Hacking the Privacy Legislation
Agenda

- Privacy versus Security
- “Un”enforced Privacy
- Privacy Requirements that Work
  - People
  - Process
  - Technology
Privacy versus Security
Types of Privacy

- Territorial Privacy
  - Setting boundaries on intrusion into an explicit space or location

- Physical Privacy
  - Defining intimate acts, behaviour or body parts

- Informational Privacy
  - Legislatively defined
“Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others” (Westin 1967)

Any information concerning the personal or material circumstances of an identified or identifiable person

"personal information" (PI) means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization
In computers, security refers to ensuring the:

- Confidentiality
- Integrity
- Availability

of the data and systems that process data.

This definition transforms security from a value into a technical objective.
Without technology, privacy is a part of physical reality

- I walked down the street, if no one else was there, I could assume I was unobserved
- Video-surveillance cameras = a hidden camera can observe me even when I think I'm alone
- Technology evolves, digital cameras = cheap and compact to store the video forever, machines can read it without human intervention
Her blind date seemed nice enough, but he could be anybody... A huge Star Trek fan, a porn webmaster, or even, God help her, a right-wing blogger!

The man she forgot to google! Don't let it happen to you!
Technology Risks to Privacy

- Technology amplifies the possibility of surveillance
- Technology enables the misuse of personal information
I think of privacy as the use of the data by somebody you gave it to, and security as the theft of the data or the interception of the data by the unknown third party. If I buy a ticket from Travelocity, what Travelocity does with my data is a privacy issue. If somebody hacks into Travelocity and steals that data, that’s a security issue. (Cate, 2008)
Privacy and security are on a collision course. Your desire to be kept safe will soon collide with your wish to be left alone.
Oh, don't worry Mrs Davidson. It is only a small micro-chip implant behind the ear. No one with a clear conscience need have any concern.
Smile!
You’re on CCTV
Making Brighton & Hove a safer city
Please remove any remaining civil liberties and place them in the tray, sir.
Security techniques can help protect personal information

Security techniques can affect the privacy of a data subject
A Case Study: Super Bowl XXXV

- Goal: increase the apprehension rate for known criminals

- Super Bowl XXXV
  - Face recognition software was used to scan all people entering the stadium, looking for known criminals, and possible matches were sent to a police control room

- Privacy objections: it was done without the knowledge or consent of the people being scanned

- Security impact: the existence of such knowledge or consent would have changed the security function of the system from detection to deterrence
Information Security Models

- Bell LaPadula
- Lattice Model of Information Flow
- Biba Model
- Clark Wilson Model
- Chinese Wall Model
- RBAC Model
- Task Based Authorization Model
- Object-Oriented Security Model
Information Security Criteria


- Focus on protecting the system and the organization, not the users and the data subjects
## Privacy Evaluation of Security

<table>
<thead>
<tr>
<th></th>
<th>BLM</th>
<th>LM</th>
<th>BM</th>
<th>Clark</th>
<th>Chinese</th>
<th>RBAC</th>
<th>WAM</th>
<th>DOOM</th>
<th>MOON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of confidentiality of personal data</td>
<td>(yes)</td>
<td>(yes)</td>
<td>No</td>
<td>Yes</td>
<td>(yes)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>(yes)</td>
</tr>
<tr>
<td>Protection of integrity of personal data</td>
<td>No</td>
<td>No</td>
<td>(yes)</td>
<td>Yes</td>
<td>(yes)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Necessity of personal data processing</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>(yes)</td>
<td>No</td>
<td>(yes)</td>
<td>Yes</td>
<td>(yes)</td>
<td>No</td>
</tr>
<tr>
<td>Purpose binding of access to data</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Ability to provide pseudonymity or anonymity</td>
<td>(yes)</td>
<td>Yes</td>
<td>(yes)</td>
<td>(yes)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td>Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect confidentiality, integrity and availability of PI</td>
<td>Protect PI from unauthorized collection, use and disclosure (including theft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect PI from accidental disclosure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect PI from unlawful destruction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect PI from alteration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure availability of PI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect data subjects as system users</td>
<td>Enable anonymization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable pseudonymization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support informational self-determination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Assessment Participants

<table>
<thead>
<tr>
<th>Security Assessments</th>
<th>Privacy Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Specialist</td>
<td>Privacy Specialist</td>
</tr>
<tr>
<td>Business Program Management</td>
<td>Business Program Management</td>
</tr>
<tr>
<td>Application Developer</td>
<td>Application Developer</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>Service Providers</td>
<td>Service Providers</td>
</tr>
<tr>
<td>Auditors</td>
<td>Auditors</td>
</tr>
<tr>
<td></td>
<td><strong>Records Manager</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Legal Counsel</strong></td>
</tr>
</tbody>
</table>
"Un"enforced Privacy
Private Sector Privacy Legislation

- Private sector companies are legislated by the *Personal Information Protection and Electronic Documents Act* (PIPEDA)

- PIPEDA is regulated by the Office of the Privacy Commissioner of Canada (OPC)
  - Complaint-based
  - Right of audit
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- **Complaint-based enforcement rate: 2%**
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Complaint-based enforcement rate: 3%
Consent

- The knowledge and consent of the individual are required for the use, or disclosure of personal information, except where inappropriate.

- Complaint-based enforcement rate: 41%
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

- **Complaint-based enforcement rate: 9%**
Limiting Use, Disclosure and Retention

- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

- Complaint-based enforcement rate: 10%
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- Complaint-based enforcement rate: 2%
Safeguards

- Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

- Complaint-based enforcement rate: 11%
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Complaint-based enforcement rate: 3%
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Complaint-based enforcement rate: 19%
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Complaint-based enforcement rate: 0%
Privacy Requirements that Work
Privacy legislation plays an important role in designing, implementing, and using privacy-enhancing systems (Fisher-Hubner 2001)
Privacy Design Requirements

- Privacy design requirements are:
  - A group of documented needs that enable a system (people, process and technology) to protect the informational privacy of the data subject

- Used as a basis for:
  - Building privacy compliance from the concept phase
  - Limiting resource costs associated with retrofitting for compliance purposes
  - Enhancing the privacy risk posture of an organization
Top Three Areas to Work On

- Consent
- Individual Access
- Safeguards
Privacy Design Requirements

Consent
Consent - People

- Train all staff on how to collect consent properly
Develop consent management program:
- Voluntary nature of consent
- Ability to withdraw / alter
- Allow restriction and / or limitation on disclosure

Document any authority / rationale for secondary use
Track and implement consent preferences at the data element level
  - Display consent statements prior to collection
  - Record terms of consent and timestamp

Issue new consent when notice of collection changes

Allow revocation of consent preferences (any/all)
  - Record terms of revocation and timestamps

Serve explanatory notices of the ramifications of consent revocation

Complete purging of PI as requested
Privacy Design Requirements

Individual Access
Train any staff with direct data subject contact procedures for managing requests for access
Individual Access - Process

- Glossary of terms for all data fields

- Policies and procedures should be in place to support requests for access
  - Different formats for release of data
  - Requests for review / correction
  - Validation of the data subject
  - Written communication with the data subject on outcome / recourse
Provide PI at the least possible cost to the data subject
  • Enable data subject direct access to their PI

Amend or annotate any PI subject to disagreement regarding accuracy (including logs)

Notifications to any parties who received incorrect PI within the last year

Enable access to PI in multiple formats

Support multiple format queries for PI (e.g. one query should return all PI held about a given data subject across different application where necessary for service delivery)

Segregate PI in records by data subjects
Privacy Design Requirements

Safeguards
All staff should be provided with privacy and security training
Safeguards - Process

- Document policies and procedures to safeguard the confidentiality, integrity and availability of PI
  - Avoid archiving of hard copy PI
  - Conducting Threat Risk Assessments

- Document policies and procedures on incident management reporting and investigation, including notification of data subjects (where necessary and/or appropriate)

- Implement procedures to revoke access privileges (including tokens) from staff where necessary (e.g. termination, transfer, promotion)

- Contracts with third parties should specify privacy and security requirements and expectations, and include audit processes

- Physical security measures should be in place to protect electronic and hard-copy PI (e.g. locked doors and server rooms)

- Disaster recovery and business continuity plans should be in place for all mission critical business processes
Support the immediate revocation of access privileges to PI

Have controls in place over the process to grant authorization to add, change or delete information from records

Be designed so that access and changes to PI can be audited by date and by user identification

Labelled, transmit and store PI in accordance with information classification requirements