Lang Michener LLP
Lawyers – Patent & Trade Mark Agents

PrivacyBrief

Summer 2008

In This Issue

page

Identity Theft and Technology – How Bill C-27 Responds 1

Security of Electronic Records – Does Current Legislation Adequately Protect? 4

Technology has had an effect on crime – a prime example being identity theft. In "Identity Theft and Technology – How Bill C-27 Responds", Howard Simkevitz looks at Bill C-27, *An Act to Amend the Criminal Code* and examines what the federal government has proposed to combat identity theft in the digital age.

Security and privacy are key prerequisites for successful adoption of a healthcare system based on the single electronic health record. However, comprehensive legislative standards currently do not exist. In "Security of Electronic Records – Does Current Legislation Adequately Protect?", David Young provides an overview of how existing laws respond.

Identity Theft and Technology – How Bill C-27 Responds

Howard Simkevitz

The methodologies of committing crimes in cyberspace are different from their counterparts in real space. The importance of addressing this difference becomes more pronounced in light of society's increasing reliance on information and technology infrastructure. As such, legislators must duly account for the use of technology as an integral piece of sound legislative initiatives. It can no longer be a case of using old laws to adapt to new technology.

Identity theft provides an excellent example of the impact technology has had on crime. Reports of identity theft run rampant in the popular press. However, the *Criminal Code*,[1] as currently written, does not contain a specific identity theft offence. In fact, most of the provisions attempting to address identity theft are fraud provisions that predate the advent of the Internet save for offences dealing with credit and debit cards,[2] and "[u]nauthorized use of computer."[3] This latter section is useful insofar as it can be used to capture fraudulent use of identity information over the Internet. The section reads as follows:

> 342.1 (1) Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
>
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)…[4]

The effectiveness of the Code provisions regarding unauthorized use of a computer and fraudulent use of credit or debit cards is limited. For example, although it is illegal to fraudulently use personal information, there is nothing to address the unauthorized collection, possession or trafficking of such personal information. Seemingly, policy makers have caught on (or have been impelled to catch on) that there is a need to close such legislative gaps. In short, not only is Canada lacking a clear definition of the crime (i.e. identity theft), but law enforcement lacks the ability to intervene until, more often than not, it is too late.

Bill C-27

Bill C-27[5] had its second reading on January 30th of this year and is now in committee. One may assume that the Bill is in a reasonable position to pass through the House of Commons expeditiously for at least two reasons: 1) the Bill has not received any significant opposition in either of its readings thus far; and 2) there seems to be recognition by most members of Parliament that something needs to be done to contend with identity theft.

The general purpose of the Bill is to create three new offences:

1. obtaining or possessing identity information with the intent to use it to commit certain crimes;[6]
2. trafficking in identity information with knowledge of or recklessness as to its intended use in the commission of such crimes;[7] and
3. possessing and trafficking certain government-issued identity documents belonging to another person – expanding the relevant documents from passports to include Social Insurance Numbers, drivers' licenses, birth certificates, and a number of other identity papers.[8]

Furthermore, and importantly, the Bill introduces the concept of restitution for the victim.

The Criminal Code, as currently written, does not contain a specific identity theft offence. In fact, most of the provisions attempting to address identity theft are fraud provisions that predate the advent of the Internet.

What It Does

The Bill's proposed amendments are laudable in three ways. First and foremost, by criminalizing the foregoing, the Bill gives law enforcement the ability to intervene at the stage of possession and trafficking – before fraud has actually been committed.

Second, the Bill is forward thinking and tries to anticipate the use of technology and not shy away from it. For example, the Bill does a good job of capturing the various technical manifestations of identity, including biometrics which will undoubtedly be a significant source of identity theft in future years. The anticipatory nature of the Bill becomes evident when looking at the very definition of "identity information" in the section 402.1 of the Code:

> For the purposes of sections 402.2 and 403, "identity information" means any information – including biological or physiological information – of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, such as a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's licence number or password.[9]

Although more restrictive than the definition of "personal information" in the *Personal Information Protection and Electronic Documents Act*,[10] the list in section 402.1 is non-exhaustive, so it does leave room for other incarnations of identity-information, as technology inevitably evolves.

Third, the Bill appears to recognize the power of market forces in assisting in regulating the prescribed conduct. As

mentioned above, in addition to jail time for fraudulent acts, identity thieves will now be facing the possibility of having to reimburse their victims for costs incurred as a result of the fraud (e.g. the price of rehabilitating one's identity, replacing cards and documents, and correcting one's credit history).[11]

This notion of restitution becomes increasingly relevant in the scenario where the accused is an employee of a company. Although the focus of this article is not one of corporate liability, it is important to note that this concept can be found in the present Code. Criminal intent may become attributable to an organization where: (i) the organization benefits, to some degree, from the offence; and (ii) a senior officer is a party, or where a senior officer has knowledge of the commission of the offence by other members of the organization and fails to take all reasonable steps to prevent or stop the commission of the offence.[12] However, such a finding requires that there is a threshold of reasonableness by which criminal intent can be imputed.

Section 402.2 of the Bill states:

> (1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a **reasonable** inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
>
> (2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing or believing that or being **reckless** as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.[13]

When one talks about identity theft, whether one uses the term identity information or, more broadly, the term personal information, these are distinct privacy-related terms. To date, there are standards for security only – there are no equivalents for privacy.

Issues

Two issues come to the fore: 1) what are the circumstances that would give rise to a "reasonable" inference that the information is intended for fraud; and 2) how is one to determine that a person was "reckless" as to whether such information could be used for fraud. The standard(s) by which one could impute reasonableness and recklessness in the realm of identity theft is/are less than clear.

When one talks about identity theft, whether one uses the term identity information or, more broadly, the term personal information, these are distinct privacy-related terms. To date, there are standards for security only – there are no equivalents for privacy. Thus, without clear standards related to privacy, it may make it difficult for companies to mitigate against risk – to assess what is reasonable and what is reckless.

Until a comprehensive set of standards are developed in this area, it may be helpful to look to the following for guidance: i) industry standards and best practices; ii) Privacy Commissioners, specifically orders they render which include promulgation of standards;[14] iii) relevant legislation[15] (e.g. privacy acts such as *PIPEDA*); and iv) jurisprudence in the area.[16]

The Bill comes at time when there is increased support for the notion that something must be done to combat identity theft. However, the Bill may not represent the panacea, and stakeholders should recognize that there is still a need to develop a comprehensive framework for contending with identity theft.[17] Privacy standards would be an invaluable addition to the mix. Furthermore, public awareness about how individuals and organizations should handle identity information would also go a long way to ensure the Bill succeeds.

1 R.S. C. 1985, c. C-46

2 *Ibid.* s. 342

3 *Ibid.* s. 342.1 (1)

4 *Ibid.* s. 342.1 (1); and see the definition of computer system is found in s. 342.1(2), captures Internet activity as follows: "computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;.

5 Bill C-27, *An Act to amend the Criminal Code (Identity Theft and Related Misconduct)* 2nd Sess., 39th Parl., 2008 [**Bill**].

6 *Ibid.* s. 10.

7 *Ibid.*

8 *Ibid.* s. 1.

9 *Supra* note 6.

10 2000, c. 5. Compare the definition of "Personal information" in *PIPEDA* which includes any information about an identifiable individual as opposed to that of "identity information" in the Bill which must "identify or purport to identify" an individual.

11 *Supra* note 6.

12 See ss. 22.1 and 22.2 of the Code.

13 *Supra* note 6 [emphasis added].

14 See e.g. information Order H0-004 wherein the Commissioner stated: "[t]o the extent that PHI in identifiable form must be removed in electronic form, it must be encrypted" at 18.

15 See *Canada* v. *Saskatchewan Wheat Pool* [1983] 1 S.C.R. 205 wherein the SCC stated that although there was no nominate tort of "statutory breach" it acknowledged that the breach of statute may imply a standard of care.

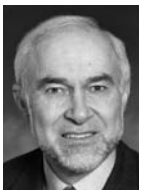
16 Although there is a dearth of case law on point in Canada (part of the reason being, of course, that no tort for breach of privacy currently exists), there may be persuasive extra-jurisdictional cases. See e.g. *Randi A.J. (Anonymous)* v. *Long Island Surgi-Center*, No. 2005-04976 (N.Y. Sup. Ct. App. Div. Sept. 25, 2007), where the court found that no written privacy plan, not following relevant legislation, and insufficient staff training, were, among other factors, sufficient for finding "negligence or recklessness" with regard to the mishandling of personal information.

17 See e.g. the Canadian Bankers Association, *Identity Theft: A Prevention Policy is Needed.*

Howard Simkevitz is an associate in the Corporate & Insurance and Privacy Groups in Toronto. Contact him directly at 416-307-4094 or hsimkevitz@langmichener.ca.

The above article will appear in the forthcoming edition of the Ontario Bar Association's Eye on Privacy: Privacy Law Section Review.

Security of Electronic Records – Does Current Legislation Adequately Protect?



David Young

In seeking to identify the existing legislative framework for security of electronic health records ("EHRs") systems, we have reference to the two basic precepts of *confidentiality* and *privacy*. Within the health sector, these are the key existing rules from which the security obligations emanate. Confidentiality and privacy are often treated interchangeably; however they are different, although overlapping, rules.

Confidentiality is an obligation imposed on health professionals and providers – including institutions – to protect and not to disclose patients' or clients' personal health information except as expressly permitted.

Confidentiality

Confidentiality is an obligation imposed on health professionals and providers – including institutions – to protect and not to disclose patients' or clients' personal health information ("PHI") except as expressly permitted. For doctors, the rule emanates initially from their Hippocratic Oath but is now found in their professional codes of practice as well as in legislation such as the *Medicine Act*.[1] For other professionals such as nurses, physiotherapists and pharmacists, the confidentiality rule is found in their professional codes of practice and in applicable legisla-

tion such as the *Nursing Act, 1991*[2] and the *Regulated Health Professions Act, 1991*.[3] Institutions such as hospitals and social agencies are subject to confidentiality obligations contained in the *Public Hospitals Act*,[4] the *Long-Term Care Act, 1994*,[5] and other similar legislation.

Typical of these confidentiality rules is the prohibition contained in the *Hospital Management Regulations*[6] under the *Public Hospitals Act*,[7] which reads as follows:

> Except as required by law or as provided in this section, no board shall permit any person to remove, inspect or receive information from records of personal health information.

This is a prohibition against unauthorized disclosure of PHI; however, it does not directly address security. Clearly, confidentiality implies security; but security *rules* and *standards* constitute a distinct category: essentially they are the means by which confidentiality is to be achieved. Therefore, while the confidentiality obligation exists for health providers, it contains no explicit directions or rules that address security, or guidance as to the standard of care that can be expected. The obligation does impose potential liability on providers if it is breached however, which creates an incentive for providers to adopt appropriate security measures.

The significance of stipulating the security requirement under the new privacy laws is important: not only does it set a regulatory standard but it also creates a civil standard of care.

Privacy Law

The other key precept from which security criteria emanate is the privacy law. Privacy is distinct from confidentiality because it derives from the *right* of individuals *to control* their personal information, in contrast with the obligation of providers, which is to keep PHI confidential. However, maintaining confidentiality is an aspect of protecting privacy – so the two precepts overlap.

Privacy implies security because one of the principles of a privacy regime – such as is contained in the Canadian Standards Association's *Model Code for the Protection of Personal Information* ("CSA Model Code") – is that an individual has the right to have any of his or her personal information that is held by a data collector protected from unauthorized disclosure. The privacy precept therefore is more specific than the confidentiality precept in that it expressly articulates a security requirement.

This security requirement is set out expressly in the privacy laws, and it is these laws that form the primary mandate to health care providers to establish appropriate security systems with respect to PHI both generally and, potentially, specifically with respect to EHRs and systems. It is worth emphasizing therefore that the primary source of statutory direction for security of PHI constitutes the privacy laws.

The significance of stipulating the security requirement under the privacy laws is important: not only does it set a regulatory standard but it also creates a *civil standard of care*, which means that if practitioners or institutions fail to meet this standard, they may be liable in damages to the individuals whose information has been compromised.

The privacy laws not only articulate a required standard of security but contain, in varying degrees, guidance for data collectors as to the nature of the security systems and procedures that should be adopted. However, the primary security obligation contained in Ontario's *Personal Health Information Protection Act*[8] ("PHIPA") is stated in quite general terms. It requires that a custodian take steps *reasonable in the circumstances* to protect information within its custody or control against theft, loss and unauthorized use or disclosure.[9] The Act contains certain additional specific guidance, addressing protection against unauthorized copying, modification or disposal, secure handling and disposal of records. The Act also provides for regulations prescribing more detailed procedures for records retention procedures, electronic data collection and management and electronic network service providers. To date however, only regulations relating to network service providers have been enacted.[10] There are no regulations

respecting records management or electronic data procedures, although such regulations are clearly contemplated by the legislation. This deficiency is particularly relevant to the adoption of EHR systems.

PHIPA's limited detailed guidance respecting security procedures contrasts with the federal law, the federal *Personal Information Protection and Electronic Documents Act*,[11] which through its adoption of the CSA Model Code provides an outline of the nature of the protections that should be adopted. The PIPEDA rule makes clear that such protections should include physical, organizational and technological measures and provides examples of each of these categories. The PIPEDA rule also stipulates that organizations must ensure that their employees are trained in security procedures. PHIPA's approach also contrasts with the other health privacy laws which follow the particularity stipulated in PIPEDA.

While this specificity of required procedures is not currently found in PHIPA, it is clear that, in order to comply with the legislation, custodians are *expected* to adopt detailed procedures. The only difficulty with this approach is that the law itself does not provide the required guidance. Instead, practitioners and institutions must look to other sources, such as international standards setting bodies, industry associations and other stakeholder organizations.

Computerized databases of personally identifiable information are more vulnerable than paper-based systems because they may be accessed, changed, viewed, copied, used, disclosed, or deleted more easily and by many more people than paper-based records.

Security is Critical

Why is security such a critical element of a privacy regime?

Firstly, the elemental concept of privacy implies an individual's control over and in effect ownership of his or her personal information. Recognition of this concept dictates that if that information is entrusted to another person, that person must take appropriate precautions to prevent that information from being misused, lost or stolen. Furthermore, implicitly, a privacy regime recognizes that if personal information is misused, an individual may suffer injury – whether it be financial, psychological or physical. The security rule seeks to prevent such injury.

Within the health sector, these and other additional reasons underscore why the security rule and effective compliance measures are important. The unauthorized disclosure of an individual's personal health information can have significant injurious impact – whether it be to the individual's dignity and self-esteem, the perception of his or her place in their family and community, or their workplace status. Clearly, this is the most important reason why personal health information must be protected with secure measures.

However, the nature of potential risks goes beyond direct psychological and social impact upon the individual. Identity theft has become a major concern today, and it is a real concern within the health sector. Furthermore, beyond the specific issue of identity theft, there are concerns for protection of the integrity of the health record itself.

In many commercial organizations and to an increasing extent in large health care entities, privacy and security are identified as distinct reporting responsibilities. While it is recognized that they may overlap in many applications – particularly in the health sector – they can have competing priorities and therefore can potentially be in conflict. This circumstance was recognized by the Ontario Information and Privacy Commissioner's recent report on Smart Systems for Health Agency[12] which recommended that in that organization privacy and security responsibilities should be separated and furthermore that distinct policies should be adopted for each responsibility.

Electronic Health Records

While electronic health records ("EHRs") offer significant advantages to effective health care, they pose challenges

to the security of PHI. Locks and pass-keys, though potentially sufficient in a paper-based system, are inadequate in an electronic environment. Further, in a computerized environment the detriment made possible in the event of unauthorized access is magnified. Computerized databases of personally identifiable information are more vulnerable than paper-based systems because they may be accessed, changed, viewed, copied, used, disclosed, or deleted more easily and by many more people than paper-based records. The technological means to secure or render unidentifiable PHI do exist. The challenge is not to invent the technology but rather to ensure that the law has done all that it can to protect the individual's reasonable expectation of privacy and security of PHI.

As an important adjunct to EHRs, electronic health networks and related software and hardware systems are being adopted aggressively both within institutions as well as province-wide networks. Examples can be found in Ontario's Continuing Care e-Health program, SSHA and the many local and regional networks that share health information. We need to look no further than the recent Ottawa Hospital case[13] for an example of how easy it can be to subvert security procedures in an electronic network.

The potential security risks to information collected and managed through these systems are many, but they can be addressed through strong protective technology and rigorous procedures.

Should Canada's laws reflect a pro-active leadership role in establishing basic principles for EHR security, or should we rely on general legal precepts of security to ultimately generate a set of rules, through a more circuitous process?

How Do the Privacy Laws Address Electronic Security?

We see, therefore, that it is under the privacy laws that security of PHI is addressed. As mentioned above, PIPEDA provides substantial guidance in this area; however, it only applies to commercial entities (and the commercial activities of other entities) and therefore has certain limitations in scope when dealing with the health sector. Four provinces have adopted specific health-sector privacy legislative (Ontario,[14] Manitoba,[15] Saskatchewan[16] and Alberta[17]). Furthermore, all of these laws address, with greater or lesser specificity, the security requirement. All of the provincial laws, except Ontario's, mandate health information custodians to address the three categories of safeguards identified in PIPEDA: administrative, physical and technological.

However, only Manitoba has addressed with any specificity electronic security. In that province's Act and regulations, protection respecting unauthorized interception, secure destruction and mobile devices is addressed and user logs and audit trails are required. The rules stipulated are quite general in nature but can be contrasted with the other provincial statutes and PIPEDA which at present contain no rules specifically addressing EHRs and the use of electronic systems by custodians.

In the absence of legislative guidance, the Ontario Information and Privacy Commissioner has articulated certain criteria through her order-making power and through informal guidelines. For example, in Order HO-004[18] the Commissioner has set out certain criteria to address the security of PHI maintained on portable electronic devices. This Order contains a number of recommended administrative procedures; its specific application for portable devices addresses recommended procedures for maintaining and providing access to PHI held on such devices. Essentially, the Order mandates effective encryption of such information and the use of multi-layered access authorization procedures.

The question that may be posed is the following: Should Canada's laws reflect a pro-active leadership role in establishing basic principles for EHR security, or should we rely on

general legal precepts of security to ultimately generate a set of rules, through a more circuitous process? If we believe that privacy laws should be instructive and preventative, not reactive, we would argue that providing guidance for users to avoid pitfalls is preferable to penalizing them for breaches. More, importantly, compliance and breach avoidance protects those who would suffer injury: the individual users of the system.

---

1 S.O. 1991, c. 30.; *Professional Misconduct*, O. Reg. 856/93, s. 1(1)(10).

2 S.O. 1991, c. 32.; *Professional Misconduct*, O. Reg 799/93, s. 1(10).

3 S.O. 1991, c 18, s. 36(1).

4 R.S.O. 1990, c. P.40, s. 14.

5 S.O. 1994, c. 26, s. 3(1)(9).

6 R.R.O. 1990, Reg. 965, s. 22(1).

7 *Supra* note 4.

8 S.O. 2004, c.3, Sch. A., s. 12(1).

9 *Ibid.* s. 12(1).

10 See O. Reg. 329/04, s. 6

11 S.C. 2000, c. 5.

12 Review of the Smart Systems for Health Agency (SSHA): An Electronic Foods and Service Provider to Health Information Custodians under the *Personal Health Information Protection Act, 2004*, March 16, 2007

13 Order H0-002 (Ontario Information and Privacy Commissioner).

14 *Supra* note 8.

15 *Personal Health Information Act*, C.C.S.M. c. P33.5.

16 *Health Information Protection Act*, S.S. 1999, c. H-0.021.

17 *Health Information Act*, R.S.A. 2000, c. H-5.

18 Order H0-004 (Information and Privacy Commissioner/Ontario).

David Young is a partner and Co-chair in the Privacy Group. Contact him directly at 416-307-4118 or dyoung@langmichener.ca.

PrivacyBrief

Editor: David Young
416-307-4118
dyoung@langmichener.ca

RETURN UNDELIVERABLE CANADIAN ADDRESSES TO:

Lang Michener LLP
Brookfield Place
181 Bay Street, Suite 2500
P.O. Box 747
Toronto ON M5J 2T7
Tel.: 416-360-8600 Fax.: 416-365-1719
e-mail: info@langmichener.ca

Lang Michener LLP
Lawyers – Patent & Trade Mark Agents

Toronto
Brookfield Place
181 Bay Street, Suite 2500
P.O. Box 747
Toronto, ON M5J 2T7
Tel.: 416-360-8600 Fax.: 416-365-1719

Vancouver
1500 Royal Centre
1055 West Georgia Street
P.O. Box 11117
Vancouver, BC V6E 4N7
Tel.: 604-689-9111 Fax.: 604-685-7084

Ottawa
Suite 300
50 O'Connor Street
Ottawa, ON K1P 6L2
Tel.: 613-232-7171 Fax.: 613-231-3191