Focus

PRIVACY LAW

Jordan Walbesser

Last month, the Court of Justice of the European Union (CJEU) ruled that individuals have the "right to be forgotten." Practically speaking, the ruling allows Europeans to force companies to remove links to embarrassing information. The CJEU decision sets the stage for extra-territorial regulation of companies headquartered outside the EU.

In the case, Mario Costeja, a 59-year-old lawyer, sued Google Inc. and Google Spain over a link to a 1998 news article. The properly published news article mentioned that Costeja had to sell his house to pay outstanding debts. Costeja found the link "embarrassing."

On May 13, the CJEU ruled that Google must remove the link to the news article because the information was no longer relevant or accurate. The news article will remain online, but the link will no longer appear in some Google searches.

To reach this outcome, the CJEU found two key elements:

■ The right to be forgotten provisions apply to U.S.-based Google Inc. Google's search function is performed by Google Inc. in the U.S. and Google Spain's profitable advertising service (which collects personal data about EU citizens) occurs in Spain. The CJEU held that the two activities were "inextricably linked." Therefore, the CJEU found jurisdiction.

■ With jurisdiction established, Google Inc. is required to comply with the EU privacy law. Finding information containing personal data (even if published by others on the Internet), indexing that information automatically, storing that information (even temporarily), and making that information available to users in an ordered list classifies it as "processing of personal data." As such, the CJEU classified Google Inc. as a data controller —allowing European individuals to request removal of certain data.

The CJEU made clear that any right to be forgotten is not absolute. A request to remove links must be balanced against the "preponderant interest of the general public." Google now has to decide if "in all the circumstances" the personal information is "inadequate, irrelevant or no longer relevant, or excessive." Such an analysis inevitably becomes subjective and onerous for a large company like Google.

On the first day accepting takedown requests, Google received over 12,000 submissions, with 31 per cent linking to fraud/scam articles. Arrests for violent crimes accounted for 20 per cent, and 12 per cent were related to child pornography arrests. Understandably, these links embarrass the requesters. But the same links provide valuable information to the public. It's unclear how Google will balance these competing interests.

The biggest impact of the CJEU decision is jurisdictional. The CJEU took an exceedingly broad view of its geographic reach. As a result, non-EU companies with limited sales operations or equipment in the EU are potentially subject to EU privacy laws.

Jurisdiction, Page 15

Focus PRIVACY LAW

When medical records go missing

Legal regimes and remedies in Ontario differ depending on the source of the information

Nina Bombier
Paul-Erik Veel

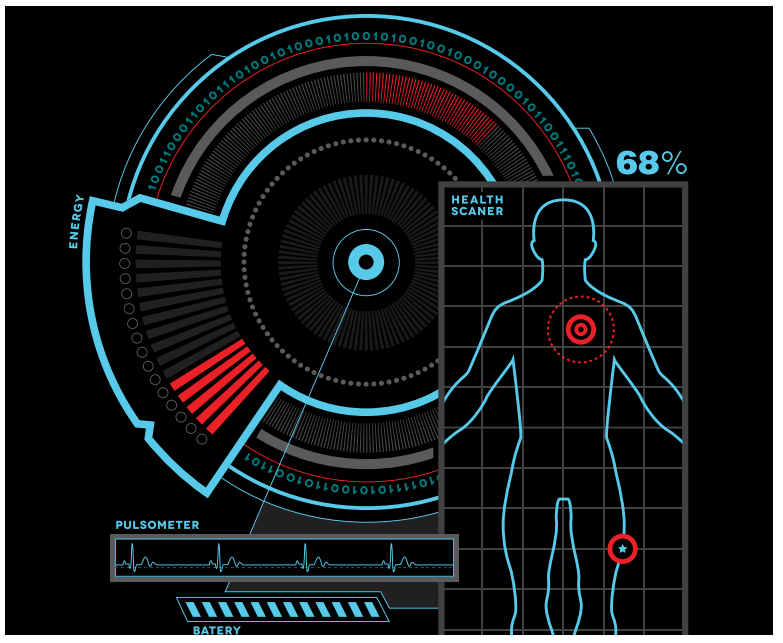
As lawyers, we routinely come into the possession of medical records. Unfortunately, those medical records can sometimes be lost or stolen. We may accidentally leave our briefcase somewhere and it is then nowhere to be found; even worse, our laptop may be stolen from the car or office.

While we are familiar with our obligations to safeguard confidential information, medical records contain personal health information that is subject to the unique regime of Ontario's *Personal Health Information Protection Act*. This regime may govern the loss of medical records.

Our duties turn on how we obtained those records. Three situations may occur: (i) records come from and relate to our own client; (ii) records come from an opposing party in the course of litigation; or (iii) records come from our client (a doctor or a pharmacist) but relate to someone else. In each, different considerations apply.

The clearest case is the third: we obtain medical records from our own client about someone else. In that case, *PHIPA* explicitly dictates our obligations.

PHIPA applies to any "personal health information" (PHI) held by a "health information custodian." PHI is broadly defined and includes any identifying information about an individual that relates to her physical or mental health. PHI includes the mere fact that a person provides health care to an individual. "Health information custodian" is also broadly defined and includes any health-care professional or organization that maintains health-care records.



VALENTIN_SAUTS / ISTOCKPHOTO.COM

PHIPA obliges health information custodians to take reasonable steps to ensure that medical records are protected against theft, loss and unauthorized use or disclosure. In the case of medical records stored in electronic form, records must be password-protected and encrypted. Custodians are also obligated to notify an individual, at the first reasonable opportunity, if their medical records are stolen, lost or accessed by an unauthorized person.

Lawyers are not health information custodians under *PHIPA*, but they may constitute "agents" of custodians. An agent can only collect, use, or disclose PHI on a custodian's behalf if the custodian permits the agent to do so, and such collection, use or disclosure is lawful. *PHIPA* also requires that an agent notify the custodian at the first reasonable opportunity if the PHI is stolen, lost or accessed by an unauthorized person.

Two points are important for lawyers who obtain medical records from a client who is a health information custodian. First, the client remains responsible for that information while it is in our possession. In order to safeguard the client's interests, we must treat those records in the same way as the custodian. Second, as soon as we become aware of any loss or unauthorized access of those records, the client should be notified immediately, and the person whose PHI has been stolen or lost ultimately notified. In some circumstances, it may be prudent to obtain independent legal advice for the client as to their obligations.

> "Lawyers are not health information custodians under PHIPA, but they may constitute 'agents' of custodians.
>
> **Nina Bombier and Paul-Erik Veel**
> Lenczner Slaght

By contrast, where a lawyer obtains PHI from and relating to their own client, *PHIPA* is not engaged. However, lawyers are bound by their legal and ethical duties to their clients to maintain the confidentiality of that information and notify their client if it has been compromised. While the *PHIPA* obligations do not apply directly, compliance with the same norms would likely meet the lawyer's duties to her client in this regard.

Finally, lawyers who come into the possession of medical records from another party (for example, through the discovery process in civil litigation) are also not agents of the health information custodian. Consequently, *PHIPA* does not directly apply.

Where medical records are produced in the course of litigation, they are subject only to the common law and statutory deemed-undertaking rules. The deemed-undertaking rule precludes an opposing party from using evidence or information obtained through the litigation process for purposes other than the proceeding in which that evidence was obtained.

The rule generally protects against the intentional use or disclosure of an opposing party's PHI, although it has been criticized by Ontario's information and privacy commissioner for not going far enough to protect privacy interests. While the deemed-undertaking rule may not specifically require lawyers to safeguard such information or to notify an opposing party if that information is lost, best practices would be to act like an agent of a health information custodian.

While the legal regimes differ depending on the source of the personal health information, the way in which such information is treated by lawyers arguably should be the same in any case. Reasonable steps should be taken to safeguard medical records. Electronic medical records should be both password-protected and encrypted. PHI transferred in electronic form should be secure. Finally, if medical records are lost, either clients or the opposing party should be informed of any loss or theft.

Nina Bombier is a partner at Lenczner Slaght whose litigation practice focuses on commercial, insurance, professional negligence and regulatory matters. Paul-Erik Veel is an associate at Lenczner Slaght with a diverse commercial litigation practice that includes class actions, competition law, defamation and media, employment disputes, and professional liability.

Jurisdiction: European decision could have international consequences

Continued from page 14

In addition, the CJEU's jurisdictional logic can be applied to more than search engines — hosting companies, publishers and other technical intermediaries may be affected. This is especially true because the EU classifies personal data more broadly than Canada and the U.S. For example, personal data includes public information as well as information an individual voluntarily disclosed.

Europeans are likely to make similar demands from websites that contains links, old photos, news items or other potentially embarrassing information. Although the CJEU decision applied to published data, Europeans might try to extend the right to be forgotten to unpublished data, such as marketing data.

So far, neither Canada nor the U.S. has made a major decision related to the right to be forgotten. Under PIPEDA, Canadians may compel a company to correct or delete personal information it "collected, used, or disclosed." However, the company need not make the subjective judgment required by the CJEU — only whether the individual withdrew consent or corrected information.

Companies that automatically index and publish personal data should review their corporate structures and business operations in light of the CJEU ruling. For example, companies that collect information from North America but have offices in the EU may be affected.

Companies affected by the CJEU ruling should work closely with EU regulators to confirm that their practices conform to EU law. In addition, companies should decide whether to make compliance changes for all users or just European users. Customer relations and cost efficiencies will factor heavily in this decision.

Companies should take this opportunity to review and update their terms of use and privacy policies. For example, companies should have appropriate policies and procedures for data retention and destruction. Further, companies affected by the CJEU ruling can no longer rely on content licenses from users. Europeans can request to remove their personal data at any time, regardless of a prior license.

Compliance may be a legal and technical challenge. Canadian and U.S. companies can expect to see a significant increase in the number of Europeans requesting the deletion of material and filing complaints against those who are unwilling to oblige.

Jordan Walbesser, a lawyer at Hodgson Russ, concentrates his practice in intellectual property law, with a focus on patents and business methods. He is also well versed in software, cloud computing, social media, and peer-to-peer networking issues.