

For Your Eyes Only - Proactive Steps to Avoid Privacy Issues

Institutions must take proactive steps to avoid privacy issues. With technology making large amounts of personal information readily available and easily accessible companies and institutions are under increasing pressures to ensure that any personal information they have in their custody is kept confidential and well secured. At the same time, people and consumers are more aware and concerned about safeguarding their privacy and ensuring that personal information is protected. Incidents of identity theft and fraud are becoming common. Institutions must proactively safeguard information they have and protect not only their users' information, but also information regarding their company and employees.

The earliest and most inexpensive way to safeguarding personal information and protecting your institutions from liability is to develop and implement a strong privacy policy and train your staff regarding the importance of safeguarding personal information. It is common for staff to disclose personal information without even being aware that they have done so. As an example, in a case decided by the Privacy Commissioner of Canada, a chartered bank had a complaint filed against it because a representative of the bank at a reception desk had left the desk unattended, with a computer on. A customer had looked at the computer screen and accessed personal information while the desk was unattended. With training this easily could have been avoided.

It is critical for institutions to develop thorough policies containing the ten principles of Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable provincial legislation (for example in Ontario, the Personal Health Information Protection Act) which embody the ten principals. The ten principles are: accountability for the collection of information; identifying the purposes for the collection of information; getting consent to the collection; limiting the collection to only information that is necessary; limiting the use; disclosure and retention of information; ensuring the accuracy of information that is kept; ensuring that there are good safeguards for the information; openness around the collection of information; individual access for people to verify their information is accurate; and allowing individuals the right to challenge compliance.

For institutions, it is important to understand that privacy is not the same as security. Privacy deals with concerns related to an individual's control over their own information. Security, relates to the organizational control over information that it has in its possession.

Security obviously entails making sure that there are adequate technological measures in place, but it also deals with staff training and being aware of the importance of maintaining security and confidentiality. It is important to have a policy, but it is just as important to periodically audit the enforcement and use of that policy by staff members. Also, institutions must continually train, refresh and remind staff as to the importance of privacy threats.

For a chief privacy officer of an organization, after the first step of developing the privacy policy to meet the privacy expectations of your public, the chief privacy officers must ensure that collection and use of information is appropriate. Further, chief privacy officers must periodically do risk assessments. Introducing rules and controls for privacy risk management helps reduce an organization's liability and reduces threats of litigation or privacy audits by the Privacy Commissioner.

Organizations must continue to audit, train and reinforce the importance of privacy through a model of continuous improvement. If there are new technological threats or methods of privacy attacks on organization, the chief privacy officer must be aware of these risks and adapt the privacy policy and training appropriately. Privacy diagnostic tools are critical weapons in ensuring that an organization is up to date.

By taking proactive steps with policy compliance and periodic audits, an organization can greatly reduce their liability risks as well as manage complaints in the new environment of consumer sensitivity to privacy issues.

Graham Porter
Partner, Lerner LLP, London, ON
gporter@lerner.ca