THE GLOBE AND MAIL

JILL PRESSER

Here's why the Supreme Court made it tougher to look into your online life

JILL PRESSER
Contributed to The Globe and Mail
Published Monday, Jun. 16 2014, 8:27 AM EDT
Last updated Monday, Jun. 16 2014, 2:43 PM EDT

Jill Presser represented the Intervener, the Criminal Lawyers' Association, at the Supreme Court of Canada in Friday's decision which ruled that police must obtain search warrants when seeking private information from Internet providers. She is a partner with Schreck Presser Barristers in Toronto.

We are all Internet users now. This means that we are all affected by the recent Supreme Court of Canada decision *[http://www.theglobeandmail.com/news/national/supreme-court-privacy/article19155295/#dashboard/follows/]* dealing with online privacy.

More Related to this Story

- DAVID BUTT Five ways the Supreme Court ruling affects online privacy
- Canadians have right to online anonymity, Supreme Court rules
- Conservatives mum on changing privacy bills after Supreme Court ruling

To understand the decision, let's start with the basics. Your Internet identity is made up of three things: your Internet name, your "IP address" and the match between the IP address and who you are in the real world. Internet privacy is all about the barriers between the people who can see your Internet activity (hey, it's a public place) and their ability to match your IP address with your real-world identity. The matchup info is held in trust by your Internet service provider, usually one of the big four telecom companies.

Friday's case was about how hard it should be for the police to make the telecom companies match IP addresses to real-world identities. Once the telecom provider gives the police the matchup info, all of your Internet activity – which you've conducted under the veil of your online identity – becomes irrevocably linked to your real-life identity.

What you watch and what you say and what you read on the Internet is up to you. You may choose to make it clear who you are, to spell out your real-world identity. Or you may stay behind an online identity. You can see things, read things, and say things that are against the law or within the law. This case writes new rules about what happens when you perform Internet activities behind your veiled online persona.

So here are a few key things Internet users need to know:

- Law-breaking is still illegal. Canadians online must not interpret Friday's decision as a permit to write hate literature, view child pornography or listen to pirated music. No laws were overturned in Friday's decision. The rules are still the rules. They should be obeyed. And if you don't like them, ask Parliament to re-write them. Don't go thinking the Court just re-wrote them for you and don't try to re-write them yourself;

- You are still in control of whether you reveal your real-world identity or not. Friday's decision, broadly speaking, makes it harder for those who want to monitor your online activity to link it to your real-world identity;

- If you are being investigated for unlawful Internet activity, e.g. hate speech, child pornography, Internet fraud, it just got harder for the police to obtain your real-world identity. Before this decision, law-enforcement officials were obtaining increasingly routine access to telecom company data matching IP addresses with real-world identities. The key question before the Court was whether a search warrant is needed for police to seek out the matchup data from the telecom company. The Court ruled that a warrant is required. That makes it somewhat tougher for law enforcement to catch cybercriminals.

Readers may ask at this point why the Court just made it somewhat harder to catch cybercriminals. The answer lies in the right to be free from unreasonable search under the Canadian Charter of Rights and Freedoms. The Charter is the supreme law of Canada. It is an expression of the very high value Canadians place on this fundamental human right. Our right to privacy is expressed as a right to be free from state intrusion through unreasonable search. The Supreme Court correctly put this right ahead of making it a little easier for the police to do their job.

The Supreme Court has considered the new territory of the Internet and set the borderline between the power of the police and the privacy of the individual in an expansive way. A great deal of space has been reserved for privacy. Indeed, within that space, a reasonable expectation of privacy through anonymity has been laid out. What does this mean? It means that it will take some convincing for a government actor to persuade a court that a consumer or online user's interest in remaining anonymous should give way to a law-enforcement objective. And, in fact, the prospect of having to argue about this in court at all may operate to powerfully restrain governments and businesses from pushing into the domain of consumer anonymity.

The effect of this ruling may well be felt most acutely in the cutting-edge government and corporate cyber-communities. Those who are planning "smart billboards" that recognize real-world individuals and spew consumer information at them will likely need to reprogram. Biometric surveillance, which looks at individuals, not at records, data and online behaviours, may come under pressure. Consumers may feel the effects of this decision more in what does not occur than in what does.

Friday's decision is indeed a landmark, marking out an expansive domain of privacy deep into the new world of cyberspace.

Follow us on Twitter: @GlobeDebate *[https://twitter.com/@GlobeDebate]*

More Related to this Story

- Globe editorial Get a warrant if you want to get into an IP address

Topics:

- Supreme Court of Canada