Week 6 - Info2222

Privacy and users

Core learning objectives for Week 6 - privacy

- What does privacy mean, in the context of IT?
- What the meanings of as well as similarities and differences between: secrecy, confidentiality, availability, auditability, access control, anonymity and privacy?
- How do people vary in their privacy preferences?
- What is the privacy paradox?
- What is privacy by design?
- What is the right to be forgotten?

But first….

Some famous/infamous comments

“You have zero privacy anyway
Get over it.”
Scott McNealy ….. SUN Microsystems

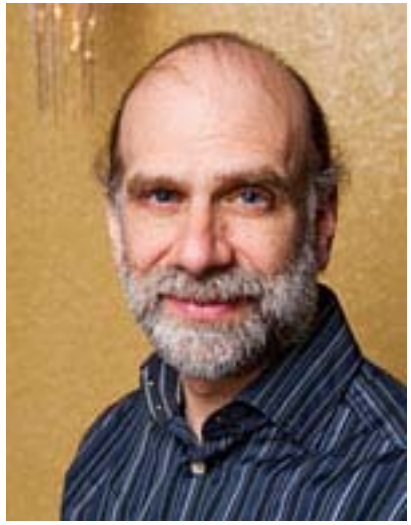
Polly Sprenger, Wired 01.26.99

Sun on Privacy: 'Get Over It,

”….If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. If you really need that kind of privacy, the reality is that search engines -- including Google -- do retain this information for some time …."

Csnews, You Have Zero Privacy Anyway -- Get Over It

David Adams, 11th Dec 2009 01:25 UTC



Comment by Bruce Schneier

2006

https://www.schneier.com/blog/archives/2009/12/my_reaction_to.html

For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness….

Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control.

What does privacy mean, in the context of IT?

Some key definitions of privacy

“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.”

Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. 2087 (2001).

“the right to be let alone”

Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193 (**1890**)

“to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds”

“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

Technology – IT – has altered the challenges of achieving privacy

As well as people's awareness of
when their privacy is compromised

Table 1. Evolution of the Information Privacy Concept Following the Evolution of IT (adapted from Westin 2003)

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Summary: privacy is complex

BUT

We all have mental models about privacy

Even children …

Blaze Ur, 2017, Univ of Chicago

Privacy ….

Important enough to have legislation controlling it, even for the case of person data on computers

What the meanings of as well as similarities and differences between: secrecy, confidentiality, availability, auditability, access control, anonymity and privacy?

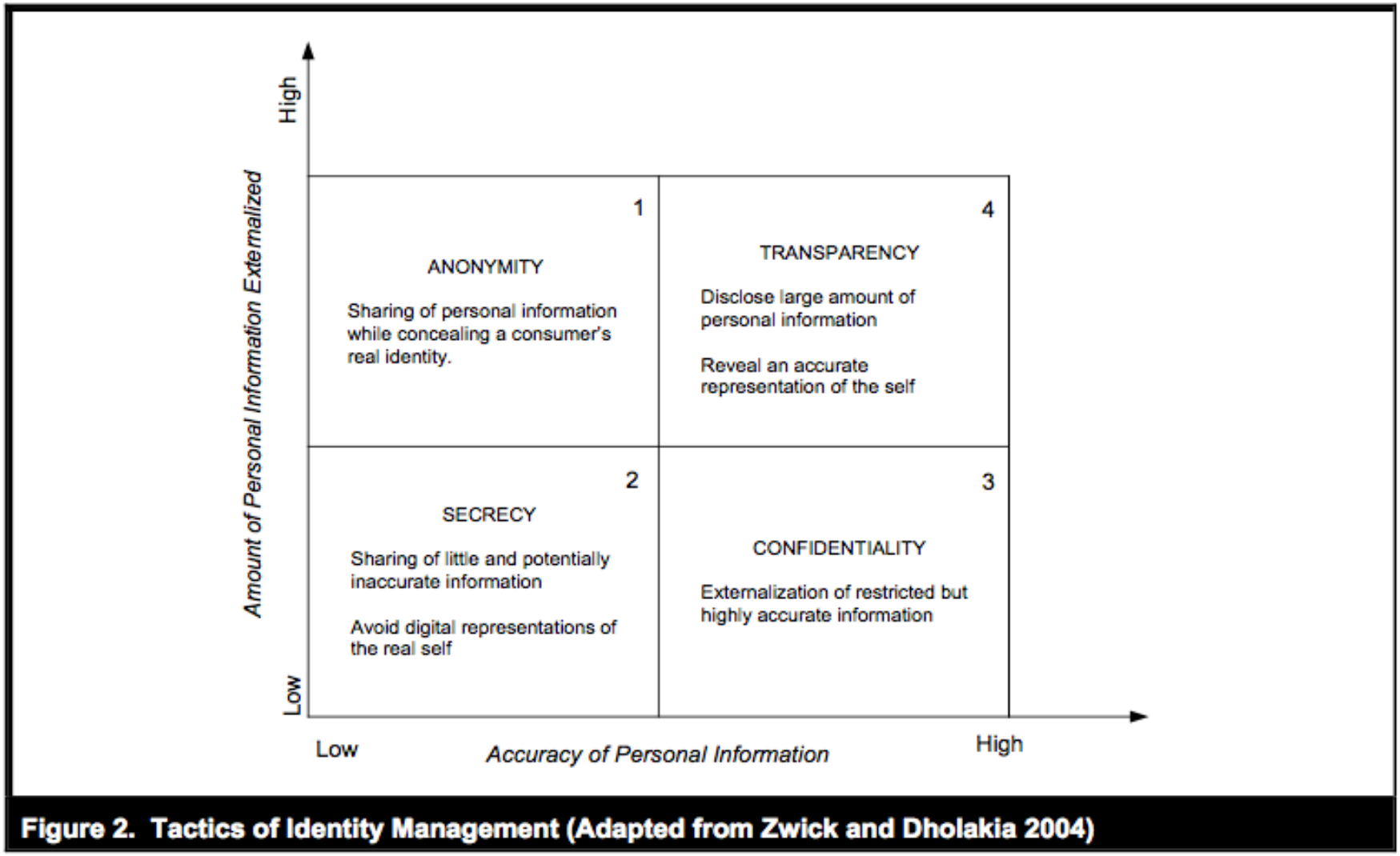


Figure 2. Tactics of Identity Management (Adapted from Zwick and Dholakia 2004)

- Secrecy – keeping things hidden
- Confidentiality – keep someone else's data hidden
- Availability – opposite of secrecy

- Anonymity – keep the identity of the person associated with the data secret

- Privacy – principles/rules to control availability of data

- Auditability – able to keep a record of data made available
- Access control – the rules for controlling privacy

- Personal Data – data about a person, linked to their identity
- Provenance – the history of ownership of data
  eg Data from individual … Facebook … Cambridge Analytica …

Summary: privacy involves a balance of secrecy and availability

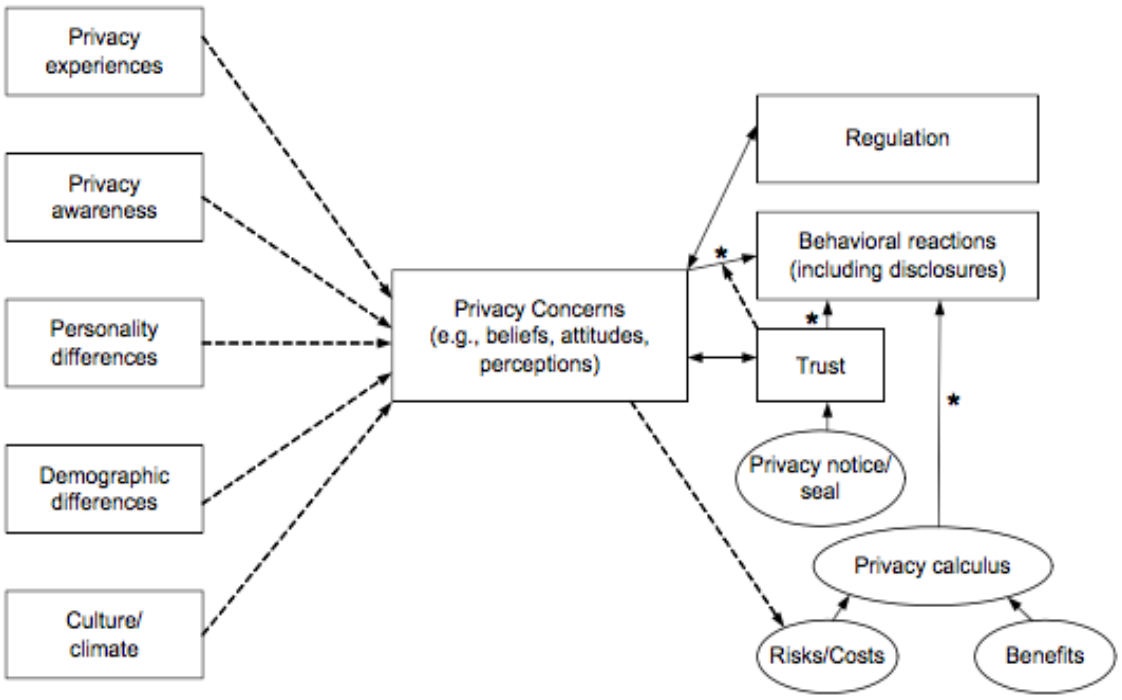
How do people vary in their privacy preferences?

Different people have different preferences

One person has different preferences at different times and for different data

Some people are more concerned about privacy than others

This comes from people's privacy **worldview**, which is determined by complex aspects of people's mental models about privacy and a complex of associated factors



Dotted lines indicate that the relationship is tenuous (i.e., has not been confirmed through repeated studies).

Not shown: Possible two-way loop, in which some actions on the right may impact some constructs on the left.

*Results threatened by privacy paradox, since usually intentions (not behaviors) have been measured.

Figure 3. Relationships Between Privacy and Other Constructs: Antecedents → Privacy Concerns → Outcomes (APCO Macro Model)

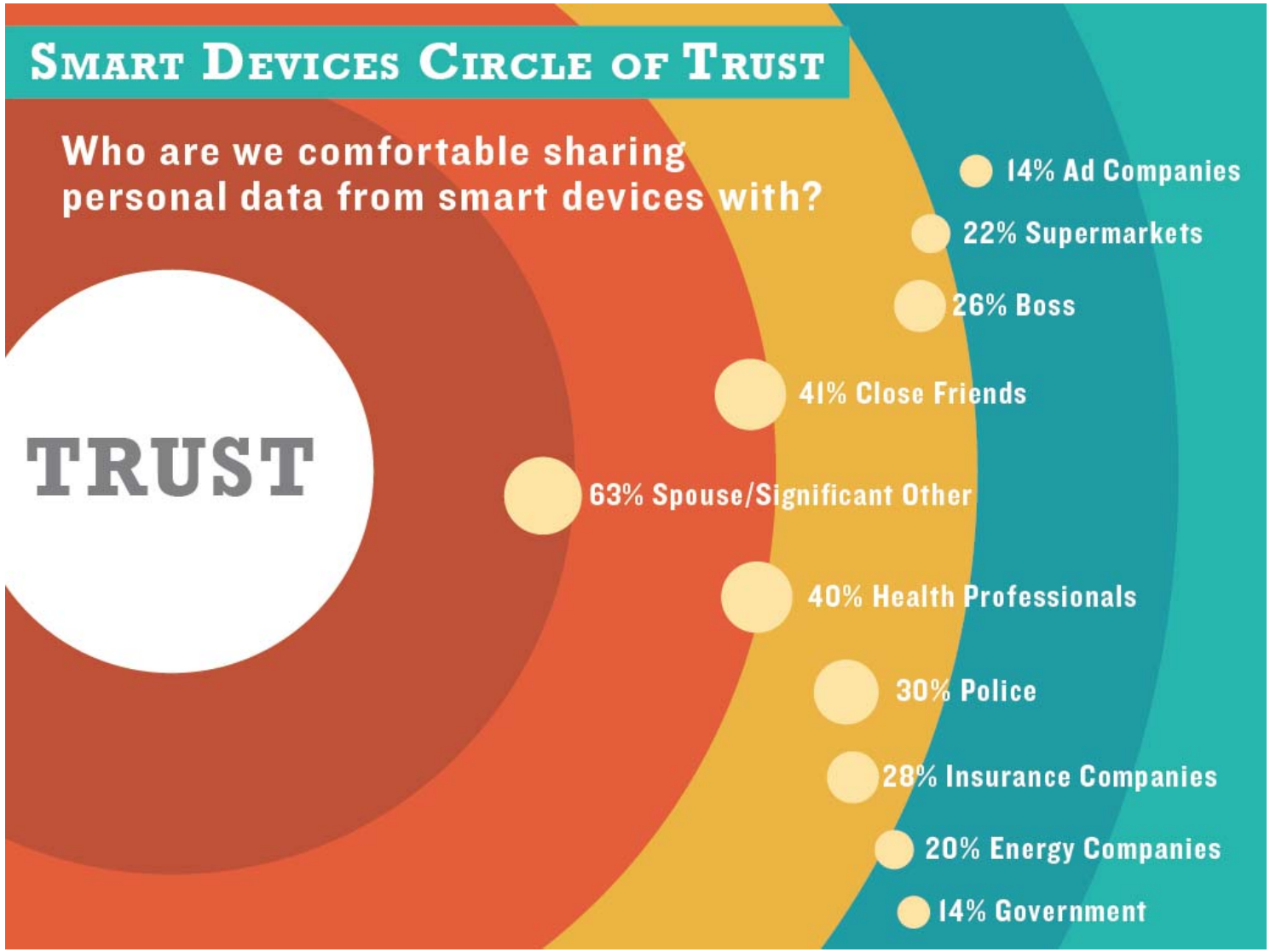
Privacy zealots

average citizen

People unconcerned about privacy

We have different privacy preferences for sharing with different people

On average people show similar comparative assessments for certain classes of personal data



Internet of Things Industry Brings Data Explosion, but Growth Could be Impacted by Consumer Privacy Concerns

http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns/

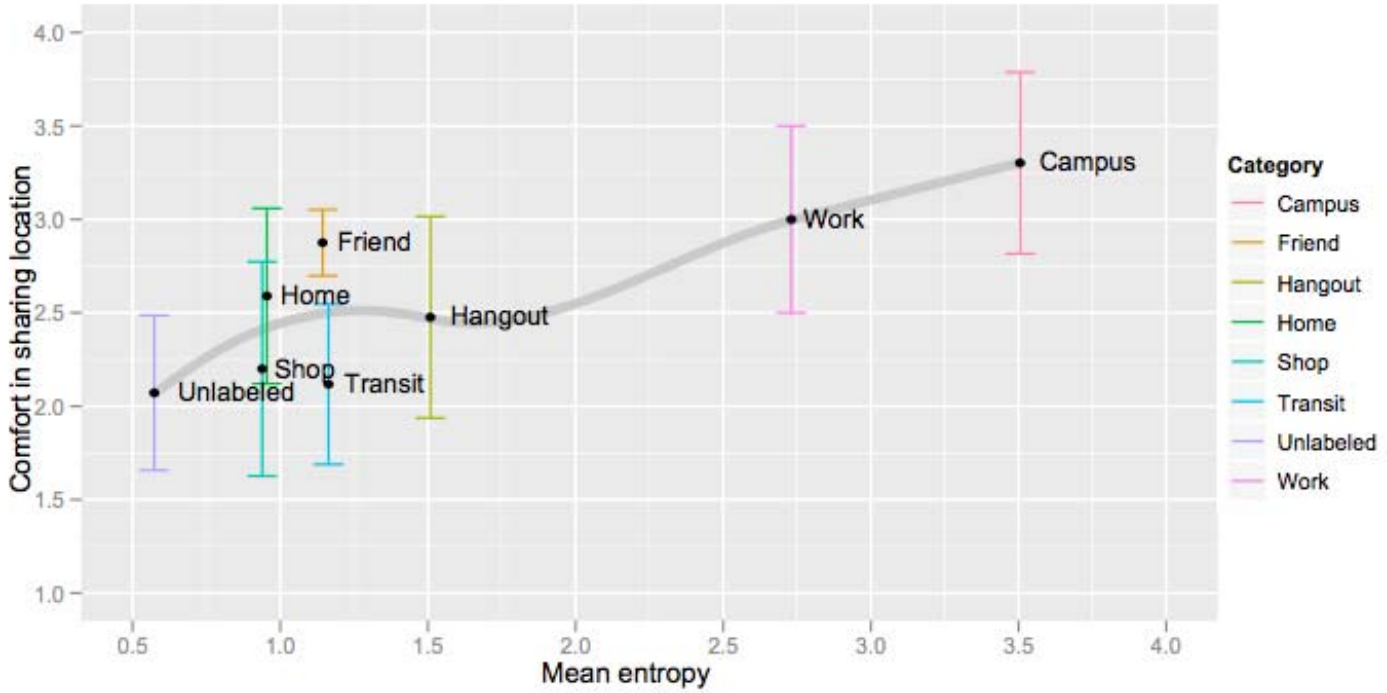


Figure 6. Comfort in sharing location with an average of scores for university population, acquaintances and everybody, according to entropy. Each points is the average of the category (e.g., "Campus" for university location, "Friend" for a friend's home, "Hangout" for restaurants and coffee shops, and so forth. Comfort in sharing location is based on a four point scale, where 1 is "very uncomfortable" sharing a location and 4 is "very comfortable." The blue line depicts the moving average using local polynomial regression fitting.

Location sharing

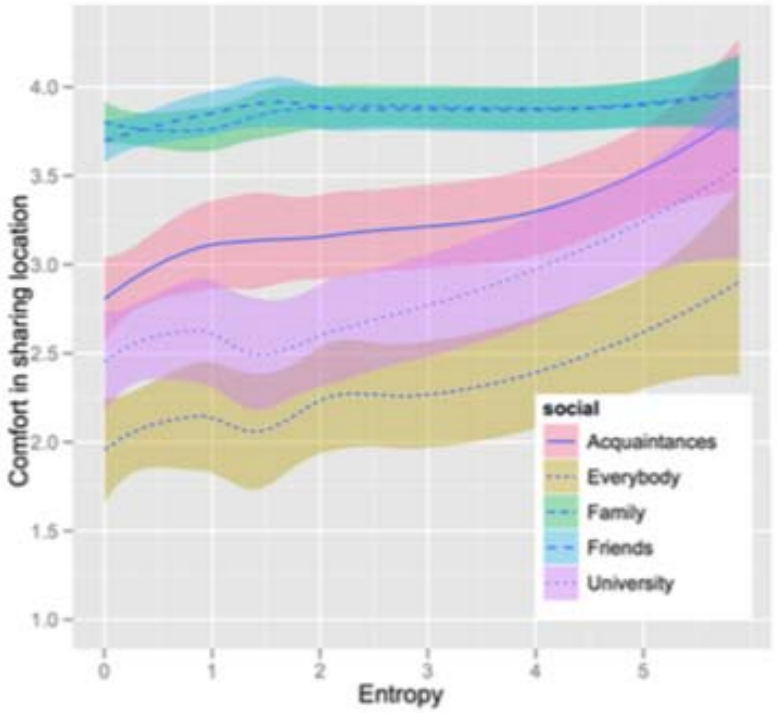


Figure 7. Comfort in sharing location versus entropy, for 5 social groups. Comfort in sharing location is based on a four point scale, where 1 is "very uncomfortable" sharing a location and 4 is "very comfortable." Lines represent moving averages, based on local polynomial regression fitting. Colored areas are error bounderies. The lines for Friends and Family averages overlap. We can see that for the acquaintances, everybody, and university groups, sharing comfort is strongly correlated with entropy.

Toch, E., Cranshaw, J., Drielsma, P. H., Tsai, J. Y., Kelley, P. G., Springfield, J., Cranor, L., Hong, J., and Sadeh, N. Empirical models of privacy in location sharing. In Proceedings of the 12th ACM International Conference on Ubiquitous Computing, UbiComp '10, ACM (New York, NY, USA, 2010), 129–138.

Some data is more sensitive …
ie people want to keep it secret

On average people show similar comparative assessments

Privacy In All Things Includes the Internet of Things

July 1st, 2014 by Alexandra Ross

"recent TRUSTe research …. 6 out of 10 (59%) of internet users have basic privacy awareness of IoT – they know that smart devices such as smart TVs, fitness devices and in-car navigation systems could collect data about their personal activities. Not surprisingly, users want more information and control

85% agreed that they would want to **understand** more about data being collected **before using smart devices**

88% agreed that they would want to **control** the data being collected through smart devices before purchasing or using a device

…

87% are concerned about the type of personal information collected through smart devices

These privacy concerns could be a potential barrier to the growth of the IoT market as only 22% of respondents agreed that the benefits of smart devices outweighed any privacy concerns."

What is the privacy paradox?

Privacy paradox: actual behavior is inconsistent with stated beliefs

People say they care abut digital privacy

But they sign up for Facebook, do not read privacy policies

What is privacy by design?

"a methodology that enables privacy to be ‘built in’ to the design and architecture of information systems, business processes and networked infrastructure. PbD aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information

https://www.cpdp.vic.gov.au/menu-privacy/privacy-organisations/privacy-organisations-privacy-by-design

Privacy by Design features seven Foundation Principles:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy – Keep it User-Centric

https://www.cpdp.vic.gov.au/menu-privacy/privacy-organisations/privacy-organisations-privacy-by-design

PbD calls on the broad range of stakeholders, including software engineers, the take a deeply human-centred view of the design for privacy and user control

Legislators refer to it

Eg European Union regulations – General Data Protection Regulation (GDPR) which come into force in May 2018

Just a glimpse….. Of GDPR

Art. 25 GDPR

Data protection by design and by default

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) [1] The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2] That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3] In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

What is the right to be forgotten?

From 2006 European Union legislation

With the first cases seeing Google defeated and required to remove “personal information” about

Recent News

Google Occupies an Odd Role in Enforcing Privacy Laws. A Businessman's Landmark 'Right To Be Forgotten' Win Just Revealed It.

David Meyer April 16, 2018

http://fortune.com/2018/04/16/google-right-to-be-forgotten-case-loss/

“Google lost a landmark, “right to be forgotten” case at the end of last week, with the High Court in London ruling that it had to delist from its search results articles relating to a businessman’s past crimes.

Core learning objectives for Week 6 - privacy

- What does privacy mean, in the context of IT?
- What the meanings of as well as similarities and differences between: secrecy, confidentiality, availability, auditability, access control, anonymity and privacy?
- How do people vary in their privacy preferences?
- What is the privacy paradox?
- What is privacy by design?
- What is the right to be forgotten?