



Privacy Breaches: It Can Happen To You

(What Not To Do)

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

Gowlings Technology Seminar Series

Toronto, Canada

May 3, 2006



Presentation Outline

- 1. The Incident*
- 2. The Investigation*
- 3. The Order*
- 4. Five Recent Incidents*
- 5. Solutions*
- 6. RFIDs*
- 7. Conclusion*



The Incident



“The Incident”

October 1, 2005

- I was contacted by a newspaper reporter from the Toronto Star who advised me that patient health records were being blown around the streets of downtown Toronto;
- The records were being used as props on the location for a film shoot about the September 11, 2001 terrorist attacks on New York’s World Trade Center;
- The seriousness of such an incident, coupled with the potential devastating impact on patient privacy, prompted the need for immediate action.



“The Incident”

October 1, 2005 (Cont'd)

- I conducted an immediate site visit and personally attended at the film location;
- When I arrived, the medical records had been retrieved, as the reporter indicated might be the case;
- While I found no evidence of patient health records on the streets, I did retrieve a one page memo that, while containing no personal health information, involved some sensitive information;
- I immediately alerted the Executive members of my office and initiated an investigation pursuant to s.58(1) of the *Personal Health Information Protection Act (PHIPA)*.



“The Incident”

October 2, 2005

- The Toronto Star ran a story describing the incident, along with a picture of the film set littered with what would appear to be patient records;

Film shoot uses real medical records

Privacy official has plans to investigate

RAJU MUDHAR

STAR REPORTER

A TV miniseries filming in downtown Toronto may have to answer to Ontario's privacy commissioner after it was discovered that "fake garbage" used in the movie actually consisted of patients' medical records from a Barhurst St. clinic.

The paper littered the sidewalk on Wellington St. W., near York St., yesterday for filming of *The Untold History Project*, a Touchstone Television production about the Sept. 11, 2001, terrorist attacks on the United States that will air on ABC. Toronto is filming in for New York City, and fire trucks, police cruisers and strewn garbage are being used to recreate the scene.

But much of the garbage yesterday was actually medical documents — mostly information about X-rays bearing the address of a Barhurst St. clinic. The material, noticed by someone on the movie set, included information about ultrasounds, chest X-rays and even dismos-



Mounds of medical records strewn along Wellington St. W. yesterday during filming of a TV miniseries on the 9/11 attacks. Below, an ultrasound report picked from the pile.

- A close-up of one patient health record from an X-ray and ultrasound clinic also appeared with the story;
- The patient's name had thankfully been removed from the photograph of the actual health record.



The Investigation



The Investigation:

First Steps

- My office's “**privacy breach protocol**” was immediately implemented:
- **Containment:** Identify the scope of the potential breach and take steps to contain it;
- **Notification:** Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly;
- **Investigation:** Conduct an internal investigation into the matter, linked to the IPC's investigation and with law enforcement if so required;
- **Remediation:** Address the situation on a systemic basis where program or institution-wide procedures warrant review.



Commissioner's Investigation

- The investigation determined that the health records originated with a Toronto X-ray and ultrasound clinic;
- Boxes containing the records were removed, without notice, from a locked storage area by the Toronto Clinic's landlord and placed near the building's common parking area;
- A Toronto Clinic staff member, realizing that the records were not secure, placed them in her vehicle and drove them to a Richmond Hill clinic owned by the same corporation;



Commissioner's Investigation

(Cont'd)

- From there, the boxes were picked up by the Paper Disposal Company that provided shredding services for both clinics;
- Because of a misunderstanding on the part of an employee of the Paper Disposal Company, some of the boxes were marked for recycling, not shredding;
- These boxes were passed on to a recycling company who subsequently sold the records – intact – to a film company for use on its film shoot.



Findings of the Investigation

- The information in the records qualified as personal health information as defined in the *Act*;
- The Paper Disposal Company was an “agent” of the Toronto Clinic as defined in the *Act*;

The Toronto Clinic failed to:

- Take reasonable steps to ensure the security of the personal health information in its custody or control;
- Ensure the security of the personal health information within its custody and control;
- Comply with the requirements of section 17(1) of the *Act* which makes it responsible for ensuring the proper handling of personal health information by its agent, the Paper Disposal Company.



The Order



Impact of the Order

*“This Order will establish the practice to be followed by all health information custodians **and their agents** in Ontario, with respect to the Commissioner’s expectations for the secure disposal of health information records under Ontario’s new Health Information Privacy Law.”*

— Order HO-001, October 2005



Five Recent Incidents



Health Records Sold at B.C. Public Auction

March 4, 2006: *“Thousands of B.C. private health records sold at public auction: Government tapes contain information on conditions such as HIV status, mental illness.”*

— Vancouver Sun

Personal Information among the files included:

- Records showing medical status of individuals such as mental illness, HIV or substance-abuse problems;
- Details of applications for social assistance, and whether or not people are fit to work;
- Social insurance numbers and medical conditions;
- Hundreds of caseworker entries divulging extremely intimate details of people's lives;
- A document containing more than 65,000 names along with social insurance numbers, birthdays and amounts paid to each person for social support and shelter.



Blowing in the Wind

- British Columbia's privacy commissioner is opening an investigation after scores of confidential and highly personal documents were found blowing around the streets of downtown Vancouver in April 10, 2006.
- A home video shot from an apartment balcony showed hundreds of documents blowing around a downtown Vancouver street;
- The papers were found to contain confidential information, including names, addresses, phone numbers, health care numbers and psychological assessments;
- **It is believed that the files came from a Vancouver law office that handles personal injury claims.**



Alberta: Law Firms

- **July 2005**, a privacy investigation conducted by Alberta's Privacy Commissioner, Frank Work, found that two law firms and their corporate clients breached Alberta's *Personal Information Protection Act* (PIPA) in the course of a transaction;
- At issue was the disclosure of employees' personal information – home addresses and social insurance numbers – which were posted onto the publicly accessible SEDAR website;
- Although all parties involved were found to be accountable, the Commissioner was less forgiving of the two law firms, finding that neither had exercised adequate diligence in the handling of the personal information;

Commissioner's recommendations to both law firms:

- In-house privacy training for all lawyers and staff;
- Continuing legal education in the area of privacy;
- Review of processes involving business transactions where personal information is involved;
- Appoint a privacy officer and implement a privacy policy.



Dumpster Divers

Shop violated customers' privacy: Dumped receipts end up in criminals' possession, The Edmonton Journal, April 20, 2006.

- An Edmonton beauty supply shop failed its customers by allowing personal credit and debit information to end up in criminal hands;
- In the summer of 2005, Monarch Beauty Supply threw out more than 2,600 sales receipts with customers' credit and debit card numbers into a *dumpster*;
- The Alberta Information and Privacy Commissioner, Frank Work, has launched an investigation into Monarch's security practices after Edmonton police alerted him of a woman who complained that she discovered a \$500 laptop computer purchase on her credit card bill;
- Further, a confidential informant "well-placed" within the criminal community handed the Edmonton police a bundle of Monarch receipts taken from the dumpster;



Gone With the Wind

- *Police documents found blowing in the Winnipeg wind, CBC News, April 27, 2006;*
- Winnipeg police are investigating how confidential documents were found blowing in the wind outside the city's main police station;
- A pedestrian found crumpled, papers, held together by a crushed paper clip, outside the Public Safety Building in downtown Winnipeg and turned them over to the CBC;
- The documents were found to contain sensitive information from the Winnipeg police crime division;
- The police acknowledged that they were unaware the documents were missing until they were contacted by the CBC;
- Irene Hamilton, Manitoba 's Ombudsman, has called for the City of Winnipeg to launch an investigation into the matter.



Solutions



Secure Destruction: *Need for Industry Standards*

- The facts of these cases demonstrate the critical need for the secure disposal of personal information records;
- Industry standards would clarify that secure disposal means permanently destroying the records by irreversible shredding or pulverizing, thus making them unreadable;
- ***Recycling can never be equated with secure disposal;***
- Reliance on a third party to dispose of records must include a written contractual agreement setting out the obligation for secure destruction and requiring the third party to provide written confirmation once the destruction has occurred.



Responsibility and Obligation

- Every organization, whether in the public or private sector, needs to follow responsible, secure procedures for the destruction of records containing personal information;
- In many cases, it's not just a matter of being responsible, protecting one's reputation, or preventing identity theft – *it's the law*;
- All three of Ontario's privacy laws (FIPPA, MFIPPA, PHIPA) and federal legislation (PIPEDA) covering private sector organizations — require that personal information, including personal health information, be disposed of in a secure manner, whether it is in paper or electronic format.



Match the Destruction Method to the Media

- **Paper:** cross-cut shredding is recommended, not simply continuous (single strip) shredding, which can be reconstructed. Consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place;
- **Electronic and Wireless:** destruction means either physically damaging the item and discarding it. If re-use of electronic media within the organization is preferred, employ wiping utilities provided by various software companies. *However*, wiping may not irreversibly erase every bit of data on a drive;
- **Remember:** Consider not only the “official” files but any duplicate copies of documents made for in-office use (documents should carry “shred after” dates or “do not copy” warnings).



Outsourcing Records Destruction

- If you are engaging an external business to destroy records, be selective;
- Look for a provider accredited by an industrial trade association such as NAID;
- Look for a provider willing to commit to upholding its principles, including undergoing independent audits;
- Look for a provider that will provide a “certificate of destruction;”
- Check references, and insist on a *signed contract* detailing the terms of the relationship.



Service Provider Contract

The contract should:

- Set out the responsibility of the service provider for the secure destruction of the records involved;
- Specify how the destruction will be accomplished, under what conditions, and by whom;
- Require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator;
- Include a provision that would allow you the option of witnessing the destruction, wherever it occurs, and to visit the service provider's facility;



Service Provider Contract (Cont'd)

- State that employees must be trained in and understand the importance of secure destruction of personal information;
- Require that if any of the work is subcontracted to a third party, the service provider must notify you ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to you;
- Specify a time within which records collected from you will be destroyed, and require secure storage pending such destruction;

— IPC, *Secure Destruction of Personal Information Fact Sheet*,

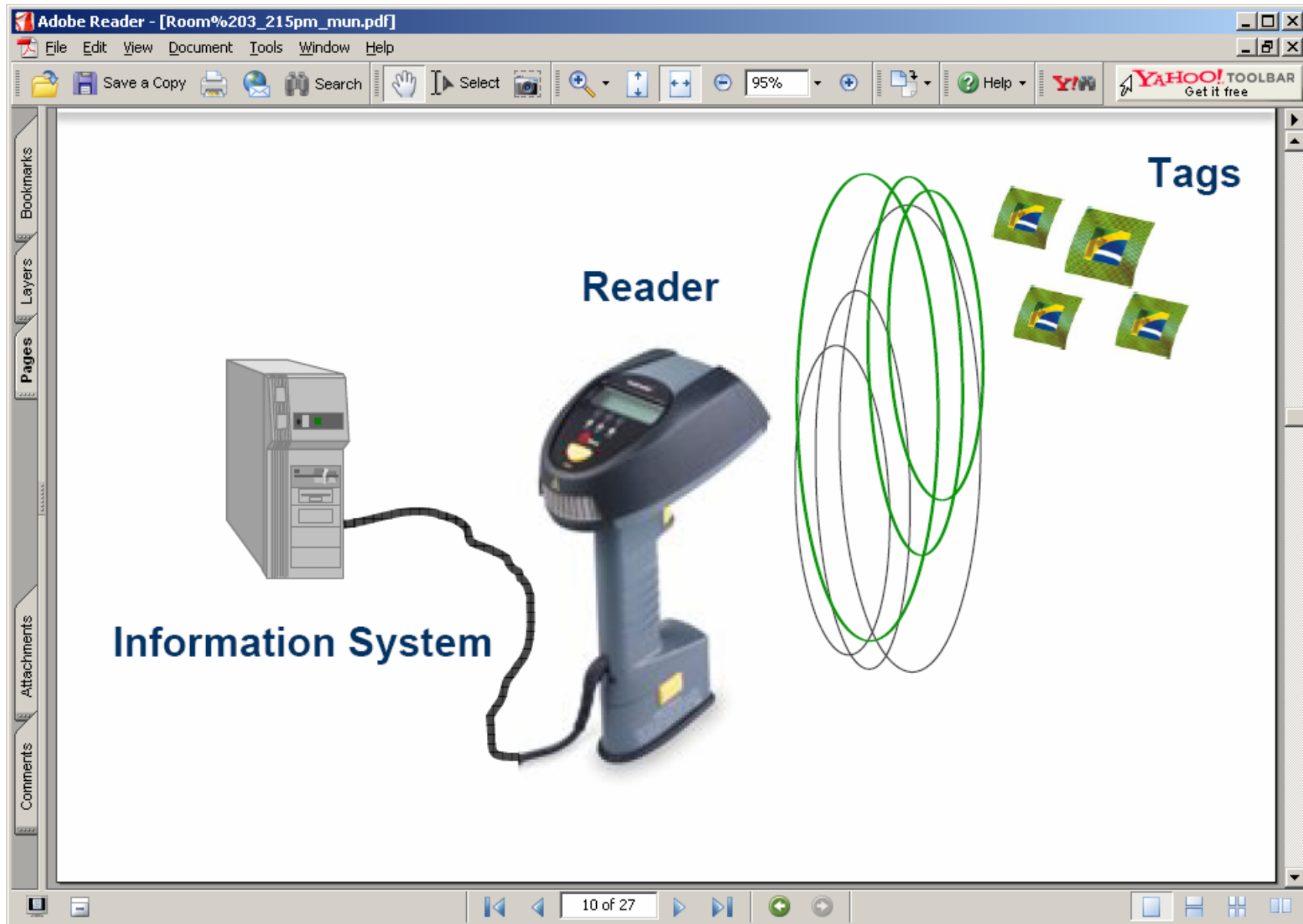
www.ipc.on.ca/userfiles/page_attachments/fact-10-e.pdf



RFIDs



RFID: What Is It?





Properties of RFID Systems

- RFID systems are *information* systems;
- RFID tags contain *globally unique* data;
- RFID tag data can be collected automatically and remotely – and without knowledge, consent or involvement of people;
- *Time* and *location* data can also be collected.



Benefits of RFIDs

The promise of RFID technology:

- More efficient management and tracking of goods and inventory through the supply chain process;
- Reduced labour costs (e.g., no manual scanning of individual items is required);
- Better post-sale service for consumers, warranty servicing, etc.



Broader Future Deployment Trends

0-5 years

- **Supply Chain Management;**
- **Retail, back-end;**
- **Warehouse management and automation;**
- **Asset Management.**

5-10 years

- **Track and Trace to item level;**
 - **Airline Luggage;**
 - **Pharmaceuticals;**
 - **Library Inventory;**
 - **Animals;**
- **Retail, smart shelves;**



Potential for Surveillance

Item-level RFIDs may facilitate tracking:

- The ability to track consumers who have purchased a product;
- The establishment of a widespread surveillance infrastructure;
- The linkage of product information and personal information without consent.

Consumer Backlash:

- How real are consumer concerns?
- Could privacy issues potentially deter the roll-out of RFIDs?



How to Respond?

Follow Privacy Principles

- **Give notice**
- **Obtain consent**
- **Be open and transparent**
- **User control**
- **Use limitation**



Retail Privacy Solution:

De-activation plus Re-activation

- RFID tags should be de-activated (“killed”) at the point of sale;
- While de-activation at point of sale should be the default, it is not without its problems because it limits the post-sale benefits of RFIDs;
- Re-activation, at the behest of the consumer, is key: *consumer choice and control must form the basis of any item-level RFID rollout.*



Conclusion

- Build “end-to-end” information management practices – from collection to secure destruction: Privacy and security are both essential;
- When faced with a breach, lead with openness and transparency: Contain the damage and notify affected parties;
- Apply existing privacy principles to new technology developments: *RFIDs are a case in point*;
- Privacy enhances consumer confidence and trust;
- Think strategically about privacy: *it makes good business sense.*



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

Web: www.ipc.on.ca

E-mail: commissioner@ipc.on.ca