Legislative Summary LS-637E

BILL S-4: AN ACT TO AMEND THE CRIMINAL CODE (IDENTITY THEFT AND RELATED MISCONDUCT)

Nancy Holmes
Dominique Valiquet
Legal and Legislative Affairs Division

14 April 2009
Revised 5 June 2009

Library of Parliament
Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL S-4

HOUSE OF COMMONS	SENATE
Bill Stage	

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL S-4: AN ACT TO AMEND THE CRIMINAL CODE (IDENTITY THEFT AND RELATED MISCONDUCT)*

INTRODUCTION

Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct) was introduced in the Senate on 31 March 2009. The bill will create several new *Criminal Code* offences specifically targeting those aspects of identity theft that are not already covered by existing provisions. Essentially, Bill S-4 will focus on the preparatory stages of identity theft by making it an offence to obtain, possess, transfer or sell the identity documents of another person. The bill contains essentially the same provisions as former Bill C-27,(1) with the addition of new offences that can lead to electronic surveillance.

On 4 June 2009, the Standing Senate Committee on Legal and Constitutional Affairs made four fundamental changes to Bill S-4:

BACKGROUND

Identity theft has been called the crime of the 21st century. With the proliferation of personal and financial information as a result of such electronic media as the Internet and associated technology, new life has been given to an old crime. Not so long ago, assuming and using another person's identity was a relatively small-scale operation that required time and effort to execute (e.g., stealing a purse, breaking into a house, overhearing a private conversation). Today, however, perpetrators of identity theft can operate at a distance from their victims, access databases containing large amounts of personal information and transmit stolen data quickly and easily around the world.

The nature and scope of identity theft have made it not only difficult to define the term, but also to measure the extent of the problem. With respect to a definition of "identity theft," some commentators refer to identity fraud in relation to the fraudulent use of personal information, and identity theft as pertaining to the unauthorized collection of the

Once obtained, personal information can be used to open bank accounts, obtain loans or credit cards, gain employment or transfer land title in the victim's name. Stolen or reproduced personal documents can also be used to obtain government benefits or government-issued documentation. There also appears to be a growing trend of using identity theft to facilitate organized crime and terrorism activities (e.g., to mislead or avoid detection by law enforcement officials).

Victims of identity theft may suffer significant financial loss as well as damaged reputation or credit ratings. There may also be losses suffered in terms of the time, expense and emotional stress associated with restoring reputations and recovering financial and other losses incurred. Governments and businesses may also suffer financial loss and damaged reputations, and to the extent that identity theft is used to support terrorist activities, there may be national security implications.

Given that it can take months or even years for identity theft to be detected, coupled with the fact that most cases go unreported, statistics in this area are fairly unreliable. PhoneBusters, a national anti-fraud call centre jointly operated by the Ontario Provincial Police, the Royal Canadian Mounted Police and the Competition Bureau Canada, is the principal source of data on identity theft in this country; however, its statistics are complaints-based and as such may represent only part of the problem. According to PhoneBusters, for the calendar year ending December 2008, a total of more than $9 million in losses was reported on the basis of over 11,000 complaints.[6]0.585 0 Td(cad(this arN5redl8(22.0012 Tc 0.045)ts.)]Ttts.)eV.04 Tm(()TjEMC /

Calls for amendments to the

DESCRIPTION AND ANALYSIS

A. General Offences

1. Illegally Possessing or Trafficking in Government Documents (Clause 1)

The bill's first clause creates a new hybrid offence

Clause 7 protects from prosecuti

The bill defines identity information as "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" (clause 10).

This definition differs from the definition of "personal information" in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[19] The PIPEDA definition states that "personal information" means "information about an identifiable individual." This definition may thus include information that does not permit identification of an individual, but rather information about an identifiable individual (for instance, his or her shopping preferences).[20] The definition of "identity information" in the bill is more restrictive, because such information must "identify or

Some information, such as a Social Insurance Number, fingerprint or DNA profile, is unique, in that it is sufficient in itself to identify an individual.

b. Indictable Offences Including Fraud, Deceit or Falsehood

Second, to obtain a conviction for identity theft the prosecution would also have to prove that the accused had obtained or possessed another person's identity information *in circumstances giving rise to a reasonable inference that the information was intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence*. Under the new subsection 402.2(3) of the Code, this would include the following indictable offences:

- forgery of a passport or uttering a forged passport
- fraudulent use of a certificate of citizenship
- personating a peace officer
- perjury
- theft, forgery, etc., of a credit card
- false pretence or false statement
- forgery
- uttering, trafficking in or possession with intent of forged documents
- fraud
- identity fraud.

4. Trafficking in Identity Information (Clause 10)

Clause 10 creates another hybrid offence, trafficking in identity information (new subsection 402.2(2) of the Code). It involves the transmission, making available, distribution, selling or offering for sale, or posseck5bri/TTp/TTm5(4886 T4 0 Tdy050her hybrid offence,)Tj-0

This new offence, like identity theft, is punishable by a term of imprisonment not exceeding five years (new subsection 402.2(5) of the Code).

5. Identity Fraud (Clause 10)

The bill replaces the current offence of "personation with intent"[(21)] (i.e., pretending to be another person to gain an advantage for oneself or cause a disadvantage to someone else) with "identity fraud" (clause 10 of the bill amending section 403 of the Code).

Clause 10 also adds to the existing offence the fact of pretending to be another person to avoid arrest or prosecution or to obstruct the course of justice (new section 403(1)(*d*) of the Code).

Clause 10 further specifies that the expression "personating a person" includes pretending to be that person or using that person's identity information as if it pertained to the person using it (new paragraph 403(2) of the Code). The definition of "identity information" in the new section 402.1 of the Code applies to the offence of identity fraud as well.

The maximum sentence for identity fraud is the same as that currently provided for personation, 10 years in prison (new section 403(3) of the Code).

B. Specific Offences

1. Personating a Peace Officer (Clause 2)

At present, personating a peace officer is an offence punishable on summary conviction,[(22)] which means that the maximum sentence is a fine of not more than $5,000 or six months' imprisonment or both.[(23)]

Clause 3 makes it a hybrid offence and increases the maximum sentence to five years in prison (new subsection 130(2) of the Code).

---

(21) S. 403 of the Code.

(22) S. 130 of the Code.

(23) S. 787(1) of the Code.

2. Use and Copying of Credit Card Data (Clauses 4 and 5)

Section 342(3) of the Code currently governs the offence of fraudulently possessing, using or trafficking[24] in credit card data. Clause 4 stipulates that such data include **"personal authentication information" in order to take into account any future identification technology. This term includes "a personal identification number or any other password or information that a credit card holder creates or adopts to be used to authenticate his or her identity in relation to the credit card."** The definition of a credit card already includes debit cards.[25]

Section 342.01(1) of the Code currently provides for the offence of making, selling, exporting, importing or possessing an instrument for falsifying or forging *credit cards*. Clause 5 adds a similar offence for instruments used to copy credit card also gain time for pursuing fraudulent activities without the victims' knowledge. Clause 6(1) tackles this problem by creating the offence of