Privacy in the digital society

Alberto Marchetti Spaccamela: Fall 2019

Lesson 1

- To define Privacy is difficult:
  - elusive to define: there is not a common definition
- What kind of information is private
- Who is interested: (foreign) government, companies
- Why privacy matters even if you have "*Nothing to hide*"
- Aggregation and correlation
- Accountability

Wikipedia: http://en.wikipedia.org/wiki/Privacy

- **Privacy** (from Latin: *privatus* "separated from the rest, deprived of something, esp. office, participation in the government", from *privo* "to deprive") is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.
- The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a *person*, it usually means there is something to them inherently special or sensitive. The domain of privacy partially overlaps security, including for instance the concepts of appropriate use, as well as protection of information.

Difficult 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."

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

- The right not to be subjected to unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' privacy laws, and in some cases, constitutions.

- Examples:
  - Almost all countries have laws which in some way limit privacy; an example of this would be law concerning taxation, which normally require the sharing of information about personal income or earnings.
  - In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures.

- Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits and very often with specific dangers and losses, although this is a very strategic view of human relationships.
- Example: a person may volunteer personal details (often for advertising purposes) in order to gamble on winning a prize or to have a discount or using some software or application.
- Personal information which is voluntarily shared but subsequently stolen or misused can lead to *identity theft*.

- The concept of universal individual privacy is a modern construct associated with Western culture, English and North American in particular, and remained virtually unknown in some cultures until recent times.
- Most cultures, recognize the ability of individuals to withhold certain parts of their personal information from wider society - a figleaf over the genitals being an ancient example.
- The word "privacy" is sometimes untranslatable, and many languages do not have a specific word for "privacy".
  - Examples: Russian combines the meaning of solitude, secrecy and private life other borrow from English "privacy" (as Indonesian *Privasi* or Italian *la privacy*).

Nothing to hide?

- What is the "nothing to hide" argument?
- Sometimes the nothing to hide is posed as a question:
  - If you have nothing to hide, then what do you have to fear?
  - If you aren't doing anything wrong then what o you have to hide?
- It assumes that information that you want to hide are bad things

Nothing to hide: US government

Privacy is really just a euphemism for concealment, for hiding specific things about ourselves from others.

- We conceal aspects of our person, our conduct and our history that, if known, would make it more difficult for us to achieve our personal goals
- Civil liberties groups worry about governmental surveillance of people's computer files and other stored data.
- Surveillance technology used by our government is also used by our enemies.

Nothing to hide?

- What is the "nothing to hide" argument?
- How is it used to argue for limited privacy rights?
- What counter-arguments are there?

Solove, Daniel J., "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" . San Diego Law Review, Vol. 44, 2007 Available at SSRN: http://ssrn.com/abstract=998565

"Privacy's function...is not to protect the presumptively innocent from true but damaging information, but rather to protect the actually innocent from damaging conclusions drawn from misunderstood information." -- Lawrence Lessig, *Privacy and Attention Span* 2001

Nothing to hide? - 2

- Solzhenitsyn: "*Everyone is guilty of something or has something to conceal. All one has to do is look hard to find it is*"
- Flaherty: *There is no sentient human in the western world who has little or no regard of his/her personal privacy; those that claim such things cannot withstand even a few minutes questioning about intimate aspects of their lives without capitulating to the intrusiveness of ceratin subject matters.*
- If you have nothing to hide give me that photo of you naked and drunk. And I can give to the person that will interview you for a new job
- If you have nothing to hide give me your credit card number

Nothing to hide? -3

- Everyone has *something* to hide: Saying you have nothing to hide equates to "I don't care what happens so long as it doesn't happen to me"
- A society without privacy protections would be suffocating
- Privacy is a benefit to society because it provides individuals with space to be themselves apart from the rest of society where they must observe rules and social norms
- Faulty premise -- privacy is not about hiding bad things

Nothing to hide? -4

- Surveillance of legal activities can inhibit people from participating in them -- chilling effects
- Even if you have nothing to hide, data mining may result in your profile matching a profile that predicts you have done something wrong or will do something wrong, and may be relied on even if the prediction has no merit
- Privacy invasions cause a variety of harms, beyond just revealing secrets

Nothing to hide? -5

Nothing to hide focuses primarily on the information collection problems associated with state security (e.g. terrorism). It claims that limited surveillance of lawful activity will not limit indivuals and will have larger security benefits. Problems:

i) **aggregating data**: combination of small bits of innocuous data; when aggregated these data say many things (sophisticated data mining)

ii) **exclusion:** people do not have knowledge about their information is used and cannot change and correct wrong data

iii) **secondary use:** data collected for one purpose can be used for other purposes

Britney Spears: "We just need privacy"

"You have to realize that we're people and that we need, we just need privacy and we need our respect, and those are things that you have to have as a human being."

— Britney Spears
15 June 2006
NBC Dateline

http://www.cnn.com/2006/SHOWBIZ/Music/06/15/people.spears.reut/index.html

“We just need privacy”: what does it mean?

Multiple conceptions of privacy not clear

THERE IS NOT a definition good for all

- Personhood
- Intimacy
- Secrecy
- Limited access to the self
- Control over information

Privacy of personal space

- Historically, depended a lot on the type and proximity of available housing
- In 18th century Europe, most people lived in cities where houses were close together, but small number of people lived in each house
- In 18th century America, people lived far away from each other but many people lived in each house and even shared beds

Privacy of personal space

In 18th century America, colonists lived houses far away from each other.

Social and security issues

- They began to collect information about each other (Census, birth and death records, school records, tax records)
- Informants reported people who behaved badly (Disorderly children, nightwalkers, Sabbath breakers, atheists, drunks)

Communication privacy

- When all communication was oral, communication privacy depended on
  - Communicating without someone overhearing
  - Communicating with people who wouldn't tell others
- Written communications brought new opportunities for privacy violations
- In 18th century America, postal mail was not necessarily private
  - Sealing wax, basic encryption used to increase privacy
  - 1782 – US Congress made it illegal to open other peoples' mail

Telegraph

- In the late nineteenth century the telegraph became a popular means of long distance communication
- Messages could be coded, but you could not recover damages due to transmission errors if the message was coded
- Telegraph operators were supposed to keep messages confidential
- Occasional subpoenas for telegraph messages

Cameras

- Cameras, especially portable "snap" cameras (1888), raised new privacy concerns
- Telephoto lenses
- Video cameras
- Hidden cameras
- Web cams
- Satellite images

Today

- Internet companies like Google, Facebook, Linkedin, ecc offer “free” services. Capitalization stock market (Sept. 2019)
  - Google: 852 Billion US $, Facebook 532 Billion US $
  - Italian stock market (whole Italy) 640 Billion Euro
- Google & Facebook business: publicity, advertisement
- Advertisement is focused using private information
- Big data analytics: allow to obtain unexpceted information

Today

Privacy issues arise in many different contexts and aspects of human life:

- Data collection by companies, public organiztions, social netwoorks, supermarkets, banks, ...
- Different social contexts: family, small group, social networks
- Control of private information vs collection of private information

Limited access to self

"*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.*"

Ruth Gavison, "Privacy and the Limits of the Law," *Yale Law Journal* 89 (1980)

Limited access to self

- "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"
- "Desire for privacy is never absolute"
- "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...."
- Westin "Privacy and Freedom" 1967

How does each goal relate to privacy?

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

Westin's 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

Westin's control over information

Example: It is the your decision to let people know if you have cancer

1. You buy a book on Cancer. This does imply you have cancer

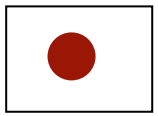
2. You buy a wig. This does not imply you have cancer

BUT 1 + 2 increases the possibility that you might have cancer

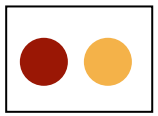
Note: if you buy on Amazon then they correlate the information

Westin's four states of privacy

- Solitude: individual separated form the group and freed form the observation of other persons

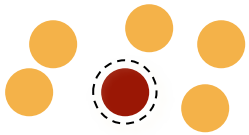


- Intimacy: individual is part of a small unit



- Anonymity: individual in public but still seeks and finds freedom from identification and surveillance

- Reserve: the creation of a psychological barrier against unwanted intrusion - holding back communication



Westin's four functions of privacy

- Personal autonomy
  - control when you go public about info
- Emotional release
  - be yourself
  - permissible deviations to social or institutional norms
- Self-evaluation
- Limited and protected communication

Realizing limited access and control

- Limited access
  - Laws to prohibit or limit collection, disclosure, contact
  - Technology to facilitate anonymous transactions, minimize disclosure
- Control
  - Laws to mandate choice (opt-in/opt-out)
  - Technology to facilitate informed consent, keep track of and enforce privacy preferences

Information privacy

- Information privacy concerns the collection, use, and disclosure of personal information
- European Union rules for data protection
- *... it includes to safeguard human dignity and specific measuresto protect the legitimate interests and fundamental rights of the parties concerned, in particular as regards the transparency of the treatment, the transfer of personal data....*

Solove's privacy taxonomy

- Information Collection
  - Surveillance
  - Interrogation
- Information Processing
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion
- Information Dissemination
  - Breach of Confidentiality
  - Disclosure
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
  - Distortion
- Invasion
  - Intrusion
  - Decisional Interference

Floridi: Human Dignity and Privacy

The over-quoted text of EU regulations implies two concepts:

- the person concerned is a natural person, whose dignity must be safeguarded (a legal person cannot enjoy human dignity);
- human dignity differs from "legitimate interests and fundamental rights".

Floridi: the protection of privacy should be based directly on the protection of the human dignity and not indirectly on the basis of other rights, for example the property' or freedom 'of expression

Floridi: Human Dignity and Privacy

- "[...] greater respect and protection of human dignity could act as a counterweight to the pervasive surveillance and the asymmetry of power with which individuals must now compare. It should be the focus of a new digital ethics.
- [...] the private life is an integral part of human dignity and the right to data protection was originally conceived in the 70s and 80s as a means to compensate for the potential erosion of privacy and dignity through the processing of personal data on a large scale.

Information vs. decisional privacy

- Information privacy concerns the collection, use, and disclosure of personal information
- Decisional privacy concerns the freedom to make decisions about one's body and family

Decisional privacy

Limited access vs. control

- Privacy as limited access to self
  - the extent to which we are known to others and the extent to which others have physical access to us
  - CA (Cambridge Analytics): know about 4000 facts about 230 million of US citizens; using 70 “facebook like” CA knows you more than your friends; 150 more that your mate
  - Personalized ad campaing (e.g. recent US presidential elections)

Decisional privacy

Limited access vs. control

- Privacy as control over information
  - not simply *limiting* what others know about you, but *controlling* it
  - this assumes individual autonomy, that you can control information in a meaningful way (not blind click through, for example)

Multiple facets of privacy

- How can posting personal information about myself on my web site result in a reduction of my privacy? How can it result in an increase in my privacy?
- Privacy as deprivation?
  - Deprived of being heard and seen by others
  - Deprived of being contacted by others
  - Deprived of benefits that come as a result of your personal information being available to others

Privacy policies

- Policies let consumers know about site's privacy practices
- Consumers can then decide whether or not practices are acceptable, when to opt-in or opt-out, and who to do business with
- The presence of privacy policies increases consumer trust

What are some problems with privacy policies?

Privacy policy problems

BUT policies are often

- difficult to understand
- hard to find
- take a long time to read
- change without notice

Privacy policy components

Identification of site, scope, contact info

Types of information collected

Including information about cookies

How information is used

Conditions under which information might be shared

Information about opt-in/opt-out

Information about access

Information about data retention policies

Information about seal programs

- Security assurances
- Children's privacy

There is lots of information to convey -- but policy should be brief and easy-to-read too!

What is opt-in? What is opt-out?

Policy: 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 (I agree or continuing browsing)
- Claim: This allows free and informed consensus by providing tradeoff between privacy and benefits
- Is it true? Very long documents that nobody reads

Cost of reading 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

What would happen if everyone read the privacy policy for each site they visited once per year?

- 1 person: Time = 244/hours year, Cost = $3,534/year
- US National opportunity cost for time to read policies: $781 billion

How are online privacy concerns different from offline privacy concerns?

Web privacy concerns

- Data is often collected silently
  - Web allows large quantities of data to be collected inexpensively and unobtrusively
- Data from multiple sources may be merged
  - Non-identifiable information can become identifiable when merged
- Data collected for business purposes may be used in civil and criminal proceedings
- Users given no meaningful choice
  - Few sites offer alternatives

Browser Chatter

Browsers chatter about

- IP address, domain name, organization,
- Referring page
- Platform: O/S, browser
- What information is requested: URLs and search terms
- Cookies

To anyone who might be listening

- End servers
- System administrators
- Internet Service Providers
- Other third parties
- Advertising networks
- Anyone who might subpoena log files later

Typical HTTP request with cookie

GET /retail/searchresults.asp?qu=beer HTTP/1.0
Referer: http://www.us.buy.com/default.asp
User-Agent: Mozilla/4.75 [en] (X11; U; NetBSD 1.5_ALPHA i386)
Host: www.us.buy.com
Accept: image/gif, image/jpeg, image/pjpeg, */*
Accept-Language: en
Cookie: buycountry=us; dcLocName=Basket; dcCatID=6773;
dcLocID=6773; dcAd=buybasket; loc=;
parentLocName=Basket; parentLoc=6773; ShopperManager
%2F=ShopperManager
%2F=66FUQULL0QBT8MMTVSC5MMNKBJFWDVH7;
Store=107; Category=0

Referer log problems

- GET methods result in values in URL
- These URLs are sent in the referer header to next host
- Example:

```
http://www.merchant.com/cgi_bin/order?
   name=Tom+Jones&address=here
   +there&credit
   +card=234876923234&PIN=1234&-
   >index.html
```

Cookies

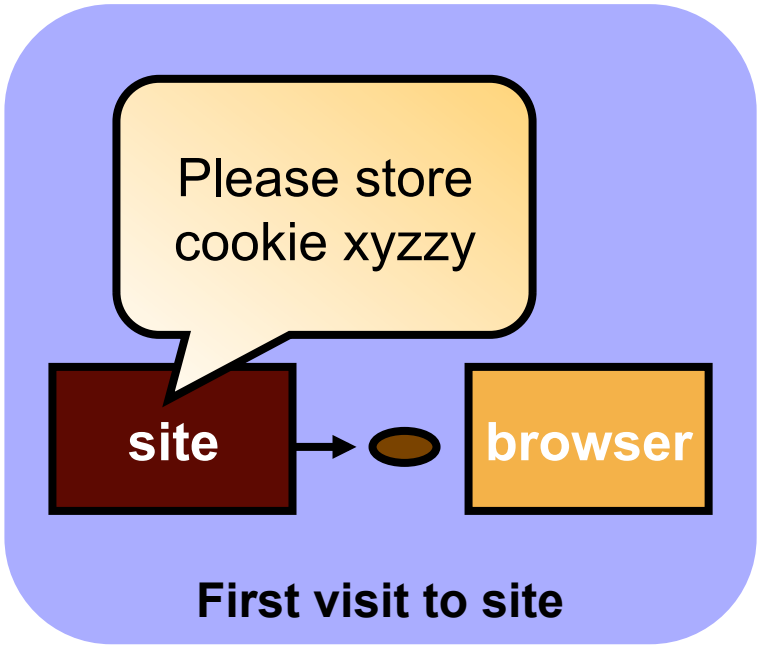
- What are cookies?
- What are people concerned about cookies?
- What useful purposes do cookies serve?

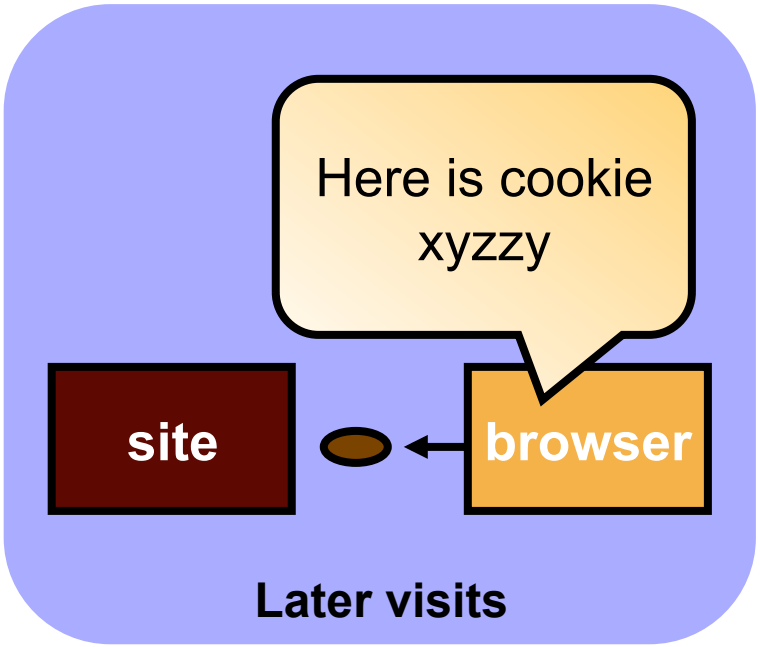
Cookies 101

- Cookies can be useful
  - Used like a staple to attach multiple parts of a form together
  - Used to identify you when you return to a web site so you don't have to remember a password
  - Used to help web sites understand how people use them
- Cookies can do unexpected things
  - Used to profile users and track their activities, especially across web sites

How cookies work – the basics

- A cookie stores a small string of characters
- A web site asks your browser to "set" a cookie
- Whenever you return to that site your browser sends the cookie back automatically

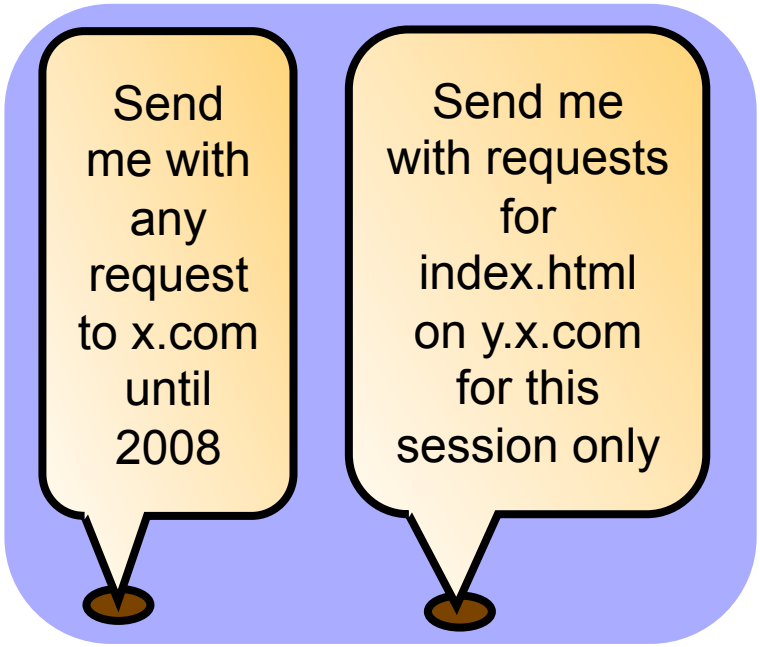




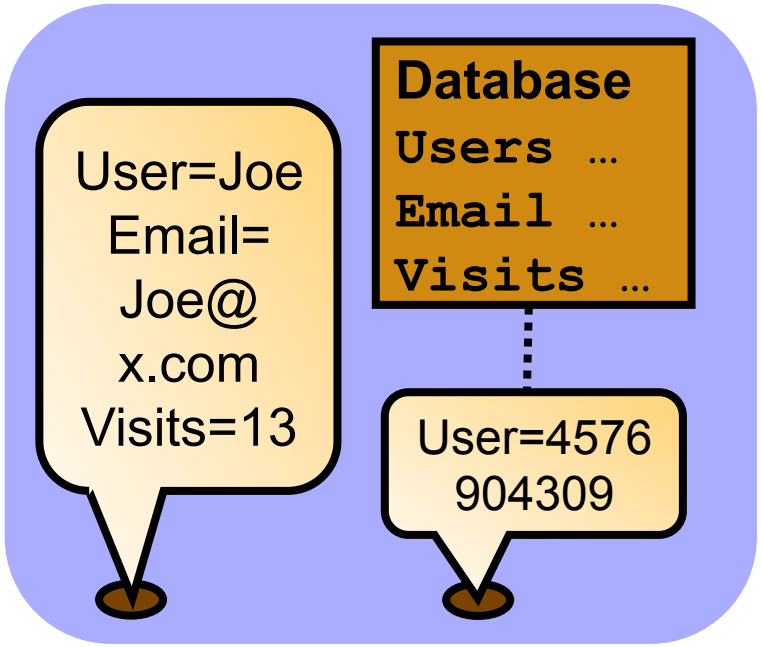
How cookies work – advanced

Cookies are only sent back to the "site" that set them – but this may be any host in domain

- Sites setting cookies indicate path, domain, and expiration for cookies



Cookies can store user info or a database key that is used to look up user info – either way the cookie enables info to be linked to the current browsing session



Cookie terminology

- Cookie Replay – sending a cookie back to a site
- Session cookie – cookie replayed only during current browsing session
- Persistent cookie – cookie replayed until expiration date
- First-party cookie – cookie associated with the site the user requested
- Third-party cookie – cookie associated with an image, ad, frame, or other content from a site with a different domain name that is embedded in the site the user requested
  - Browser interprets third-party cookie based on domain name, even if both domains are owned by the same company

Web bugs

- Invisible "images" (1-by-1 pixels, transparent) embedded in web pages and cause referer info and cookies to be transferred
- Also called web beacons, clear gifs, tracker gifs,etc.
- Work just like banner ads from ad networks, but you can't see them unless you look at the code behind a web page
- Also embedded in HTML formatted email messages, MS Word documents, etc.
- For software to detect web bugs see:

  http://www.bugnosis.org

How data can be linked

- Every time the same cookie is replayed to a site, the site may add information to the record associated with that cookie
  - Number of times you visit a link, time, date
  - What page you visit
  - What page you visited last
  - Information you type into a web form
- If multiple cookies are replayed together, they are usually logged together, effectively linking their data
  - Narrow scoped cookie might get logged with broad scoped cookie

Towards a privacy "nutrition label"?

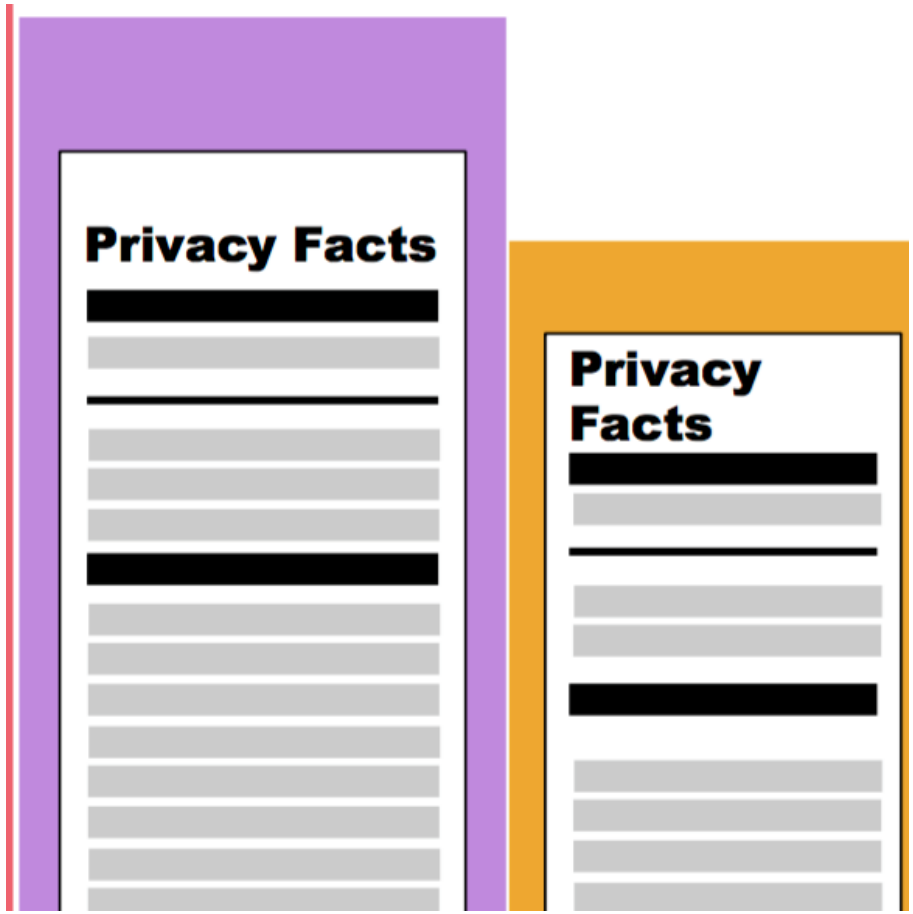
Standardized format

- People learn where to find answers
- Facilitates policy comparisons
- Standardized language
- People learn terminology
- Brief, we find info quickly
- Linked to extended view
- Get more details if needed

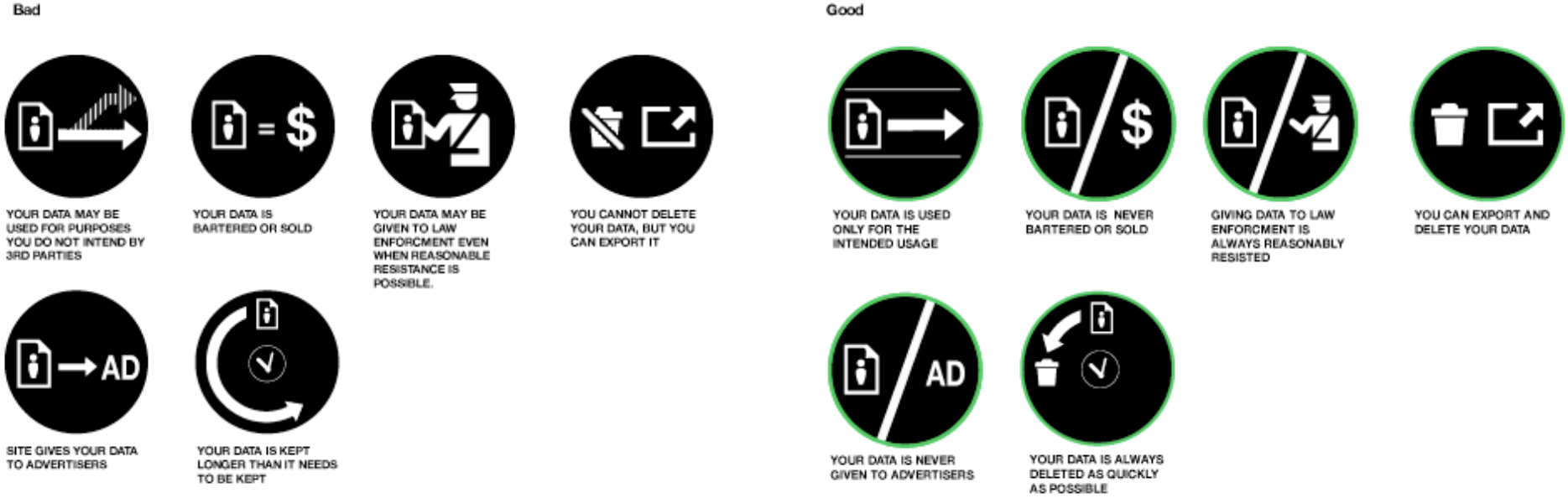
Towards a privacy "nutrition label"

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



Towards a privacy “nutrition label”



To be read

D. J. Solove: **Why privacy matters even if you have Nothing to Hide" and Other Misun-derstandings of Privacy,** George Washington U. Law School

R. Posner: **Privacy is overrated,** New York Daily news, 2013

Luciano Floridi: **On Human Dignity as a Foundation for the Right to Privacy** Che Futuro!

D.Powazek: I'm not the product, but I play one on the internet

Sites spying you in new ways

Video: http://www.abc.net.au/lateline/content/2015/s4327242.htm

To read (before Thursday)

D. J. Solove: **Why privacy matters even if you have Nothing to Hide"**

R. Posner: **Privacy is overrated,** New York Daily news, 2013

Luciano Floridi: **On Human Dignity as a Foundation for the Right to Privacy** Che Futuro!

Discussion questions

Your experience

- What does privacy mean to you?
  - How would you define privacy?
  - What does it meant to you for something to be private?
- How has your privacy been invaded?
  - Describe an incident in which your privacy was invaded by a friend, or a family member or a stranger or an institution
  - What is the funniest invasion of privacy that ever happened to you or someone you know?

Discussion questions

What will happen in the near future?

- Let's focus on the Kafka argument: list Government functions/agencies that use data about citizens to make decisions that have a significant impact on their lives.
- In general, as these processes become more data-driven and automated, do you feel that the potential for Kafkaesque treatment has increased or decreased?

Discussion questions

What should be private

- Should everything be private all the time?
- Should everyone have an absolute right to control what information about them is private?
- What are the costs of privacy?
  - Personal costs?
  - Societal costs?

Discussion questions

What will happen in the near future?

The underlying social values that require privacy are themselves changing. For example, it used to be the case that you had to keep your sexual orientation private if you were gay, but that is less important now because society is more tolerant of different sexual orientations.

Discussion questions

What will happen in the near future?

- Now think about Solove's example of cancer. How might society adapt so that in the future it is less of a problem if our health conditions were made public? Do you think this kind of adaptation will actually happen?

Discussion questions

Technologies

- Which technologies are privacy invasive?
- Which technologies are privacy protective?
- Can we turn one into the other?