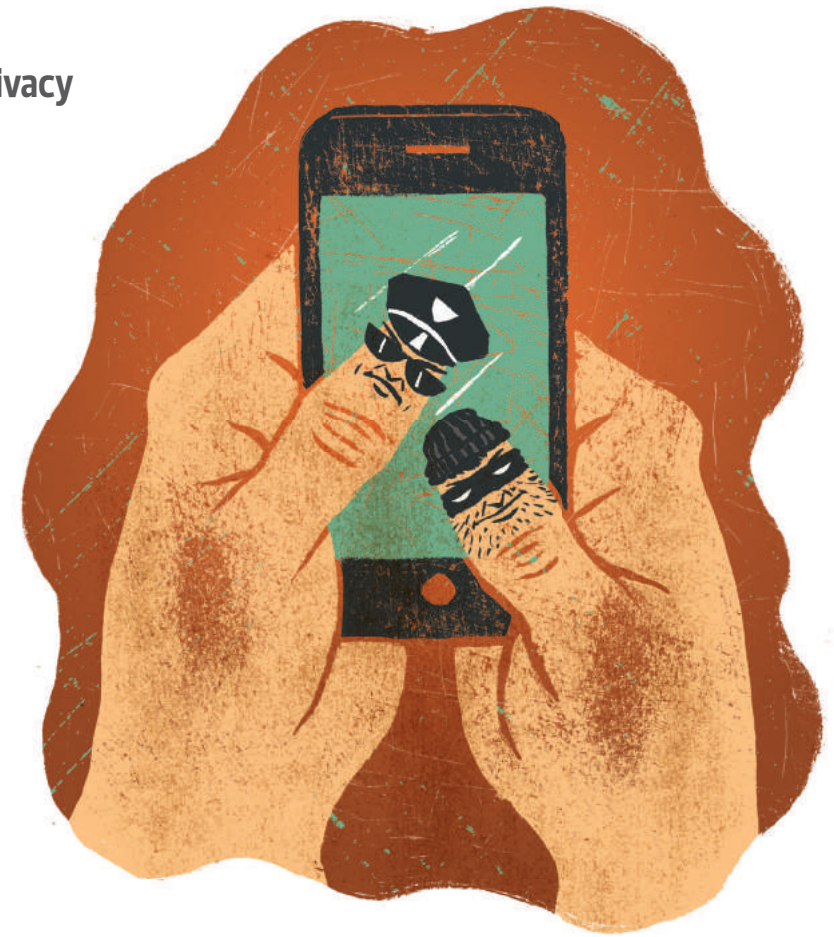
# Privacy law a bomb waiting to go off

**Federal legislation, court challenges helping to determine guidelines of privacy rights and obligations in cyberspace.**

BY MARK CARDWELL



OLEG PORTNOY

When Toronto lawyer Scott Hutchison was called to the bar in 1989, personal computers were confined to desktops, cellphones were the size, shape, and weight of bricks, and fax machines were all the rage in telecommunications. Now likely past the midpoint in a legal career devoted largely to civil, regulatory, and criminal litigation, he marvels at the quantum leaps in technology that have turned small portable devices into personal communication and computing powerhouses. "The eight-ounce phone that people carry around in their pockets can create content, send and receive text-based communications, [and] are calendars, phone books, and mailboxes all at the same time," says Hutchison, a senior partner at Stockwoods LLP and a former Ontario Crown attorney. "I've heard it said — and I like to repeat — that people walk around today with more personal information on their person than their parents generated in their entire lifetimes."

That's why he and jurists who are deeply interested in the issue of privacy are anxious to see pending federal legislation that seeks to both clarify and establish the rights and obligations of people and businesses in regards to personal information in cyberspace. And, as with other recent legislation on the issue and related changes to the Criminal Code, they expect the new provisions will be challenged in the courts almost immediately, joining a long list of cases that are helping to sharpen the focus of a fast-growing and wide-ranging national and international legal and ethical debate.

Introduced in the House of Commons in September and expected to be passed into law this spring, bill C-12 — the safeguarding Canadians' personal information act — proposes several amendments to the Personal Information Protection and Electronic Documents Act, which has governed and regulated the collection, storage, use, and disclosure of personal information in mostly commercial dealings by business and government since 2000. A reintroduction of bill C-29, which made it to second reading before dying on the

**"The Criminal Code and all federal legislation need to be modernized quickly in order to keep pace with the ubiquitous nature of electronics. Either Parliament or the courts will have to step in."**

FRANK ADDARIO

order paper when the 2011 election was called, C-12 is primarily designed (according to an Industry Canada backgrounder) to sharpen the legal teeth of PIPEDA in an effort to protect and empower consumers and "enable effective investigations by law enforcement and security agencies."

Among other things, the changes would make it mandatory for businesses to report "material breaches of security safeguards" to a privacy commissioner and to notify individuals if it determines the sensitivity of the personal information involved in the breach is such that, if misused, would put those individuals at "real risk of significant harm," which includes everything from bodily harm and humiliation to loss of property or employment.

Though businesses already have a civic duty to report crimes and evidence of offences to police (a mandatory obligation for Internet service providers in regards to child pornography since last March, when Bill C-22 was passed), the proposed legislation does not require businesses to turn over evidence without a warrant or production order, thereby preserving the current voluntary standard for them to report crimes and/or co-operate with police in cases where they have been victims of cybercrime or suffered a security breach or hacking.

The lack of incentive and the proposed scope of discretion for companies to report and disclose are the most problematic provisions for many observers of bill C-12, which one legal wag has already dubbed the "anti-privacy privacy bill." In terms of consumer protection, the legal counsel for the Public Interest Advocacy Centre, an Ottawa-based, non-profit consumer protection group, thinks C-12 will do little to bolster consumer confidence about the safeguarding of their personal information in a fast-paced world where electronics are ubiquitous.

"Data breaches affect consumer confidence (but) in bill C-12, a breach remains in the eye of businesses," says John Lawford. He co-authored a report issued by the PIAC in January that recommended companies be required to report breaches to the federal privacy commissioner, who should also be granted the power (which the privacy commissioner argued unsuccessfully for in public hearings on C-12) to both assess the level of "significant harm" involved and order companies to contact individuals if the need to do so is determined.

For Lawford, companies today have myriad methods and manners to monitor and collect personal data and to build profiles about people when they interface with the Internet, either with their permission or without. "That ability will just keep accelerating [and] cross-referencing as e-commerce continues to grow and develop," says Lawford. "Voluntary reporting is a nice idea, but it's probably pretty weak in helping a company decide whether or not to report or disclose a breach that could compromise its future or reputation."

Consumer protection however pales in comparison to the legal debates and Charter-based court challenges that C-12 and bill C-30, a broader piece of cybercrime-fighting, Criminal Code-altering legislation that was introduced in the House of Commons in February, are expected to generate in regards to privacy law. Bill C-30 will notably make it mandatory for ISPs to provide customer names and addresses to police on request and without a warrant, and to preserve information.

According to Andrea Slane, a lawyer and associate professor with the Faculty of Social Science and Humanities at the University of Ontario Institute of Technology, businesses that have been victims of cybercrime, such as the Sony PlayStation Network, which was paralyzed for weeks by a massive data breach late last year, are notoriously reluctant to report such crimes for fear of repercussions from investors and/or customers.

"Even if [C-12] becomes law, businesses will continue to weigh the various factors that could tip the balance of civic duty toward disclosure," says Slane. She adds that voluntary reporting could become even trickier for businesses in cases where employees or customers were found to be using its Internet services and/or its hardware to commit cybercrimes. That's why she believes that the scope of discretion for private entities proposed in bill C-12, together with a growing body of appellate-level case law that focuses on the proper application of s. 8 of the Charter of Rights and Freedoms, which protects against unreasonable search and seizure, will make for some impressive legal fireworks. "I think it's a no-brainer that someone somewhere will mount a s. 8 challenge," Slane tells *Canadian Lawyer*.

Frank Addario agrees. He is the lawyer for Richard Cole, a Sudbury, Ont., high school teacher who was charged after nude photos of a Grade 10 student were found on a laptop issued to him by his regional school board — photos that were ruled inadmissible by the Ontario Court of Appeal a year ago on the principle, which the Supreme Court will begin

hearing an appeal against on May 16, that Cole had a right to expect his personal files on the computer's hard drive would remain private. Addario says the courts need to and will play a pivotal role in helping to shape and provide new and profound real-world meanings to the privacy rights and obligations of individuals and companies in the ether-based realm of information technologies. "The belief that ownership means control of privacy is now an old-school way of looking at privacy," says Addario. "A key issue that will require the courts to think carefully about information technology is the reality that many people now use employer-owned devices for personal and work-related communications. There is rarely an ability to distinguish the two."

Addario also points to the ground-breaking majority ruling from the Saskatchewan Court of Appeal in March, *R. v. Trapp*, which sided with a Saskatoon man who was arrested and charged after his Internet service provider SaskTel gave police his address and telephone number after they discovered child pornography in a shared electronic file. Brian Trapp successfully argued in his appeal from conviction on charges of possessing and distributing child pornography that he had a reasonable expectation of privacy in the IP address SaskTel assigned him, and that the disclosure constituted an unreasonable search under s. 8. "The Criminal Code and all federal legislation need to be modernized quickly in order to keep pace with the ubiquitous nature of electronics," says Addario. "Either Parliament or the courts will have to step in."

For Hutchison, the *Cole* and *Trapp* rulings, together with groundbreaking decisions in two other Ontario Court of Appeal cases in 2011 suggest that privacy law is a bomb waiting to go off. *R. v. Manley* accepted the proposition that police need a search warrant to go through an arrested person's cellphone; and *R. v. Jones* said no to a police search of a database to try to find child pornography. "Police will do whatever they have a right to do to investigate crime, as they should, and for that same reason we should be very careful about the powers and tools we give them," he says. "The courts are doing their part to craft the privacy rules of the road for information technology. But the problem is lawmakers are having a hard time keeping up with all the changes in electronic devices.

"I understand that it's complicated [and] PIPEDA is an incredibly dense statute [and] the federal justice department is trying to accommodate the wants and needs of police forces to find palatable and workable solutions for Canadians and businesses," adds Hutchison. "But we've been talking about this for a decade now and we still don't have clear privacy policy for the gathering, collection, and distribution of data. Unfortunately, bill C-12 isn't going to change that."