Privacy Protection and the CHI Community

Andrew Patrick
NRC Canada & Carleton University

see http://www.andrewpatrick.ca
Global trend for worsening privacy protection
(Privacy International 2007)
Recent Canadian issues

e.g., can’t collect fingerprints from students writing LSAT tests because no justification

e.g., can’t swipe driver’s licenses when entering night clubs because no justification
Privacy matters
You do have something to hide, and you should

• “I don’t do anything wrong so I don’t have anything to hide”
  • but who decides what is wrong, and what if the definition changes?
  • privacy is a basic human need (watch children growing up) and a fundamental right
Privacy and power

- Those who have privacy, have power over those who do not (e.g., police asking for your ID, versus you asking for theirs)
- power of surveillance and amateur journalism
Security versus privacy

- most privacy-invasive security measures do little to protect security, and might make things worse (ID cards, eavesdropping, data mining): Schneier
- it is a false dichotomy created for political purposes: there is no security without privacy (let alone dignity)
Situation in Canada
Statutory rules at various levels (but weak powers)

http://www.privcom.gc.ca/
But, video surveillance increasing without justification

Recent case in Toronto where video surveillance of public transit was approved by privacy commissioner even though there was little evidence of effectiveness.
But, no-fly list tied to USA
But, biometric ID being considered

mostly because of pressure from the USA
Role of HCI professionals
• do projects related to privacy issues and solutions
  • “privacy” not found in paper titles, 2 found in posters, some coverage in workshops
  • some good work being done on privacy-sensitive ubiquitous computing (e.g., Lederer, Briggs)
• get involved with privacy-protecting technologies (e.g., Tor)
• develop courses on usable privacy and security (e.g., Cranor, Hong, Reiter: http://cups.cs.cmu.edu/course-guide/)
• become the advocate for privacy protection, if your organization doesn’t have one
• use your knowledge of empirical methods to demand solutions that are actually effective (e.g., surveillance cameras do little to deter crime or aid in investigation – London underground bombings)
• designing for privacy in new applications (e.g., collaboration, personalization). See Cranor (2004), Table 2 or Patrick & Kenny (2003)
• become familiar with fair information practices and privacy-protection design principles
Many services operated at international level (e.g., Facebook)
e.g., International standards on privacy, and privacy-related technologies. I am involved in standards efforts relation to personal and social impacts of biometric identification systems
Privacy by design, in everything we do