Office of the Information and
Privacy Commissioner of Alberta

Data Privacy Day Op-Ed: Privacy Breaches

Jill Clayton, Information and Privacy Commissioner

Submitted to the Edmonton Journal and Calgary Herald
January 28, 2016

January 28 is the day that Canada, along with many countries around the world, recognizes Data Privacy Day. This year, my office is using Data Privacy Day as an opportunity to emphasize the importance of valuing and protecting personal information by raising awareness about privacy breaches, and what we can all do to reduce the risk to ourselves, our clients, customers and employees.

When you give your personal information to organizations with whom you do business or government agencies providing services to you, or your health information to health practitioners helping you on the road to recovery, you expect it will be protected.

In Alberta, privacy laws require private sector businesses, public bodies, and healthcare providers to make sure reasonable safeguards are in place to protect your personal and health information. In the private sector, the law requires businesses to report privacy breaches to my office where there is a real risk of significant harm as a result of a privacy breach.

Since 2012, private sector businesses report roughly one breach every five days to my office. In 2015, there were nearly 250 breaches reported by the public, health and private sectors. These incidents affect millions of Albertans each year.

Privacy breaches reported to my office reflect our increasingly online world. Personal information submitted to e-commerce websites is often a target for hackers. Malware is used to compromise servers, and social engineering ploys are used to trick employees and consumers into giving up personal information.

We regularly hear from all sectors reporting lost or stolen mobile devices. In almost all of these cases, the risk of harm resulting from the breach could have been reduced or eliminated by not storing personal or health information on the device, or by encrypting it.

We are also seeing an increasing number of “snooping” cases – privacy breaches that occur when authorized users of an information system abuse their access rights to look up others without a legitimate reason to do so. Last year saw charges laid in three cases where healthcare workers were alleged to have inappropriately accessed health information. In another case, an individual was convicted for accessing health information in contravention of Alberta’s *Health Information Act* and for falsifying documents under Canada’s *Criminal Code*.

Many other privacy breaches reported to my office don't involve malice, but rather result from human error. Nonetheless, tax slips sent to the wrong recipient, or a technical glitch that leaks employee information on a public-facing website can have real consequences for individuals.

The risk of many of these breaches occurring can be mitigated with more rigorous safeguards including information system audits, proactive monitoring and encryption, policies and procedures, and staff training, education and awareness.

Individuals must also be vigilant: shop only on reputable and trusted websites, don't respond to phishing emails that ask you to share personal information, ask why your information is being collected and how it is protected, monitor your credit report, and exercise your rights under legislation to know more about to whom and in what circumstances your personal information has been accessed or disclosed.

Jill Clayton
Information and Privacy Commissioner of Alberta

The Commissioner is an Officer of the Legislature and is independent of government. The Commissioner has oversight for compliance with the Freedom of Information and Protection of Privacy Act (FOIP), the Health Information Act (HIA), and the Personal Information Protection Act (PIPA).