
David Fraser
McInnes Cooper, Halifax
"People get upset about privacy stuff when they're surprised, so the key is to not surprise people."

Michael Geist
University of Ottawa

"Surely, I, as the user, ought to be allowed to be as granular in my choices with respect to privacy as anything else."

MIKE PINDER

PRIVACY FOR SALE

The real cost of social networking.

With sites like Facebook and Twitter shrinking the globe down to a roomful of 'friends' and 'followers,' every movement in our personal lives can be discreetly monetized. Demographic data is the bread and butter of a social network's business model and primary revenue stream. But at what cost to our privacy? And can this country's decade-old privacy law stand up?

By Jason Scott Alexander

It's hardly a good sign for the world's largest social networking site when typing "How do I..." into Google ranks "delete my Facebook account" at the top of the search results.

Earlier this year, a mass exodus nearly erupted when a relatively small but determined faction of Facebook's 500 million users became so outraged with privacy concerns on the service that they took it viral and encouraged others to boycott or leave the site. Many high-profile bloggers, tech-celebrities and media types led the charge, culminating with a "Quit Facebook Day" on May 31.

Ultimately, it's hard to measure the campaign's success, but it marks the first large-scale social response to a very long run of privacy controversies that have plagued Facebook over its six-year existence.

In 2008, a class action lawsuit against Facebook claimed privacy violation over the company's Beacon program that published information about users' purchases — such as movie rentals, which is contrary to law — to the users' Facebook Wall and to their friends' feeds. Facebook eventually terminated Beacon in 2009, and a settlement was approved by a U.S. federal court in March of this year for $9.5-million (U.S.)

That very same year the Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the Faculty of Law, University of Ottawa, launched Canada's first official volley against Facebook Inc., filing a much broader set of complaints

MARVIN MOORE

Jennifer Stoddart
Privacy Commisssioner of Canada, Ottawa

"This is spawning a digital arms race in terms of the collection of personal information. […] We're seeing too many cases where the innovators innovate and the lawyers mop up after the fact."

to the Office of the Privacy Commissioner (OPC). An investigation resulted in a report issued in July 2009; Facebook was given one year to clean up its act or file a defence.

Facebook entered negotiations with the Canadian government over changes to its privacy policies and, for a while, things were looking up. But on April 19 of this year, the site once again faced a wave of criticism after launching its highly controversial "Instant Personalization" program, which allowed it to automatically share users' personal information, without their consent, with third-party websites. The purpose was to personalize users' experience on other websites, relying on data about their tastes, interests, hobbies, political affiliations, religious views, socio-economic status and mountains of other personal information shared on Facebook.

Then in May, Facebook updated its privacy policy offering users a one-stop shop for selecting privacy settings and restricting access to users' personal information by third party application developers. These developers now must be more transparent about the information they collect from users. In September, Privacy Commissioner Jennifer Stoddart declared herself "pleased" with Facebook's efforts, but concurrently announced fresh investigations into complaints about new Facebook features, namely the increasing usage of the "Like" button on other websites.

Fear and expectations

David Fraser, a partner at McInnes Cooper in Halifax, and chair of the CBA's National Privacy and Access Law Section, sees privacy online as a big-picture issue which cuts across law into sociology and culture. It also underlines, in his view, a significant shift in how privacy is understood.

"When the Internet first became commercial and popular, there was a widespread fear," Fraser recalls. "There was this belief, and probably in the end incorrect, that on the net were a whole bunch of thieves, fraudsters and brigands just waiting to prey on anybody who put their information out there. Obviously something has changed dramatically in the last 10 or 15 years. It's hard to put your finger on it exactly — whether Facebook is the cause, or an accelerator."

In fact, users knowingly share more privacy today than they probably care to admit — something called the privacy paradox. People always express concern about their personal information, says Fraser, but they'll easily trade privacy for a perceived benefit. "If you give them a candy bar, they'll give you their SIN number."

Complicating the debate is the subjective nature of privacy. Thresholds vary dramatically from person to person. Most people expect information to be collected, but many also have an expectation about who will have access to it and how it will be used.

In a sense, that's the bargain struck between the user and a company like Facebook, says Michael Geist, law professor at the University of Ottawa where he holds the Canada Research Chair in Internet and E-commerce Law. Backlashes occur, he adds, "when Facebook overreaches and they adjust their policies in a way that is, quite simply, inconsistent with the expectations that their users have about the way in which their privacy will be protected." The mistake has been to make "certain choices mandatory, effectively, where they haven't given people the opt-out. Surely, I, as the user, ought to be allowed to be as granular in my choices with respect to privacy as anything else."

That argument is the basis of a Canadian class action lawsuit filed by the Merchant Law Group. The suit claims that Facebook's rollout of Instant Personalization was a bait-and-switch process: In order to provide users the luxury of demographic sales targeting, Facebook opened the doors on users' personal information to the world, by default.

"It was a retreat from their privacy policy," explains Evatt Merchant, from MLG's Saskatoon office. "It's not sufficient for Facebook to simply send out a notice to people saying in the coming weeks we're changing everything and, to figure out how to address all that, you just have to jump through a couple dozen screens and change your settings. As it stands, even a savvy computer user would have had difficulty going

À vendre : vie privée

Avec des sites comme Facebook et Twitter, chaque renseignement personnel peut être monétisé. Mais l'opposition s'organise.

Ça ne peut être un bon signe pour le plus grand site de réseautage au monde lorsque l'une des recherches les plus fréquentes dans Google est : « Comment effacer mon compte Facebook ».

Plus tôt cette année, un exode d'usagers a culminé dans la « Journée pour quitter Facebook », après que des blogueurs influents et des célébrités du monde de la technologie ont lancé une campagne, préoccupés par des questions de droit à la vie privée sur le site.

L'année précédente, des étudiants de l'Université d'Ottawa ont déposé une série de plaintes auprès du Commissariat de la protection de la vie privée du Canada. Dans un rapport publié en juillet 2009, la commissaire a donné un an à Facebook pour remédier à une série de problèmes.

En septembre, la commissaire Jennifer Stoddart s'est déclarée satisfaites des modifications apportées par Facebook qui a mis en place des mesures afin de limiter la communication de renseignements personnels aux tiers développeurs d'applications. Toutefois, la commissaire a annoncé l'ouverture d'une nouvelle enquête concernant des nouvelles fonctions, entre autre les boutons « J'aime » qui figurent sur d'autres sites.

David Fraser, un associé chez McInnes Cooper, à Halifax, et le président de la section nationale du droit de la vie privée et de l'accès à l'information de l'ABC, estime que la dimension « vie privée » sur internet traverse des changements importants.

Les utilisateurs d'internet partagent de plus en plus d'informations personnelles, note l'avocat. La situation est paradoxale, puisqu'en même temps, ces utilisateurs se disent préoccupés par la protection de leur vie privée.

Mais « si vous leur donnez une barre de chocolat, ils vont vous donner leur numéro d'assurance sociale », croit Me Fraser.

Équilibre fragile

C'est le difficile équilibre avec lequel doivent composer des compagnies comme Facebook, résume Michael Geist, professeur de droit à l'Université d'Ottawa et titulaire de la chaire de recherche du Canada sur internet et le droit du commerce en ligne. Des réactions surviennent, selon lui, « lorsque Facebook va trop loin et établit des politiques qui ne sont pas conformes aux attentes de leurs utilisateurs quant à la manière dont leur vie privée sera protégée ».

C'est entre autres ce qui a permis au Merchant Law Group de lancer un recours collectif au motif que l'un des programmes de l'entreprise, Instant Personalization, était trop intrusif et ne donnait pas assez de liberté aux utilisateurs de s'en retirer.

« Même les utilisateurs les plus expérimentés avaient de la difficulté à faire tout ce qu'ils devaient pour protéger leurs informations personnelles », explique Evatt Merchant, du bureau de Saskatoon de la firme.

D'autres sites que Facebook ont eux aussi leurs démêlées avec la justice et les organes chargés de la protéger. C'est le cas de Twitter, qui en juin a réglé hors cour une cause avec la *Federal Trade Commission* des États-Unis. On l'accusait de ne pas avoir pris les précautions nécessaires pour empêcher des hackers de pénétrer dans 55 comptes en quatre mois, dont celui du président américain Barack Obama.

La commissaire canadienne à la protection de la vie privée, Jennifer Stoddart, est consciente de tous ces problèmes. L'an dernier, son commissariat a vu une augmentation importante due nombre de plaintes liées aux nouvelles technologies. « Nous avons récemment ajouté à notre équipe d'enquête du personnel qui a une expertise de ces questions », dit-elle.

La commissaire Stoddart soupçonne que ces violations ont beaucoup à voir avec la raison d'être de ces organisations : faire de l'argent dans l'univers digital.

Vers l'avenir

Pour s'assurer que le Canada est équipé de règles appropriées pour faire face aux défis de l'heure, le Commissariat à la protection de la vie privée a confié à deux professeurs le mandat d'étudier une série de questions liées à la loi canadienne sur la vie privée, leurs impacts et les pouvoirs du commissariat.

Dans leur rapport rendu public en juillet dernier, les auteurs ont conclu que dans l'ensemble, le régime de protection de la vie privée avait été plus efficace quant aux activités des grandes entreprises que des petites firmes.

L'un des moyens de protéger les Canadiens serait de renforcer les pouvoirs du commissariat et de lui permettre d'imposer des amendes ou d'autres sanctions. Mais cette option ne fait pas l'unanimité. « La commissaire est une voix qui fait la promotion de la vie privée, et vous ne voulez pas que le juge et le policier soit la même personne. Ça me semble être un conflit d'intérêts », estime Me Fraser.

La force du droit canadien de la vie privée est qu'il demeure ouvert à l'interprétation, renchérit Ariane Siegel, une associée chez Aird et Berlis, à Toronto. « Tandis que nous évoluons et que les modèles d'affaires se développent et que de nouvelles technologies font leur apparition et même, au fur et à mesure que nos normes changent, la loi canadienne peut évoluer elle aussi. »

Me Siegel prévoit un avenir excitant dans ce domaine du droit, entre ce qu'elle voit comme des contributions incroyables du Canada dans les domaines des technologies et des communications, des régulateurs et des penseurs respectés et écoutés, et une culture entrepreneuriale à succès. « Les Canadiens sont dans une bonne position pour faire preuve de leadership dans ce secteur, tant au plan commercial qu'au plan de l'élaboration de politiques. » **N**

through all the steps needed to try and re-secure their information after the policy changes of Facebook."

In the end, Facebook is guilty of bad communication with its users, often changing rules without explanation.

"They've been rolling out new features, regularly, and not informing people about what it is that they're going to expect from the new Facebook experience," says Fraser. "People get upset about privacy stuff when they're surprised, so the key is to not surprise people."

Many observers also recommend social networking sites adopt a strict opt-in policy for privacy settings, thereby guaranteeing absolutely no disclosure of information without users' consent.

"It is absolutely crucial to realize that the devil's in the default," warns Geist. "The default choices that are made by these organizations are going to effectively be the choice for many of their users, and so they've got to in some ways choose wisely."

The question on many people's minds is how Facebook, with all-star legal and public policy experts, could misstep so often, especially while under the microscope of so many regulatory agencies.

"That's one of the things that we hope to discover over the course of the litigation," says Merchant.

Ultimately, he hopes to ensure that Facebook commits to protecting and maintaining privacy, in an ongoing manner.

The firm also believes that social networks, in general, should be forced to have a statement of privacy that is brief, succinct and tangible to the common user. "Something right up front," Merchant insists. "But we're a long way from being able to predict that things will go in that direction," he adds.

Complaints on the rise

Facebook isn't the only social networking sites dogged by privacy complaints. The U.S. privacy group EPIC filed a complaint earlier this year with the Federal Trade Commission over Google Buzz for, among other things, "violation of federal wiretap laws." And in June, the FTC settled with Twitter over a major security breach in which the social network was found guilty of not taking "reasonable precautions" in data security that saw 55 accounts hacked within a four-month period in 2009, including that of then-President-elect Barack Obama.

Indeed, the past year has marked a turning point for the OPC, with Privacy Commissioner Stoddart handling a dramatic increase in complaints involving new technologies, mostly online. Keeping abreast of such changes has forced the OPC to take a new multipronged approach.

"We recently added a number of new staff members with an expertise in technology issues to our investigations team," says Stoddart. "And we are currently working on building a research lab to examine new technologies and support our ongoing investigations."

Stoddart suspects that privacy violations have a lot to do with the raison d'être of these organizations, which is to earn a profit in the digital world.

"Some of these companies see personal information as a money-maker," she says. "This is spawning a digital arms race in terms of the collection of personal information. […] We're seeing too many cases where the innovators innovate and the lawyers mop up after the fact."

Recognizing both the jurisdictional and practical difficulties in carrying out its mandate with respect to foreign entities, the OPC increasingly treats Internet privacy as a global enforcement matter.

After concerns raised to her office about Google Buzz, Stoddart issued a public letter to Google CEO, Eric Schmidt, this time co-signed by the privacy advocates of nine other countries.

"Data protection authorities around the world are recognizing that the best way to make a difference for the privacy rights of our citizens is by working together," Stoddart says. "Despite the fact that the participating authorities, in many cases, had very different approaches to privacy, it was actually very easy to reach agreement on the substance and text of the Google letter. Huge multinational corporations are not going to be able to ignore our message if we're all saying the same thing. The Google letter initiative is undoubtedly a sign of things to come."

Educating the younger generation

With the vast number of social network users skewing quite young in age, educating young people about the risks and opportunities presented by the Internet and social networking tools has become a top priority.

"Only now as a society are we beginning to analyze in a meaningful way the impact of social networking," says Ariane Siegel, partner in Aird and Berlis's corporate/commercial group and technology team in Toronto.

"How can we expect young people, who don't have as much life experience, to figure out that you don't necessarily want everyone to know what you are doing or saying today, in 10 years? Acting out one way or another is often a rite of passage for young people. Previous generations were lucky enough not to have left behind some memories," says Siegel.

PAUL EEKHOFF

The New York Times recently ran an article entitled "The Web Means the End of Forgetting" in which Jeffrey Rosen, a professor at George Washington University, looked at the impact of the Internet and social media sites on reputation.

"There are some pretty interesting developments in there on approaches to dealing with the massive aggregation and integration of data that is occurring. Some proposals like providing individuals with the opportunity to declare reputation bankruptcy, or helping individuals segment their different selves are a good start for discussions and practices on how we deal with this complicated issue," says Siegel.

In Canada, the Canadian Marketing Association has designed guidelines for members on the collection and use of personal information of children and teens.

"Parents and schools, educators need to also work together to help teens understand privacy and understand the risks associated with the online environment," says Siegel. "I know the OPC has worked hard on a separate website targeted to youth dealing with privacy, I am just not sure that it is the first site youth will visit when they are on the web."

Best practices

Just as the "collection of personal data must be reasonable" under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the U.S. Twitter settlement brings into question just what "reasonable measures" are. How does the definition of reasonable adapt in a fast-moving technological landscape and how can companies perform due diligence if they don't know exactly where the bar will be set in the eyes of the law, today, let alone a year from now?

"One of the things that really struck fear into the hearts of businesses a number of years ago was when [former Canadian Privacy Commissioner] George Radwanski stood at a podium and said "I am the reasonable person," referred to in PIPEDA. Most people would consider him as the polar opposite of a reasonable person in that regard," muses Fraser. "Reasonable is kind of an objective-slash-subjective thing. And it may be something that you'll never get a good definition of, so that you know whether you're clearly offside."

According to Geist, companies ought to first rely on common sense smell tests about what's reasonable from a privacy perspective. "Of course, there are going to be novel business models and technologies that are going to present challenges in terms of how you apply some of those rules, but the reality is that most business people, and most lawyers, will have a pretty good sense if they're pushing the envelope," says Geist.

Siegel also recommends the simple, common sense approach, and not taking anything for granted.

"Don't copy and paste another company's privacy policy and feel confident that is all you need to do to comply with Canadian privacy requirements," she warns. "Understand that there are jurisdictional and cultural differences, both across Canada and in other countries. And always remember that customer personal information is often your most important asset. Treat it like gold. It is very difficult to overcome the negative publicity associated with distrust over privacy."

She advises clients to spend time upfront to consider how privacy practices may affect their relationship with customers. "Ontario's Privacy Commissioner coined the phrase 'Privacy by Design' many years ago. The single most important step an

organization can take is to apply that motto and build processes and personal information treatment into the operational chain."

Training and awareness sessions are particularly useful in helping individual to understand the rewards and some of the risks associated with any online activity.

"It is really important that employers recognize that there are generational differences in how individuals communicate, and changing attitudes toward our comfort levels in sharing information. Some companies have barred use of social networking sites on workplace resources, for instance; others have allowed open access. There are interesting opportunities and tools out there for branding and marketing, but consider some of the risks and adopt strategies to mitigate them. Adopt new technologies responsibly and build awareness," Siegel suggests.

Canada at the forefront

To ensure that Canadian privacy laws are robust enough to handle online privacy challenges, Stoddart asked France Houle, of the Université de Montréal, and Lorne Sossin, the Dean of Osgoode Hall Law School to examine a wide range of issues around PIPEDA, its impact and the powers of the OPC.

The report, released last July, concluded that overall, Canada's private-sector privacy regime has been more effective among large businesses than among smaller firms.

One way to protect consumers would be to expand the commissioner's powers to draw up explicit and enforceable guidelines, and to levy fines or other penalties to ensure compliance. But broad or intrusive powers may be unnecessary. "We have, in fact, witnessed a trend — in Canada and elsewhere — away from strict reliance on judicial enforcement, and toward guidance and other soft-law alternatives. With technology changing so rapidly, it may make sense to have greater regulatory speed and agility, with recourse to the courts for intractable disputes," says Stoddart.

Still, there are concerns about placing too much power into the commissioner's hands "The commissioner is an advocate for privacy, and you don't want to have the judge and the cop being the same person. To me, that seems a conflict of interest," says Fraser.

As for evolving technology, Geist reminds us that the current privacy rules, themselves based on OECD guidelines that date back to the 1980s, are pragmatic and not at all technology specific — "and that's very much a feature, not a bug," says Geist.

"The challenge is having to apply them to newer business models, newer technologies, and having a full understanding of what exactly is taking place. […] But if you take a look at the Privacy Commissioner's case with Facebook, to me it's a classic example of the commissioner digging deep into an issue and coming away with a pretty in-depth understanding of exactly what was taking place."

The strength of Canadian privacy law, says Siegel, is that it is open to interpretation. "As we evolve and as business models develop, as new technologies arise, and even as our social norms may change, PIPEDA can evolve too."

Between what she views as this country's incredible contributions to the fields of technology and communication, well-respected regulators and great thinkers in those fields, plus a growing and successful entrepreneurial culture, Siegel forecasts exciting days ahead. "Canadians are in a great position to provide business and policy leadership in this area." **N**

Jason Scott Alexander is an Ottawa-based freelance writer specializing in frontier-media and technology law topics.