

Privacy issues

AFCEA Canada IT Security Course

10h10

Nov 17, 2003

The problem...

- We have only 55 minutes, including Q&A
- Focus on public sector? Private sector?
- On technology? Operations? Policy?
- Rip through 100 slides without a breath?

No....

The approach

- Survey a range of privacy issues to introduce the subject
- Give you something to think about.
- Plant seeds of a “privacy frame of mind”....
- The chosen range:

PIPEDA & The Privacy Commissioner

Caveat

- I'm not a lawyer, I'm a security consultant with a strong management background....
 - As a consultant, audited Secure Channel PIA
 - Group Manager, Entrust.net
 - Privacy of transactions, consumer information
 - Directory specialist, Entrust
 - Privacy issues in naming directory entries
- Back to the show....

PIPEDA

- The Personal Information Protection and Electronic Documents Act (aka Bill C-6)
- In force as of Jan 1, 2001 (stage 1 of 3)
 - Non-health related personal information
 - Federal works, undertakings, businesses
 - Banks, broadcasters, inter-prov transport, telcos
 - Disclosures across provincial/national borders
 - Entire commercial sector of the 3 territories

PIPEDA

- Stage 2: Jan 1, 2002
 - Includes personal health information for organizations and activities covered in Stage 1.
- Stage 3: Jan 1, 2004
 - Provincially regulated private sector, unless substantially similar provincial legislation exists
 - Provincial legislation applies to intra-provincial use or disclosure, federal law applies to inter-provincial and international use or disclosure.

The Privacy Commissioner

- Investigates complaints from individuals who believe their rights under the *Privacy Act* have been violated. Can initiate an investigation where there are reasonable grounds to believe the *Act* has been violated.
- Can subpoena witnesses and compel testimony and enter premises to obtain documents and conduct interviews. Has a mandate to conduct periodic audits of federal institutions to determine their compliance with the *Privacy Act* and can recommend changes.
- “The powers of investigation granted to my Office under *[PIPEDA]* mirror those contained in the *Privacy Act*, although I have a greatly expanded mandate to conduct research into privacy issues, and to promote awareness and understanding of these issues among Canadians.”
- See <http://www.privcom.gc.ca>, especially 2000-2001 Annual Report, http://www.privcom.gc.ca/information/ar/02_04_09_e.asp, & 2001-2002 report, http://www.privcom.gc.ca/information/ar/02_04_11_02_e.asp

The Commissioner on PIPEDA

“Apart from some very limited exceptions, no private sector organization can collect, use or disclose personal information about you without your consent.

“It can collect, use or disclose that information only for the purpose for which you gave consent.

“Even with consent, it can only collect information that a reasonable person would consider appropriate under the circumstances.

“People have the right to see the personal information that is held about them, and to correct any inaccuracies.

“There is oversight, through me and my office, to ensure that the law is respected. And there is redress if people's rights are violated.”

Investigation of complaints

- Commissioner investigated 27 of 95 complaints from Jan 1/2001 to Nov 30/2001
- Complaints can be:
 - Well-founded: within jurisdiction, covered by PIPEDA, not subject to other law/regs
 - Not well-founded
 - Can be partially well-founded
 - Or “Discontinued” or “No jurisdiction”

Complaints under consideration

- Some well-founded, clear, and instructive
- Some not well-founded, sometimes for reasons of precedent/tradition/past practice*
- Some illustrate how poor service and staff training bring well-founded complaints

* My interpretation

Some well-founded complaints...

- IP/NetBios address collection by broadcaster
- SIN collection by telecommunications co.
- Video surveillance by commercial org.
- Bank complaints
 - Lost safety deposit records
 - Non-deletion of personal information
 - Inadequate authentication/authorization to IVRS

IP/Netbios address collection

- User complained that broadcaster was attempting to access NetBios info on user's machine; firewall blocked access.
- Broadcaster determined admin had not disabled feature in Microsoft server; subsequently disabled this feature.
- Commissioner ruled broadcaster had not met obligations to obtain consent; satisfied problem inadvertent and resolved.
- Commissioner ruled that NetBios data was PIPEDA personal info, since a 3rd party might be able to use it to obtain other information traceable to an individual (cited passwords, other personal data).
- Technical aspects unclear in Commissioner's report

SIN collection by telecom co.

- New customer told: No SIN, no connection
- Commissioner determined
 - Company policy said SIN was optional
 - But customer had received impression that SIN was condition of service: company was not in compliance with its policy or PIPEDA
- Cited his Office's position that SIN is for specific federal programs only.

Commercial video surveillance

- Security co. had cameras on its roof with live views of a main intersection
 - Had reported incidents to police
 - Purpose of cameras was marketing demo
- Commissioner ruled that monitoring of public spaces can be reasonable but must be done by lawful public authorities, with all appropriate privacy safeguards in place, where there is demonstrable need.
- Commissioner advised company that its intended public video surveillance for commercial purposes is unlawful and should not be pursued.

Bank complaints #1 & #2

- Bank lost safety deposit box records in a move, executor unable to determine whether estate's lawyer had accessed box.
 - Normally kept signature cards for 7 years, but bank policy did not require one branch to maintain another's data
- Bank refused to delete personal info after rejecting credit card application
 - Local manager had insufficient access
 - Certain others did, but specific request was required; not forwarded
 - Bank employees did not understand bank's privacy practices
 - Manual deletion contravened PIPEDA
 - Almost a “poor service” case (see later slides)

Bank complaint #3

- IVRS allowed access to credit card data with 16 digit card # and either year of birth or last 4 digits of phone number.
- Commissioner determined safeguards were inadequate.
- Bank proposed 3 phase plan to rectify situation:
 - Phase 1: All automated access disabled, customers can access data through agent by reference to preselected password.
 - Phase 2: Customers can disable their automated access, and deal with an agent, at their discretion. Included communication plan.
 - Phase 3: Implement improved scheme within three years and report to Commissioner on progress by July 31, 2002.
- Commissioner and complainant found this acceptable.

...and a few not well-founded.

- Musician, sole performer at establishment, complained professional organization could determine his salary from entertainment budget, required by organization to determine copyright fees. Commissioner determined practice was reasonable, organization had legal authority, no personal information being collected, since only entertainment budget is provided, not names of performers.
- Teller wrote account number on back of 3rd party cheque. Commissioner determined that when presenting cheque, customer is giving implied consent to disclosure of info on back of cheque, and that practice is reasonable.

Hmm, next case doubly interesting....

One partially well-founded

- Telecommunications co. employee complained that bank account and transit numbers on direct-deposit statement were improper use of her personal information, and that stubs were left “lying around”.
- Commissioner determined that employees who provide their bank account and bank transit numbers for direct-deposit could reasonably expect numbers to appear on statements for the purpose of verifying allocation of funds.
- Commissioner determined that insufficient safeguards were in place to protect this sensitive information during distribution to employees.

“Poor service”^{*} complaints

^{*}My term

- Bank stalled, involved lawyer when couple requested information on two debt products
 - Couple requested information using otherwise identical letters with different subjects;
 - Bank employee did not notice difference, assumed letters were identical, provided information on one product only.
 - Couple got information, once Commissioner investigated.

Other “service” investigations

- Phone company wanted 2 pieces of ID from new customer; CRTC permits credit check
 - Did not specify why information was needed
 - Company agreed to clarify its procedures
- Railway collected DoB, citizenship of customers going to US, sent to USC/USNIS
 - Local copies destroyed after trip
 - Staff must state collection is voluntary, intended to speed passage through customs.

One case from 2002

- Clock on the bank's computerized record of transactions 12 minutes slower than clock on video camera. Wrong person's image released to police, Crime Stoppers.
- “Being well aware that the police would likely use your personal information to make a decision about your status as a suspect, the [bank] should have taken due care to ensure that the information was accurate so as to minimize the possibility of a wrong decision with adverse consequences for you.”
- “Once privacy is violated, once an individual's personal information has been taken out of his or her control, it cannot be undone. Lost privacy cannot be given back.”

Privacy and Security

- For some reasons, privacy advocates sometimes don't trust us security types
 - Are we too technophilic? “Oh, encryption solves that....”
- In the end, privacy considerations should simply be part of our security policies, planning, implementation, and operations
 - Get the “privacy mindset”
 - Balance it with other business considerations

Conclusions

- Well, it's a complex area.... 😊/😞
- Consider “stewardship”
 - Customers own their info, keep it safe for them.
- Precedence/history play important roles
 - Would past practice pass muster today?
- New technologies being scrutinized
 - The easier it is to do, the harder it needs to be thought about. Things are getting way easier....

Q&A

Peter Whittaker
pww@EdgeKeep.com

Slide 24 of 24