IT IS VERY POSSIBLE TO BREACH PRIVACY WHEN THERE IS NO HUMAN IN THE LOOP

It is very possible to breach privacy without human in the loop, Privacy protection has become a hot topic in recent years, due mainly to the ever-growing pervasiveness of new technologies and to the millions of individuals around the world , who have found themselves victims of privacy breaches as a result. A privacy breach occurs when an individual's personal information is accessed, collected, used or disclosed in contravention of applicable privacy legislation or privacy policy.Personal information usually refers to information that is about an identifiable individual. Some of the more obvious examples of personal information include information pertaining to an individual's home address, nationality or ethnic origin, colour, religion, age or marital status; education, health, employment or criminal history; personal identification numbers, such as those listed on a driver's license or a bank account number; biometric particulars, such as fingerprints or blood type; and sexual preference or political affiliation. vIt is very possible to breach privacy without human in the loop, Privacy protection has become a hot topic in recent years, due mainly to the ever-growing pervasiveness of new technologies and to the millions of individuals around the world , who have found themselves victims of privacy breaches as a result. A privacy breach occurs when an individual's personal information is accessed, collected, used or disclosed in contravention of applicable privacy legislation or privacy policy.Personal information usually refers to information that is about an identifiable individual. Some of the more obvious examples of personal information include information pertaining to an individual's home address, nationality or ethnic origin, colour, religion, age or marital status; education, health, employment or criminal history; personal identification numbers, such as those listed on a driver's license or a bank account number; biometric particulars, such as fingerprints or blood type; and sexual preference or political affiliation. Privacy breach may arise intentionally or inadvertently, but the effect may be equally devastating to its victims. Intentional breaches can consist of theft2 or an abuse or manipulation of the technologies that are so often used to catalogue and protect personal information.3 Hacking, which consists of breaching computer systems and electronic safeguards, is a serious problem, particularly due to the heavy reliance organizations place on computerized databases. Such intentional breaches are often vicious in nature and consist of a deliberate desire to access, collect, use or disclose an individual's personal information with a view of causing a disturbance or perpetrating a crime.

While deliberate, bad faith activities, such as hacking and theft, are serious crimes that cause risks to individuals whose personal information has been exposed, human error or ignorance is often the most likely cause of privacy breaches. Privacy breaches based on human erroracy breach may arise intentionally or inadvertently, but the effect may be equally devastating to its victims. Intentional breaches can consist of theft2 or an abuse or manipulation of the technologies that are so often used to catalogue and protect personal information.3 Hacking, which consists of breaching computer systems and electronic safeguards, is a serious problem, particularly due to the heavy reliance organizations place on computerized databases. Such intentional breaches are often vicious in nature and consist of a

deliberate desire to access, collect, use or disclose an individual's personal information with a view of causing a disturbance or perpetrating a crime.

While deliberate, bad faith activities, such as hacking and theft, are serious crimes that cause risks to individuals whose personal information has been exposed, human error or ignorance is often the most likely cause of privacy breaches. Privacy breaches based on human error **Best Practices to Limit Privacy Breaches**

The best defence is a good offence. To limit privacy breaches, organizations need to be proactive and aggressive, and build their privacy practices on four pillars. First, management needs to understand their organization's obligations under law and applicable standards. Privacy breaches are often defined opposite obligations under the law. As such, one of the easiest ways to avoid privacy breaches is for organizations to have a good practical understanding of their obligations under privacy laws. While this exercise may begin with an understanding of statutory and regulatory obligations, it does not end there. Organizations then need to take a look at their own privacy policies, contracts with third parties and any industry standards to which the organizations are bound or to which they have voluntarily agreed to adhere.

Second, management needs to have a good understanding of their organization's information handling practices. This includes understanding the nature and source of personal information on intake, understanding how the organization uses, stores, transfers and discloses personal information and, of course, how understanding how the organization renders anonymous, deletes or destroys personal information for which it no longer has any reasonable use.21 Wireless and technology-based security protections are key to develop and implement, particularly in today's digital age. Thefts or hacking may be impossible to prevent, given the technological advancements that are made every day. Nevertheless, the use of strong encryption programs, password protection and digital locks will prevent unauthorized access to data that is stored on such electronic systems. Encryption has become the standard for storing personal information and health information on portable devices22 and practising privacy breach prevention can be as simple as deleting a data cache or wiping a hard drive.23

Third, management needs to ensure their organization has a privacy policy (for internal and external distribution) that reflects the organization's personal information handling practices and, of course, compliance with laws and applicable standards.24

Fourth, once a privacy policy is developed, management needs to implement the provisions of such policy. A key element of such implementation involves management ensuring its employees, officers, directors, consultants and third parties with whom such organizations do business, understand and comply with the organization's privacy policies. If employees, officers and directors are not properly educated, both with regard to obligations at law and the organization's particular privacy policies, privacy breaches are virtually impossible to prevent. Once an organization ensures that its own personnel understands their obligations, the organization needs to ensure that each third party to whom such organization has disclosed, transferred or otherwise granted access to personal information is also aware of and complies with the organization's privacy policies. Compliance obligations with third parties should be set out in written contractual terms to establish agreed on standards and avoid misunderstanding. Contractual terms should address security obligations, restrictions on use and disclosure of the personal information, breach notification obligations as well as obligations to assist in investigating allegations of privacy breaches and/or responding to inquiries and claims from individuals and

government officials. To ensure such third party's compliance with its obligations, the contract should include an audit right in favour of the organization relating to the third party's practices.

Destruction and Disposal of Personal Information

Once an organization has done its job and rationalized the personal information that it collects, uses and/or discloses, the organization will still need to ensure the personal information it does collect, use and/or store is returned, destroyed or deleted in an appropriate manner. Adequate destruction and disposal policies are a key element in the breach prevention equation.

Disposal and destruction policies and processes need to account for both physical destruction and technological elements of a file. Paper and hard copy records that contain personal information should be shredded (ideally cross shredded), and their destruction should be systematically monitored and certified, even if it occurs off-site.25 As for electronic files, unnecessary or unused sensitive data should be wiped, rendered unreadable and/or destroyed. This is particularly true if the organization intends to dispose of or donate its old computers, such that the computers could find their way into the hands of a third party.26

Responding to Privacy Breaches

Despite implementation of best practices and preventative measures, privacy breaches do still occur. Often, weaknesses in privacy protection do not come to the attention of an organization until after a breach has occurred. While such a breach may be the result of faulty business practices or operational break-downs, the organization should take key steps to immediately rectify any damage caused. The first 72 hours of the breach are crucial to its containment and to the containment of the potential harm or damages that may be suffered by third parties. If the organization does not act immediately and aggressively seek to contain and rectify the situation, the potential damages to individuals impacted by such breach becomes difficult to manage and the organization's ability to limit its liability as a result is severely compromised. As well, from a pure business perspective, getting out in front of a privacy breach with affected parties allows the organization to ensure it can control the message and limit the damage to its reputation.

The first elements of a privacy breach response are containment and assessment. Containment and assessment of the breach are essential to the mitigation of the organization's potential liability and damages, as well as to the suppression of adverse consequences felt by those individuals targeted by the breach. Containment need not be complicated, but should be immediate. Without immediate containment, the organization is permitting the breach to continue to occur and can widen the liability exposure of the organization.

The organization needs to shut down the unauthorized practice, seek to recover the compromised records, if possible, and make changes to the system that was breached, such as a change to access codes or a system shutdown, so that a subsequent or ongoing breach is inhibited.27 The organization should coordinate an investigation to determine the scope of the breach and how the breach occurred. To do so, the organization should designate a responsible individual, if not a team of individuals, to administer the investigation. This investigation should commence concurrently with the shutdown process. If the breach is found to have resulted from a criminal activity, the organization should notify the police, as they too can play a crucial role in breach containment and the restoration of compromised data. Neglecting to notify police of a privacy breach caused by criminal or potentially criminal activity can compromise the ability of an organization to investigate and mitigate the breach.28

Alongside the investigation, the organization needs to consider and scope the potential damage that may be caused by the breach. This assessment requires a review of which data elements have been compromised, the sensitivity of those elements and the context in which that information might be manipulated or abused. Understanding the risks associated with the breach is a key element in focusing the breach response and in managing the risks to the individuals and the liability of the business.

Breach Notification

After assessing the personal information involved, the cause and extent of the privacy breach, the individuals affected by the breach and any foreseeable harm from the breach, the organization should consider notifying any affected individuals, government regulators and the police. Many jurisdictions have mandatory breach notification requirements and an organization should be familiar with such requirements, as well as any obligations imposed on that organization by industry standards and/or contracts. While breach notification legislation is currently in its infancy in Canada,29 many states within the United States have established breach notification legislative provisions, many of which carry significant costs for failure to notify and for multiple violations.30

Organizations are not often willing to notify individuals affected by a privacy breach. Notification can lead to heightened consumer response, media involvement and loss of goodwill. Organizations will usually want to avoid any negative publicity or public backlash unless they are compelled by law to do so. A choice not to notify is typically premised on the belief that consumers and/or media would not otherwise find out about the breach. In this age of instant communication, premising a business strategy on a belief that word of the breach will not get out is flawed and can be quite costly. Depending on the jurisdiction where the breach occurred and the jurisdiction where damages are suffered, organizations responsible for privacy breaches can risk facing serious lawsuits and substantial monetary penalties.

While breach notification will likely affect heightened inquiries and complaints from individuals and publicity, breach notification, if handled correctly, can be beneficial to an organization. Breach notification can be an important tool in mitigating an organization’s damages and can allow the organization, and not the press or privacy commissioners, to control the message being sent to the public.

Some argue that an organization which notifies individuals impacted by a privacy breach will limit its potential damages as a result of the breach. That belief is based on the premise that notification empowers those affected individuals to take action in mitigating any harm that otherwise would have been suffered by them. In turn, this mitigation of damages mitigates the organization’s liability.

Content of Breach Notification

The content and type of breach notification is not always legislated and may vary, depending on the type of breach and the individuals affected. Notifications may be direct or indirect. Although direct communication is more personal, it addresses the specific personal information at issue for that individual, and as a result is more effective. Unfortunately, direct communication is not always practical. Content of the notification will vary, as appropriate, and may include information about the incident, details on what the organization has done and will do to control or reduce the harm, information on how individuals can protect themselves and contact information, should the individuals have any questions or concerns about the breach.31 Notification content should also be considerate of whether or not a police investigation of the breach is ongoing, as disclosure of some information may not be sensible in certain Circumstance's.