



DEPARTMENT OF JUSTICE

IDENTITY THEFT

**Privacy and Security Conference –
Synergies in an e - Society?
Victoria, British Columbia
February 10th and 11th, 2005**





Identity Theft

- Concept of “identity theft”
- Relationship between identity theft and
 - Theft
 - Fraud
- Possible options for change
- Challenges
- Further questions



What is “Identity Theft”?

Conduct can be divided into two categories:

- Preparatory acts for the future commission of criminal offences.
 - *Example:* Collecting and copying personal identification information that appears on computers or on actual documents.
 - Improper use of personal information (however acquired) as an instrument for the actual commission of other crimes.
 - *Example:* use of false or assumed identity to commit, conceal or avoid liability for crimes such as fraud.
-





Identity Theft Can Differ from “Theft”

Elements of Theft:

- Fraudulently and without colour of right takes or converts “anything”;
- The “anything” can be either tangible or intangible property; and
- The acts are done with one of four alternative intents (most common is intent to deprive)





Case Law Regarding Theft

- Where the “anything” is intangible data, rather than a tangible document:
- *R. v. Stewart*, [1988] 1 S.C.R. 963: Defines “anything” within the meaning of the theft provision. In this context “anything” is restricted in two ways:
 - a) whether tangible or intangible, it must be capable of a proprietary right; and
 - b) the property must be capable of being taken or converted in a manner that results in deprivation to the victim





Identity Theft Can Differ from “Theft”

- *R. v. Stewart*: Reasoning to find that the offence of counselling to commit theft was not made out:
- Confidential personal information is not property.
- Information cannot be “taken”.
- As for “conversion”, if one appropriates confidential information without taking a physical object evidencing it, the owner is not deprived of the use or possession of the information, but only of its confidentiality.
- There is no deprivation – thus there is no conversion.
- Confidentiality cannot be the subject of the theft because it is not “anything”.





Relationship between Identity Theft and Fraud

Elements of Fraud:

Physical Element:

Proof of prohibited act (deceit, falsehood or other fraudulent means); and

Proof of deprivation (or risk of deprivation) caused by prohibited act.

Mental Element:

Proof of subjective knowledge of prohibited act; and

Proof of subjective knowledge that performance of prohibited act could result in deprivation – no need to intend to deprive.





Relationship between Identity Theft and Fraud

- ***R. v. Stewart*: Reasoning to find that the offence of counselling to commit fraud was not committed:**
- Dishonest deprivation is necessary to prove fraud.
- The appropriation of information in this case would not have resulted in a risk of economic loss amounting to deprivation.
- There was no proof that the hotel intended to deal in a commercial way with the information.
- However, based on *R. v. Stewart* courts have convicted people of fraud where the misappropriation of the information resulted in a dishonest deprivation resulting in an economic loss or risk of economic loss.





Options: Interests Protected

Options to be considered to address any limitations in the law depend, in part, upon the interest being protected.

Interests Protected:

If confidential personal information is not “property” *per se* why should it be protected?

Is identity theft the protection of the confidentiality of personal information?

Is identity theft the protection of society from the use of confidential personal information as an instrument of crime?

Notes:

Mr. Justice Lamer in the *Stewart* case noted the difficulty of extending the notion of property to confidential information.

One approach is to avoid characterizing personal information as “property” and criminalize the misuse of the information. An approach of this nature was used to criminalize possession of credit/debit card data (subsection 342(3)) and to criminalize various activities in relation to computers (342.1)).





Options: Preparatory Acts

Option: Criminalize the Preparatory Stages of Collecting Personal Information for Criminal Purposes:

Misappropriation Offence: One option would be to create an offence that criminalizes the misappropriation of personal information for the purpose of committing subsequent criminal offences.

A person who acquired, collected or possessed personal information in circumstances where the Crown could prove beyond a reasonable doubt that the individual intended to use, or to permit another person to use, the personal information to commit a criminal offence (such as fraud, forgery or personation) would be guilty of an offence.





Option: Trafficking

Option: Criminalize Trafficking in Personal Information

An Offence of Trafficking in Misappropriated Personal Information: Persons who are involved in the producing, copying, duplicating, giving, transferring, transporting, sending, delivering, buying or selling of misappropriated personal information, for the purpose of committing a criminal offence (e.g. to forge false documents) could be subject to a trafficking offence.

This offence would be considered a more serious offence than the misappropriation offence and would carry a higher penalty.





Option: Use of Personal Information

Option: Criminalize the *Use* of Personal Information to Commit Crime:

Two options are available:

- Make piecemeal amendments to individual sections of the *Criminal Code* to ensure that the use of misappropriated personal information for economic or other benefits is adequately covered in those sections and that the provisions reflect modern technology; or
- Create a generic identity theft offence.





Challenges

- **Piecemeal Amendments:** could introduce concepts into the property offences that don't fit those offences.
- **Creating a Generic Identity Theft Offence:** could introduce an offence with elements that overlap other offences, which may undermine clarity in the law.

Notes:

Modifying the theft provisions to ensure that misappropriated personal information is included may have the unintended effect of changing legal notions of “property”.

A generic identity theft offence would invariably contain elements that overlap with other offences in the applicable criminal statute. In Canada, for example, a generic identity theft offence would likely overlap with the offence of personation. The identity theft offence could create additional proof requirements for the Crown e.g. that the accused used misappropriated personal information with the intent of committing personation (for example). Personation already has three specified, alternative mental elements. Would the Crown have to prove the mental element of identity theft in addition to one of the mental elements of the personation offence?





Further Questions

- How should “personal information” be defined?
- Should a concept of “misappropriated” personal information be used? If so, how should it be defined?
- Should an offence be created for installing, possessing, selling, distributing etc. real or virtual devices to misappropriate personal information or to commit identity theft?
- Should the new scheme contain a seizure and forfeiture scheme to seize and forfeit real or virtual devices used in commission of the offences?
- How should the mental element for possible offences be structured? Should the focus be on the purpose for which the accused collected, transferred or used the personal information? Alternatively, should knowledge that the personal information was misappropriated be sufficient?

