

Will other countries join the Canadian debate over the privacy of public records?

By Jay Cline

Federal privacy commissioner of Canada Jennifer Stoddart recently re-ignited a debate that has lied fallow for years. In her December 2008 Annual Report to Parliament, Stoddart highlighted as one of her top concerns the widespread availability of personal data among public records. With citizen and industry interests beyond Canadian borders lined up on both sides of the issue, this debate contains the ingredients to become a global conversation.

"Highly personal information about Canadians fighting for government benefits and taking part in other federal administrative and quasi-judicial proceedings is being posted to the Internet," Stoddart wrote, "exposing those people to enormous privacy risks."

If Stoddart is successful in shifting the balance between public accountability and personal privacy, she will be establishing a landmark in a centuries-long series of developments.

13th century origins

When the barons under King John of England compelled him to enumerate in the Magna Carta the limits of his powers, they were unwittingly drawing a line in the sands of time. Their principle--that the governed have a say in how they will be governed--later formed the bedrock of common law that spread throughout the British Commonwealth, the principal heirs of today's debate over public records.

That the governed need information in order to have their say was alluded to by another Brit, Sir Francis Bacon, when he observed in 1597 that "knowledge is power." But it was not until 1966 that this concept was enacted with regard to citizen access to public records. That year's U.S. Freedom of Information Act spawned over the next generation similar acts in Canada, Australia, New Zealand, Hong Kong and the UK.

The Freedom of Information Act (FOIA) request--where citizens can gain access to government documents--has since become a staple of reporters and lawyers seeking to hold democratic governments accountable to the governed. Each year, the CIA alone fields roughly 3,000 FOIA requests, according to its annual report to Congress.

The case for public access

Proponents of continued public access to government and court records that also contain personally identifiable information of government employees, convicted criminals and innocent citizens say the public has a right and a need to know this information. They say people have a right to know, for example, if they and their neighbors' homes were assessed taxes fairly, if a sex offender moves into the neighborhood and why the police raided the house down the block.

According to the *Canadian Broadcasting Corporation (CBC)*, the taxation department of the provincial government of Prince Edward Island recently launched a web-accessible database called Geolinc the gives access to property assessments, tax information, deeds and mapping information for any parcel of land on the island.

"It's used by corporations, companies that have an interest in land, financial institutions, real estate [agents], law firms," Assistant Provincial Tax Commissioner Jim Ramsay told the *CBC*.

Indeed, when the city of Victoria, British Columbia launched a similar system, the average number of daily visitors to the site reportedly jumped from 30 to 15,000.

Neighborhood concerns are also at the root of the public nature of marriage and divorce records. In 1800, marriages in the U.S. resulted in an average of seven children, a large impact to their surrounding communities. As such, the public had a high interest in stable homes that produced law-abiding citizens.

For their part, reporters and attorneys say they need access to PII within public records to hold accountable specific individuals in their dealings with the government. Taxpayers have a right to know the salaries of public officials, they argue, and to know who is donating how much to each candidate for elected office.

Several industries also support public access. Auto-insurance companies say without access to databrokers' files of driving records, they would need to set higher premiums for many to account for the added risk of the unknown. Credit bureaus and data brokers argue that they help protect privacy by using public records to offer anti-fraud services.

The case for reform

Privacy advocates counter that FOIA laws were written before the advent of the Internet. Before, they say, there was "practical obscurity" of PII in public records because there was no easy way for the public to access these records. Reporters and lawyers could dispatch their professional duties within the confines of obscure data-access processes. Now, advocates say, the Internet browser exposes this PII for uses beyond the intended purpose of the original data collection.

"But is it in the public interest," asked Stoddart in her annual report, "to make considerable amounts of an individual's sensitive personal information indiscriminately available to anyone with an Internet connection?"

"The decisions of administrative and quasi-judicial decision-makers are routinely packed with personal details that not many people would be comfortable sharing widely: salaries, physical and mental health problems as well as detailed descriptions of disputes with bosses and alleged wrongdoing in the workplace," she added.

"In addition to the types of personal information legitimately needed in these bodies' reasons for decision, seemingly irrelevant information is often included--the names of participants' children; home addresses; people's place and date of birth; and descriptions of criminal convictions for which a pardon has been granted, for example."

Canada is not alone in this experience. Carl Malamud, who operates Public.Resource.Org, has inspired U.S. lawyers to contribute 20 percent of all U.S. federal court documents to his free-access Web site. According to *Wired Magazine*, a recent search of these documents found 1,700 that included Social Security numbers, including one with a 54-page list of the names, medical problems, Social Security numbers and birth dates of 353 patients.

Malamud argues that his system helps surface these privacy exposures for the public to take action about them. "If we want to be serious about personal privacy, we can only do so if we are also serious about public access," Malamud reportedly told court administrators.

Stoddart concluded her report by proposing that privacy enhancements could be added to public records without harming the goals of government transparency.

"It is beyond debate that the public requires access to the information necessary to maintain confidence in the integrity of a tribunal's proceedings, to enhance the evidentiary process, to promote accountability and to further public education," she wrote.

"Yet in most cases, these important goals may be accomplished without disclosing the name of an individual appearing before a tribunal," she stated.

Reform options?

Many national-level freedom of information acts already contain in them exemptions and conditions that can be exercised to protect the unnecessary disclosure of personal information. But little conformity exists in the application of these exemptions, particularly at the provincial, state and local levels of government, and few were written anticipating elevated risks of the Internet.

Stoddart and others have proposed different versions of the following first steps toward reform:

- Depersonalize court decisions available on the Internet by replacing names with randomly assigned initials, or where the inclusion of names is necessary, use a web robot-exclusion protocol to minimize the ability of Internet search engines to find those names.
- Redact from existing government and court records available on the Internet all sensitive personal data, such as the data types that would trigger a security-breach notification under California SB1386.

- In any national breach-notification legislation, ensure that it overrode any provincial or state statutes that cause the public exposure of sensitive personal data.

If the reformers succeed, their efforts may amount to nothing less than a Magna Carta 2.0 that redefines the new power relationships of the Information Age.

Published in the 1to1 Privacy newsletter, 19 January 2009

<https://www.1to1media.com/view.aspx?DocID=31351>