. P-21.

6 R.S.B.C. 1996, c. 165.

7 R.S.B.C. 1996, c. 373.

5. And of even more importance is the sale of your private information between data banks. For example, Canada Post selling addresses to Dun & Bradstreet. I cannot tell what is sold and to whom and for what purpose because while I think it is *my* private information, I cannot track it to see where it is and how it is used.

III. WHAT INFORMATION CAN AN INDIVIDUAL FIND ABOUT HIM/HERSELF?

1. *BC Personal Property registry*—for security granted by me on non-land security, such as a car—I have not granted any.
2. *BC Land Title Office*—though land ownership or ownership of registered charges—I own no land or any interest in land.
3. *Quicklaw*—search of all Canadian cases for my name—very useful on occasion when a client asks "what do you know about x"—I can at least see if x has appeared as party to or witness (or indeed, judge) in any Canadian case. I do not appear.
4. *White/Yellow pages*—for telephone listing, I am listed.
5. www.mybc.com and other "search for" person listings.
6. *Search Web*—for Chris Elliott, I got two hits, one for "Chris Elliott sucks.com" and "Get a life Chris Elliott.com"—I think aimed at a U.S. professional football player. This search would not get my Web page at www.cehql.com (which means I must embed meta tags in my title page to be found).
7. Once you find appropriate Web page—view source and find who the "registered owner" of the Web name is—I know of no way so far of searching for all Web sites owned by a particular "registered owner."
8. Request for information under BC *Freedom of Information and Protection of Privacy Act*[8] for information held by BC government bodies.

---

[8] *Supra* note 6.

9. Request for information under Canada *Privacy Act*[9] for info held by federal government bodies, such as Revenue Canada.

10. Request info from provincial credit reporting agencies under BC *Credit Reporting Act*,[10] *e.g.* so you can review and respond to the information there. One of my former law firm partners requested a Gold Visa. His application was refused. He was miffed—since he had always thought of himself as a commercially responsible person. It turned out that a n'er do well, by the same name as Mr X., had defrauded a BC credit union (equivalent to a bank) for $130,000. It was straightened out—with time.

11. *Quick law* search for all instances of a name and learn the court attendance history (good for proof of character), but also the intimate financial details of any family divorce and division of family assets.

12. *Follow person* and see if the drapes are drawn on house and garage empty—it follows that resident is away. Number of cars might indicate number of individuals in the house.

13. www.spaceimaging.com—High resolution images from satellite in space for US $30 to US $300,000—for $10 you can download a picture of Saddam Hussein's palace! For example, you can tell whether your competitor behind the high walls is wiping the competition or on its last legs. USA used this for years to tell if the Russian grain harvest was going to be good or bad—and move accordingly in the market place. The information would be most useful if you are a swimming pool service provider. It would enable you to target your potential customers with exactness.

14. Ducks Unlimited Canada (and Ducks Unlimited in the USA) track waterfowl, such as ducks. They are able to insert under the duck's back skin a small battery driven transponder which beeps to a satellite once every few days and thus DU can see what the migration looks like. So can

---

9 *Supra* note 5.

10 R.S.B.C. 1996, c. 81.

you, by picking say Duck #12234 follow the duck's migration north and then south again.

15. And what can be done to a duck can be done to a person—perhaps not under the skin, but in a wallet or coat, car etc. And those in Cadillac cars with a GPS on board can call the manufacturer and ask exactly where they are and how to get to the destination. In short, you can pay for the privilege of being monitored.

16. Britain has a system of identifying people by the way they walk. This was a surprise to me, I am so short-sighted that I had always assumed that everyone identified a person walking towards them by their gait.

17. http://www.idcide.com—allows you to keep track of who is tracking you.

IV. WHAT INFORMATION CAN THE GOVERNMENT FIND OUT ABOUT YOU?

1. *Social insurance number*—the universal locator. The Federal Privacy Commissioner found that Human Resources Canada was using the SIN number to connect data drawn from several programs:

- T1 Income Tax Returns;
- child care benefits;
- immigration and visitor's files;
- National Training Program;
- Canadian Job Strategy;
- national employment services;
- record of employment;
- Social Insurance Master File;
- all gleaned by information sharing agreements with over 300 organizations with other databases;
- up to 2000 bits of information including education, marital/family status, language, citizen or immigration status, ethnic origin, mobility, disabilities, income tax data, employment insurance, religion:

- Who knows who it is given to;
- there is never any purge;
- there is no legal protective framework.

2. *Video Cameras*—In Monaco there are video cameras everywhere—and I do mean everywhere. I know of a visitor to Monaco who set up her easel to paint only to have a policeman arrive and tell her that she needed a permit to paint. They went to the station, and armed with her permit, she chose another location to paint from. An hour later the same policeman came up to her to return her wallet which she had forgotten at the police station—how was he able to find her? Monaco is small and everything is on video camera. In Vancouver now, you will find video cameras on all major intersections.

3. *Police*: motor vehicle ownership, prior criminal record, o/s warrants, convictions, age, sex, height, eyes, where you live, and propensity to violence.

4. *Review of hard drive in forensic accounting*— Because, as Oliver North found out, "delete" does not mean "destroy."

V. WHAT INFORMATION CAN CAPITALIST THIRD PARTIES FIND OUT ABOUT YOU?

- www.amazon.com—name, address, telephone number, e-mail address, and thereby your IP address—*e.g.* down to your computer, credit card number, installation of "cookies" to show your preferences when you next visit. This is an aggregation of information from previous visits. Some think that Amazon prices may depend on how may times you have visited—*i.e.* a higher price, once you have bought into the concept! As well, companies like Amazon may purchase other data and use it to flesh out the information collected by Amazon directly—and vice versa. The joke in the Privacy Commisioner's 2000 report was that a site promises that it will never divulge the information collected from an individual, unless they have a sound financial reason to do so.
- *Mastercard*—your spending habits—Mastercard will call when they see a claim in size or place outside your normal habits (*e.g.* my trip to Equador was made through Cornell).

- *Telus*—can tell where I call, who calls me, how long etc.
- *Bank*—flow of funds through account and who they are paid to. I have always objected to Air Miles—for a very few points, you give them all information on what you bought in the Safeway, how much gas you bought and from whom, and the times at which you did all the foregoing.
- *Where you go on the net*, on which pages do you stop and leave the site.
- What times do you surf and for how long—the lunch wave moves across Canada!
- Retailers knowing what you like put your profile against others and say "people who bought this book that you just bought, also bought this different book."
- All your senses may be recorded except for *smell and taste*—and no doubt that will come too.
- You went on *holiday* to Hawaii last Easter, so send travel info to that customer this December.
- Interestingly, banks use *Interac* as a trusted third party to process your request for cash while at the same time not allowing the bank which is servicing that machine to datamine and target you as a customer.
- *Landlord*—I live in a building with high security—key fobs will only let you into certain parts of the building, *e.g.* parking, ground floor and your floor. The price for that is that the landlord can print out exactly when I went in or went out, and how often.
- *List owners—e.g.* Costco—knows your spending habits and address—can organize lists which can be sold. Canada Post is in the business of targeting marketing—selling information from list suppliers, *e.g.* Dun & Bradstreet, grocery card purchases, insurance companies, movie theatres, hotels, car rental companies.
- *Insurers—Vancouver Sun*, July 6, 2000: Royal Sun Alliance, one of Canada's biggest insurance companies said that they would use genetic information when assessing a client risk. What if insurers demand genetic tests? *Federal Privacy Act* protects a right to privacy

including genetic testing. At this point, genetic testing may not be sufficiently predictive to be of much use, but I think it predictive and therefore of use in the future.

– *Vancouver Sun*, May 30, 2000: the federal government said that it would dismantle its personal information data base, which had up to 2,000 items about some individuals. Employment, tax, education, citizenship, language, government benefits, welfare, marital status, education, mobility, disabilities, the use of SIN number, religion, ethnic origin, all on 33.7 million live and dead Canadians since 1995. When the Privacy Commissioner disclosed this to the press, Human Resources Development Canada was swamped by 18,000 requests for a copy of their personal file—and the department was in a quandary on how to do this, *i.e.* they needed some mechanism to confirm the identity of the applicant! Now, apparently, the linkage between government departments is with removal of personal information?

– *BC OnLine* gives any searcher the ability to find out if you own real property, or personal property on which there is a registered security interest.

VI. WHAT IS WRONG WITH DATA COLLECTION?

1. *Marginalization*: I have a friend who has kidney failure and who is a partner in a Vancouver law firm where his billings are more than others of his partnership. He would not qualify for employment with any organization that looked at genetic profiling, because it would view him as a high risk employee. But statistics are simply that, statistics, they do not determine how a particular person would fare.

2. *Iron curtain mentality*: to feel that you are always being watched will lead to some type of iron curtain style conformity, which in turn will lead to more surveillance. The concern in the past has been "Big Brother"—government surveillance, and now the concern is not only big brother but also "big browser" working together.

3. *Living by the worst case scenario*: "To live by the worst case scenario is to give the terrorist their victory without a shot being fired. It is also alarming to think that the real battles of the new century may be fought in secret, between

adversaries accountable to few of us, the one claiming top act on our behalf and the other hoping to scare us into submission."

4. *Information collected for one purpose may be used for some completely different purpose*: Canadians have an extraordinary willingness to give up their personal privacy in return for small tangible benefits—*e.g.* they agree to having their food buying monitored (Safeway Card, Save on Foods credit card). Another example: the *New York Times* says that it does not sell its lists, but I have had e-mail from another organization that knew I was a subscriber to the *NYT*. This information can be merged with other data bases to collect a more complete picture of a consumer. This is where consumer service may likely slide into consumer stalking.

5. This is the age of the "sound bite" in which information can be collected out of context or incompletely and fed onto the Internet where it is extremely difficult to respond to the incorrect information because the sound bite is not long enough to bring context to the first sound bit. Example, Shakespeare's Henry VI "first kill all the lawyers"—taken out of the context in which the full thought was: "If you want to create anarchy, then first kill all the lawyers."

VII. BILL C-6 NOW PROCLAIMED AND IN FORCE AS FOLLOWS …

Most privacy legislation deals with "fair information collection" practices, then the right to use it and who has access, and thirdly the right to correct information. Bill C-6[11] is really about being "pro choice" in giving up personal information.

An individual's privacy is protected by statute as against the BC government and as against the Federal government. The crucial thing about C-6 is that it covers privacy in the *federal private sector*.

---

[11] *Supra* note 1.

Consent to collection of private information must be "informed"—*i.e.* organizations must say what information they are collecting and what use will be made of it. If the organization wishes to later use it for some other purpose then again consent must be obtained.

C-6 applies to both new and existing information. All businesses must review their records and destroy information which is beyond that which is necessary for current purposes—or argue tacit consent or render information anonymous.

VIII. THE ACT APPLIES TO …

Collection, use and disclosure of "personal information"—which is defined[12] to mean "information about an identifiable individual."

C-6 applies[13] to personal information that the organization collects, uses or discloses in the course of commercial activities. It does not apply[14] to information that an individual collects, uses or discloses exclusively for personal or domestic purposes. The Act:

- arguably does not apply to millions of private Web sites;
- does not apply to personal information collected, used or disclosed exclusively for journalistic, artistic or literary purposes;[15]
- currently does not apply to a business which is not federally regulated, unless the personal information crosses provincial boundaries;[16]
- after three years, the Act will apply to all businesses—query as to whether this is constitutionally possible—though the cross border nature of most information may make provincially formed companies subject to C-6;
- as well, most provinces are filling the blank by draft provincial legislation covering provincially regulated businesses.

---

12 S. 2(1).

13 S. 4(1)(a).

14 S. 4(2)(b).

15 S. 4(2)(c).

16 S. 30(1).

While it is too soon to tell, I think there may be court traffic in the following areas:

- What constitutes "private information." Even if I use a computer in a public library, someone will know the IP address of the computer and therefore the geographical area where I am located.
- Subtle collection of information: *e.g.* Yahoo asks you for your birth date if you lose your password—and then uses that information to e-mail users ideas for birthday gifts—*i.e.* how far can you stretch the need to collect private information.
- What information is *private—e.g.* "private information" might include items drawn from different publicly available resources to create something which is itself private.

CONCLUSION

You do not own your private information. There is a vast amount of publicly available information. And even more information which collates information from a number of sources and is then available for sale. The Act will at least permit an individual to find out what information an organization has and for what purposes. In short, all legislation on privacy has been required because technology has left the common law far behind and a catch-up is highly desirable.