

Identity Theft and Technology – How Bill C-27 Responds

June 5, 2008

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-275 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.

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

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 legislation¹⁵ (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.

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

This article appeared in Privacy Brief Summer 2008. To subscribe to this publication, please visit our Publications Request page.