TORONTO STAR

Source name
Toronto Star (ON)

Source type
Press • Newspapers

Periodicity
Daily

Geographical coverage
Provincial

Origin
Toronto, Ontario, Canada

Saturday, March 23, 2024

Toronto Star (ON)

• p. A18

• 1508 words

Province sued over medical data restriction

Storage of information at centre of lawsuit between Ontario Health and U.S. company Doxy.me

Patty Winsa Data Reporter

A lawsuit pitting a U.S. company against Ontario Health could determine if the province has the right to regulate where personal medical information is stored.

The company, Doxy.me, sells a video conferencing platform to health professionals for virtual appointments. The data captured by those appointments is stored in the U.S.

But in 2022, new standards were introduced by Ontario Health that said doctors and other health professionals could only bill OHIP if they used an approved virtual platform that kept patient data in Canada.

The company says it has lost about $10,000 a month since the OHIP eligibility restrictions came into effect, as doctors turned to other platforms, although a lawyer for the company said the money is not why Doxy is suing.

"This is a point of principle," said Stephen Aylward, one of the lawyers representing the company, in an email. "The amount at stake is modest in the context of Doxy.me's global operations."

Doxy.me is asking the court to quash the data residency requirement because it "is premised on the unfounded assumption that data stored in Canada is more secure than data stored in the United States," according to the court application.

Doxy's lawyers are also arguing that the residency requirement runs counter to the free trade agreement, which protects the flow of data across the borders of Canada, U.S. and Mexico.

If the case goes to court, it could not only shine a spotlight on the safety of online health data in a world where hacking and ransomware is more and more common, but also set a precedent as the first court case to decide if Ontario's data residency restriction should be allowed as an exception under the treaty.In Ontario, there is no overarching law that stipulates that personal medical data has to stay in the country.

Instead, the province's Personal Health Information Protection Act (PHIPA) governs how personal health information is collected, used and disclosed within the health sector, and regulates how it is safeguarded, said the Office of the Information and Privacy Commissioner of Ontario in an email.

Contractual agreements between the custodians who collect the data - such as a doctor or nurse, hospital or long-term-care home - and the storage providers, are used to ensure both parties are meeting PHIPA requirements.

The pandemic, however, fast-forwarded virtual medicine and, with it, some of the regulations around the storage of data.

While B.C. got rid of its requirement that data collected by public institutions be stored in the country, in the interests of finding the best technology no matter where it is, Ontario Health brought in a standard that the data stay here.

The new standard - called the Ontario Health Virtual Visits Verification Program - said in part that medical professionals could only bill OHIP if the data retained by those virtual platforms remained in Canada.

There are about three dozen technologies listed on the Ontario Health website that meet the government agency's new virtual standards.

The Ministry of Health said in an email that it couldn't comment on the case because the matter is before the courts. The government isn't expected to file a response to Doxy's court application until the fall and the case won't go to court before next year.

Doxy continues to be used by psychologists, who bill the individual and not OHIP. The platforms hosts more than 60,000 visits a month in Ontario.

The security and storage of personal and institutional data has become paramount in the past few years.

In Canada alone there were more than 70,000 incidents of fraud or scams related to the theft of online data in 2023, according to a report by the Canadian Centre for Cyber Security. The report noted that during COVID even more data moved online, not only medical appointments but grocery shopping, work and contact with family and friends.

"Ransomware incidents hit the headlines on an almost daily basis both in Canada and around the world," according to a report by the centre. "Our essential services are being disrupted, from hospitals and schools to municipalities and utility providers. Our personal and financial data are being stolen, traded, or leaked online."

In Ontario, there have been incidents of high-profile hacking, including the Toronto Public Library, the Waterloo Region District School Board and more recently, a ransomware attack in Hamilton that brought down most city phone lines and disrupted city services.

Last year, a cyber attack on five hospitals in the province accessed some patient, employee and staff data, and resulted in surgeries and appointments being postponed.

But even though data breaches occur, many experts have argued that there's a need for a global exchange of data.

"There'sbeen an ongoing policy battle globally for a number of years over both data transfer restrictions and data localization requirements," said Michael Geist, the Canada research chair in internet and e-Commerce law at the University of Ottawa. "Some countries have been trying to forcefully argue that there should be few, if any, restrictions on cross-border data transfers or requirements."

That flow is seemingly protected by the free trade agreement.

As Doxy argues in its court application, "data residency requirements are prohibited under international trade treaties to which Canada is a party."

However the treaty, which has been updated from NAFTA and is now called the Canada-United States-Mexico Agreement or CUSMA, does allow exceptions.

"Ontario can still impose restrictions if this is justified for the protection of legitimate public policy objectives," said Mira Burri, a professor of international economic and internet law at the University of Lucerne. Burri notes that if the lawsuit ends up in court, it could produce the first case law on an exception in Canada.

If there are restrictions on where data is stored, Geist believes health and financial information are at the pinnacle of concern for Canadians.

Medical information "is certainly viewed as sensitive personal information," said Geist. "And many times I think people will feel more comfortable knowing that the data is localized and subject to local privacy protections and enforcement."

Although data is subject to Canadian privacy laws no matter where it's stored, Geist points out it could be harder to enforce Canadian privacy standards and court orders in another country.

There is also, he points out, the prospect that foreign laws could be applied to the data, including the Patriot Act in the U.S.

"Whathappens if, for whatever reason, the U.S government demands disclosure of some of this data for national security purposes or some reason," said Geist. "It's much harder for the U.S government to compel disclosure of that information if the data isn't in the United States."

Many private companies make the choice to store their clients' personal data within Canada, because it's difficult to verify security compliance across borders, said Claudiu Popa, a certified cybersecurity professional.

Popa is the CEO of Datarisk Canada and managing director of Managed Privacy Canada, which assess cybersecurity and privacy respectively, and provide solutions. He is also the founder of Canada's only cyber safety foundation called Knowledgeflow, a non-profit that educates students, teachers and law enforcement, among others, on cybersecurity.

"Most companies feel intuitively almost that there is a significant risk in storing the data south of the border, or in other

legal jurisdictions, versus keeping it in Canada, where it's not just physically close, it's legally reachable," said Popa. "And that's key because they need to have legal recourse" under Canadian law, he said.

Doxy argues in its court application that it retains very little data from the online visits.

The company takes a "data lean" approach, which it explains in the court application means that while it collects certain personal health information during a virtual visit, such as temporary backup files to facilitate file transfer, it does not retain - or "hold" - any of the data.

In an interview with the Star, Aylward said the only data retained by Doxy is the appointment's date, time and length, as well as the identifier of the clinical provider for the patient, and the patient's IP address, which he said is converted into a general location record that includes the patient's city, region and country.

"It is not reasonably foreseeable that a patient's IP address could be used to identify an individual patient or to connect them with any health care services provided through Doxy.me," according to the court application.

However the company's timing may be off. The Supreme Court ruled this month that the address contains enough sensitive information that could lead to the identity of a user as well as their online activities, and as such, was constitutionally protected from unreasonable search by police.

"The court concluded that people have a reasonable expectation of privacy associated with IP addresses," said Geist. "It strikes me as a loser argument on their end at this stage given this recent court decision."