Tech advances reshaping insurable privacy risk

BY DAVID MACKENZIE

As technology that tracks and records our daily lives becomes ubiquitous, privacy risk is moving beyond data breach and ransomware, which currently dominate media attention. Advances in technology are reshaping insurable privacy risk, yet scant attention is being paid to the full extent of the exposure involved in collecting and using data, and how best to insure associated risks.

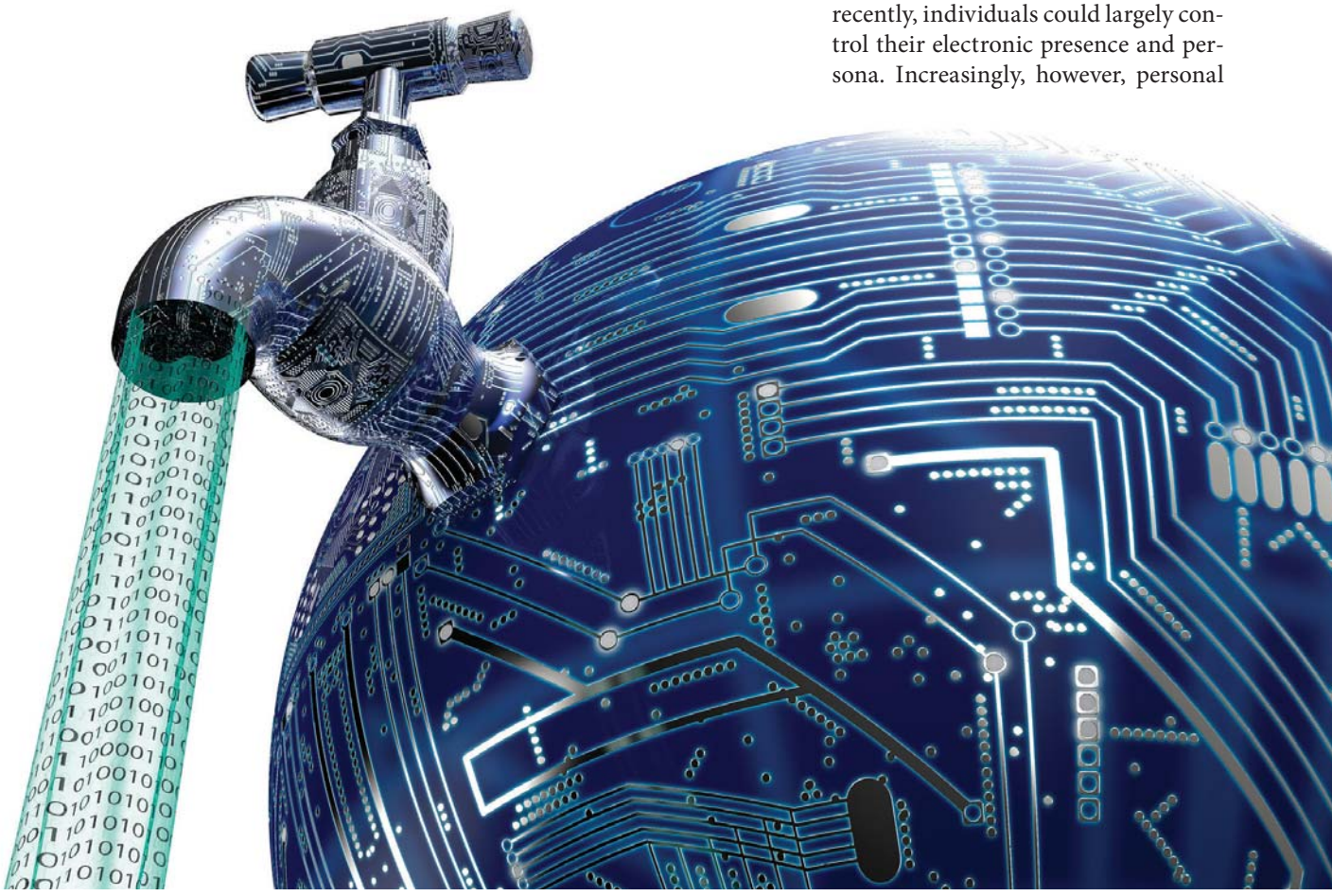
Insurance profit is generated through assessment of and protection from risk. Insurance companies, and those who act on their behalf, should be paying close attention to the growing tension between rapidly expanding technology and individual privacy interests. Opportunities are emerging.

Using existing technologies, companies are able to collect almost incalculable amounts of data from individuals, including information on family status, employment, financial information, physical and mental health status, ethnic background, sexual orientation, immigration status and even a person's regular daily habits.

Many organizations believe they are allowed to use this data as they see fit. For the most part, consumers don't understand how their data is being used and sold. But they will, and so will their lawyers, who will be turning their attention to emerging and novel grounds of liability as technology erodes traditional fee-generating areas of practice, such as automobile-related personal injury claims. Privacy litigation, technology litigation, and regulatory litigation will be the new fodder for the plaintiffs' bar.

Technology we could barely imagine a few years ago has already arrived. The Internet no longer exists solely on our computers and mobile devices. It is increasingly ambient, with many billions of sensors now in use in homes, workplaces, cars and in the environment generally.

Many people are uncomfortable with the resulting loss of privacy. Until recently, individuals could largely control their electronic presence and persona. Increasingly, however, personal



data footprints are likely to generate as much disquiet for those concerned with privacy as carbon footprints do for environmentalists. It is a future fraught with risk, but also one that portends opportunities and competitive advantages for Canadian businesses and insurers.

Because of these growing privacy concerns, new legal barriers are looming. How will companies that generate or obtain data be permitted to use it? Privacy rights, long an afterthought, have come into their own, recognized both by legislation and ever more fully by judges, who are extending broad common law recognition to concepts characterized as "intrusion upon seclusion," "public disclosure of private facts" and the "right to be forgotten."

The conflict between ever-increasing access to personal data and emerging limits on using that data foreshadows a great deal of litigation, early examples of which have recently emerged in the United States. Google has been sued for exploiting loopholes in cookie-blocking technology that allows advertisers to track users in ways to which they had not consented. LinkedIn faced litigation for accessing email contacts folders to seek out new users. Bose is fighting allegations that an app on its headphones surreptitiously collects customers' listening habits and provides that information to third parties.

Each of these claims engages privacy issues. Did Google intrude on seclusion by giving third parties access to information to which users had not consented? Did LinkedIn cast its users in a false light when it used their email contacts list to invite others to join LinkedIn, suggesting that the users themselves were involved in sending the invitation? Could disclosure of personal listening habits, as Bose is alleged to have done, embarrass headphone users with terrible tastes in music? While all the foregoing involve global corporations, privacy risk issues also exist on the most mundane levels: for example, can landlords use personal information collected by third parties to determine the suitability of tenants?

Wearable technology, GPS tracking and connected medical devices compound the problem by collecting individuals' health and physical activity data. How will companies exploit that knowledge? Do they risk liability in the approach they take?

Snapchat's new "Snapmap" function, when activated, can broadcast an individual's whereabouts to every one of their contacts. Does the company risk exposure for tracking someone's location within inches and disclosing that information to others?

All these risks can arise from technologies that many Canadian businesses are already using. Virtually all of these risks are insurable. The dilemma facing the insurance industry relates to the type of coverage and the language under which these risks should be insured.

"Cyber" coverage seems an obvious place to start. But the primary focus of these policies remains accidental or

criminal breach, rather than privacy claims related to intentional business conduct. While some cyber policies may cover this risk, the lack of standard wording suggests that many will not. To the surprise of many, perhaps, coverage is also likely to be found in other commonly used standard form policies that expose insurers to an array of privacy risks.

Many insurers have not updated their CGL, bricks and mortar property, or professional errors and omissions policies to exclude or eliminate coverage that is being sold and priced in the cyber and technology insurance markets. But as contexts have changed, the courts have not been afraid to expand existing coverage and language written in other times to make the consumer whole in the modern world.

CGL coverage, for example, offers privacy coverage for publication of material in any manner that violates a person's right to privacy. But the extent of the coverage in the modern context is unclear: did LinkedIn publish material that violated privacy rights when it sent emails to individuals found in customers' contact folders? Did Google publish material that violated privacy rights when it circumvented cookie blockers by sending information from website to website as a user was surfing? What about Bose's alleged sale of data pertaining to users' love of early Styx albums?

Is the CGL policy really the right place to cover privacy risks? Or should the industry be considering whether other policies (e.g. Cyber and Tech E&O) might be more effective? Unless the industry addresses these issues directly, only time will tell which policies will respond best. Better to understand the risk and underwrite it intentionally. "Accidental" coverage is an unpleasant and expensive surprise.

Adding grist to the mill, a recent decision from the Supreme Court of Canada (SCC) suggests that Canada is emerging as fertile ground for privacy and technology-related claims. In Douez v. Facebook, the court characterized privacy rights as "quasi-constitutional". On that basis, the court refused to enforce a clause in Facebook's terms of service that required lawsuits against Facebook to be filed in California (a jurisdiction favorable to Facebook). In another recent decision establishing individual rights broader than in most other countries, the SCC ordered Google to take down all of a company's websites, both inside or outside Canada.

Clearly, the risks related to data breach are of great concern to Canadian businesses and insurers. At the same time, a wave of privacy litigation may be emerging from under the radar. Canadian insurers will not want to ignore these developments, and will wish to consider how best to address them from an underwriting perspective. Risk, after all, creates opportunity for insurers. These new privacy risks are no exception.

David Mackenzie is Partner, Insurance Practice at Blaney McMurtry LLP in Toronto, Ontario.