NRC · CNRC

From Discovery to Innovation...

Building Usable Privacy Protection

Andrew S. Patrick

National Research Council of Canada

www.andrewpatrick.ca

FTC Workshop, Washington, May 14, 2003

User's Concerns About the Net

- 2002 study from U Washington [Friedman et al., CHI2002 Conference]
- 72 detailed interviews with consumers from rural, suburban, high-tech communities

- 93% concerned about risks or harms
  - most felt strongly that something should be done about it
- areas of concern:
  - 75% -- information security: security & privacy
  - 42% -- users: experiences, children
  - 38% -- systems: threats to computer
- little concern about trust, online identities, online interactions, information quality, content

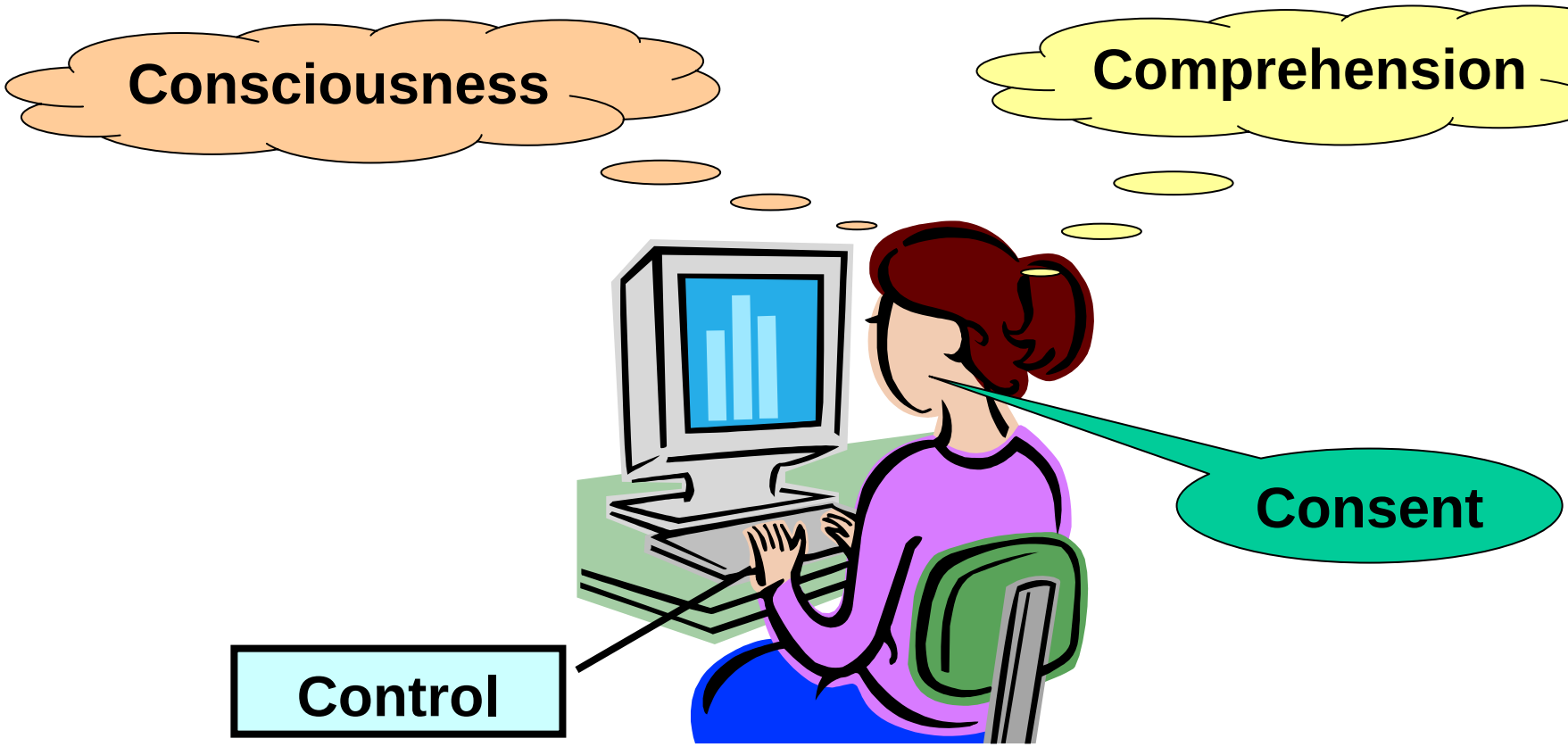
Usable Privacy

- an "engineering psychology" approach: use knowledge of cognitive processes to inform system design
- context is European and Canadian approaches to privacy protection, with emphasis on generalizability
- work with privacy principles and EU Privacy Directive
  - goal is to support "usable compliance" with privacy requirements
- translate legislative causes into human factors implications and design specifications

Ten Privacy Principles

Principle	Description
Reporting the processing	All non-exempt processing must be reported in advance to the National Data Protection Authority.
Transparent processing	The Data Subject must be able to see who is processing his personal data and for what purpose. The Controller must keep track of all processing performed by it and the data Processors and make it available to the user.
Finality & Purpose Limitation	Personal data may only be collected for specific, explicit, legitimate purposes and not further processed in a way that is incompatible with those purposes.
Lawful basis for data processing	Personal data processing must be based on what is legally specified for the type of data involved, which varies depending on the type of personal data.
Data quality	Personal data must be as correct and as accurate as possible. The Controller must allow the citizen to examine and modify all data attributable to that person.
Rights	The Data Subject has the right to acknowledge and to improve their data as well as the right to raise certain objections.
Data traffic outside EU	Exchange of personal data to a country outside the EU is permitted only if that country offers adequate protection. If personal data is distributed outside the EU then the Controller ensures appropriate measures in that locality.
Processor processing	If data processing is outsourced from Controller to Processor, controllability must be arranged.
Security	Protection against loss and unlawful processing

Human Factors Requirements



Comprehension

Requirements	Possible Solutions
• comprehend how PII is handled • know who is processing PII and for what purposes • understand the limits of processing transparency • understand the limitations on objecting to processing • be truly informed when giving consent to processing • comprehend when a contract is being formed and its implications • understand data protection rights and limitations	• training • documentation • user agreements • help • tutorials • mental models • metaphors • layout • feedback

Comprehension

Requirements	Possible Solutions
• **comprehend** how PII is handled • **know** who is processing PII and for what • **comprehend** when a contract is being formed and its implications • **understand** data protection rights and limitations	• training • layout • feedback

Privacy Comprehension Challenges

- how much information
- words, phrases, reading level, knowledge
- privacy jargon
- Internet technology (e.g., cookies)
- complexity (e.g., P3P has over 36,000 combinations)

Consciousness

Requirements	Possible Solutions
• be aware of transparency options • be informed when PII is processed • be aware of what happens to PII when retention periods expire • be conscious of rights to examine and modify PII • be aware when information may be collected automatically	• messages • pop-up windows • assistants • layout • highlight by appearance • alarms

Consciousness

Requirements	Possible Solutions
• be • be • be w • be ar • be aware when information may be collected automatically	• alarms

Privacy Consciousness Challenges

- e.g., Cranor et al. (2002): reading privacy policies
  - 29% never
  - 49% occasionally
  - 20% most when sharing personal info
  - 2% most/all

Control

Requirements	Possible Solutions
• control how PII is handled • be able to object to processing • control how long PII is stored • be able to exercise the rights to examine and correct PII	• affordances • obviousness • mapping • analogy

Control

Requirements	Possible Solutions
• control how PII is handled • be • co • be ex	• affordances

Privacy Control Challenges

- opt-in/out controls that can be found & used
- difficulty expressing preferences and trade-offs
- explicit/implicit gathering of preferences
- reasonable default settings

Consent

Requirements	Possible Solutions
• give **informed consent** to the processing of PII • give **explicit consent** for a Controller to perform the services being contracted for • give **specific, unambiguous consent** to the processing of sensitive data • give **special consent** when information will not be editable • **consent** to the automatic collection and processing of information	• user agreement • click-through agreement • **"Just-In-Time Click-Through Agreements"**

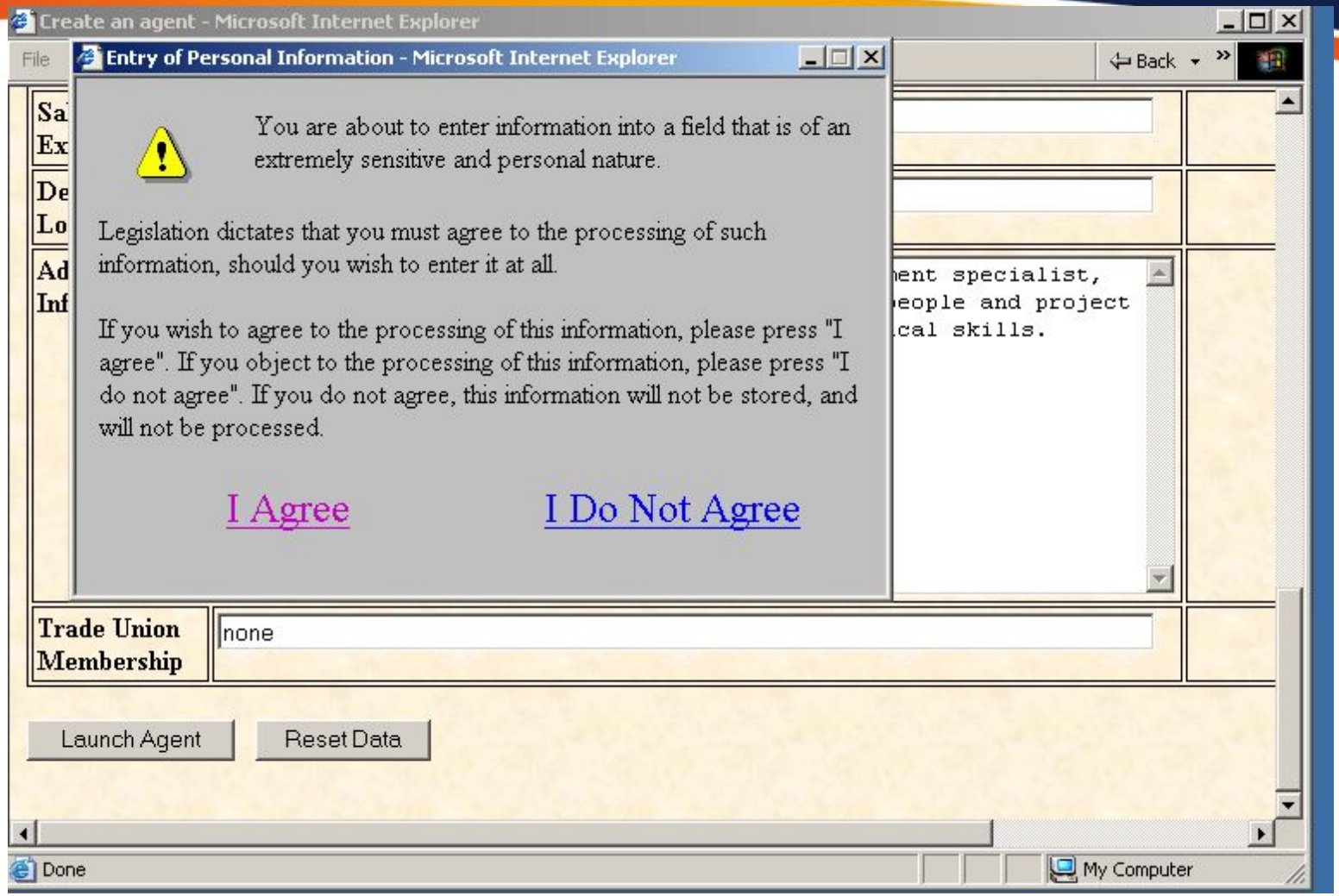
Consent

Requirements	Possible Solutions
• give **informed consent** to the processing of PII • g… C… k… • g… **consent** to the processing of sensitive data • give **special consent** when information will not be editable • **consent** to the automatic collection and processing of information	• user agreement • "Click-through Agreements"

Privacy Consent Challenges

- ignoring click-through agreements
- global consent not appropriate for multiple contexts
- tracking specific agreements

Just-in-Time Click-Through Agreements



Summary

- the 5 “Cs” for building usable privacy-protecting systems
  - comprehension
  - consciousness
  - control
  - consent
  - (context)

More Information?
www.andrewpatrick.ca