Breach Notification:
A Sound Business Practice

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

Canadian Institute
Privacy Compliance Seminar
May 11, 2006

IPC

Presentation Outline

- *The Trend to Giving Notice of Breaches*
- *Recent Developments in the U.S.*
- *Differences in Notification Laws*
- *Ontario's Requirement for Breach Notification Under PHIPA*
- *Don't Wait for Legislation: Do It Now*

IPC

The Current Privacy Storm
United States

- To date, **twenty-nine states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – a number of other states have such legislation pending;

- Although the new laws are similar to California's SB1386, ***varying state requirements will likely put pressure on Congress to pass a federal bill.***

IPC

Pending Federal Data-Breach Notification Bills

- **H.R. 3997 - *Financial Data Protection Act*:**

  Notification to consumers if "information is reasonably likely to have been or to be misused in a manner causing substantial harm or inconvenience" to commit identity theft or make fraudulent transactions;
- **H. R. 4127- *Data Accountability and Trust Act*:**

  Notification required if breach "establishes a reasonable basis to conclude that there is a significant risk of identity theft;"
- **S.1789 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if there is "no significant risk" that it has or will result in harm;
- **S.1332 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if "de minimis" risk of harm;
- **S.1408 - *Identity Theft Protection Act*:**

  Notice required if breach creates a "reasonable risk of identity theft", taking into account whether data is in the possession of a third party "likely to commit identity theft;"
- **S.1326 - *Notification of Risk to Personal Data Act:***

  Notification if breach results in "significant risk of identity theft."

* *The above pending bills are designed to pre-empt state laws.*

IPC

Data-Breach Notification

States Differ on When to Sound the Alarm

- A number of state laws also conflict with each other, define breaches differently and prescribe different thresholds for notification triggers;

Four General Areas:

1. Threshold Notification:

Discretion is allowed regarding whether or not to provide notice, on a harms/severity-of-the-breach basis;

2. Delayed Notification:

Law enforcement intervention permitted to delay providing notice;

IPC

Data-Breach Notification

States Differ on When to Sound the Alarm

Four General Areas (cont'd):

3. Consumer Reporting Agency Notification:

Some state legislation requires notification of the timing, distribution and content of individual notices to nationwide consumer reporting agencies;

4. California Model:

Notification is required as soon as the security, confidentiality, or integrity of personal information is breached, unless the data are encrypted.

IPC

Ontario's PHIPA:
Requirement for Breach Notification

Section 12 (2) – Notice of Loss:

A health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.

www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm

IPC

Data-Breach Notification
United Kingdom

- High-profile data security breaches have already affected consumers in the U.K. – yet there is no requirement for companies to warn customers if their personal data has been put at risk;

- Proponents of breach notification argue that consumers would benefit from a notification requirement, but companies are opposed to it because they fear public knowledge of a security breach will damage their reputation ***[they're wrong].***

IPC

ID Analytics National Data Breach Analysis

- Early notification of breached personal information may significantly lower misuse rates, according to ID Analytics' National Data Breach Analysis;
- There was strong evidence that once a privacy breach was made public (notice of breach), the misuse of the stolen data dropped significantly;
- This suggests that breach notification could serve as a deterrent.

IPC

Do It Now

- **Don't Wait for Legislation… *Notify;***
- **Notifying customers of a breach is a sound business practice;**
- **The risk of <u>not</u> notifying is a greater threat to a company's brand and reputation than notifying.**

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

IPC