04 - Introduction to Privacy

Lorrie Cranor, Blase Ur, and Rich Shay

January 22, 2015

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security
Today!

• What does privacy mean to you?
• Privacy goals
• Why is privacy hard to measure?
• How privacy is protected
• Privacy notice and choice (intro)
• Homework presentations
What does privacy mean to you?

http://cups.cs.cmu.edu/privacyillustrated/
Hard to define

“Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”

Limited access to self

“Being alone.”
- Shane (age 4)

“the right to be let alone”
- Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)

“our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others attention.
Control over information

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

“…each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication….”

Alan Westin, Privacy and Freedom, 1967
How does each goal relate to privacy?

*I want to have… I want to be…*

- Solitude, uninterrupted
- Unseen, unheard, unread
- Not talked about
- Not judged
- Not profiled, not targeted, not treated differently than others
- Not misjudged
- Free to try, practice, make mistakes, self-reflect
- Not surprised (contextual integrity)
- Not accountable
- Not required to reveal
- Unknown
- Forgotten
- Intimacy
- Control
- Boundaries
- Identity
- Security
- Safety
- Others?
Measuring privacy

• Why is privacy hard to measure?
• Why are attitudes about privacy hard to measure?
• Why is the cost of privacy invasion hard to measure?
How privacy is protected

• Laws, self regulation, technology
  – Notice and access
  – Control over collection, use, deletion, sharing
  – Collection limitation
  – Use limitation
  – Security and accountability
Privacy laws around the world

- Privacy laws and regulations vary widely
- US has mostly sector-specific laws, minimal protections, often referred to as “patchwork quilt”
  - No explicit constitutional right to privacy or general privacy law
  - But some privacy rights inferred from constitution
  - Narrow regulations for health, financial, education, videos, children, etc.
  - Federal Trade Commission jurisdiction over fraud and deceptive practices
  - Federal Communications Commission regulates telecommunications
  - Some state and local laws
- European Data Protection Directive - EU countries must adopt similar comprehensive laws, recognize privacy as fundamental human right
  - Privacy commissions in each country
OECD fair information principles

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability
- [http://www.privacyrights.org/ar/fairinfo.htm](http://www.privacyrights.org/ar/fairinfo.htm)
US government privacy reports

• U.S. FTC and White House reports released in 2012

• U.S. Department of Commerce multi-stakeholder process to develop enforceable codes of conduct
Privacy self regulation

Notice and Choice
Notice and choice

Protect privacy by giving people control over their information

**Notice** about data collection and use

**Choices** about allowing their data to be collected and used in that way
Why don’t we have a market for privacy?
Privacy concerns seem inconsistent with behavior

• People say they want privacy, but don’t always take steps to protect it

• Many possible explanations
  – They don’t really care that much about privacy
  – They prefer immediate gratification to privacy protections that they won’t benefit from until later
  – They don’t understand the privacy implications of their behavior
  – The cost of privacy protection (including figuring out how to protect their privacy) is too high
Nobody wants to read privacy policies

“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

Cost of reading privacy policies

- What would happen if everyone read the privacy policy for each site they visited once each month?
- Time = 244/hours year
- Cost = $3,534/year
- National opportunity cost for time to read policies: $781 billion

Privacy Icons

http://www.azarask.in/blog/post/privacy-icons/

2010

- **Your Data is Used Only for the Intended Use**
- **Your Data May be Used for Purposes You Do Not Intend**
- **Your data is never given to advertisers.**
- **Site gives your data to advertisers.**
- **Your data is never bartered or sold.**
- **Your data may be bartered or sold.**
- **Data is given to law enforcement only when legal process is followed.**
- **Data may be given to law enforcement even when legal process is not followed.**
- **Your data is kept for less than 1 month.**
- **Your data may be kept indefinitely.**
Towards a privacy “nutrition label”

- Standardized format
  - People learn where to find answers
  - Facilitates policy comparisons

- Standardized language
  - People learn terminology

- Brief
  - People find info quickly

- Linked to extended view
  - Get more details if needed
Iterative design process

- Series of studies
  - Focus groups
  - Lab studies
  - Online studies

- Metrics
  - Reading-comprehension (accuracy)
  - Time to find information
  - Ease of policy comparison
  - Subjective opinions, ease, fun, trust


Privacy label for Android

Like word games? Like weasels? This is the game for you. Word Weasel is a fast word game where you find as many words as you can from 9 letters in 50 seconds. Compete with everyone else playing at the same time, a new game starts every minute!

"The most fun you can have on your own with 9 random letters. Brilliantly simple, devilishly addictive." –Kim, Android Market comment

Ad supported, with ability to upgrade to ad-free full version in game.

Uses the SOWPODS word list containing 100,000+ words. They may be obscure, but yes those are words!

Privacy Facts

This app collects your
- Personal information
- Location
- Analytics

This app uses
- Advertising

Reviews

Average 4.6

5 stars 534
4 stars 210
3 stars 37
2 stars 5
1 star 7
Role play studies

• Task for participants in lab or online
  – Select apps for friend with new Android phone
  – Choose from 2 similar apps w/ different permission requests in each of 6 categories
  – Click on app name to visit download screens

• Post-task questionnaire

• Participants who saw Privacy Facts more likely to select apps that requested fewer permissions
  – Other factors such as brand and rating reduce effect

P.G. Kelley, L.F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. CHI 2013.
Requirements for meaningful control

• Individuals must understand what options they have

• Individuals must understand implications of their options

• Individuals must have the means to exercise options

• Costs must be reasonable
  – Money, time, convenience, benefits
More on privacy coming March 17