University of Nottingham
UK | CHINA | MALAYSIA

COMP 3056 Professional Ethics in Computing

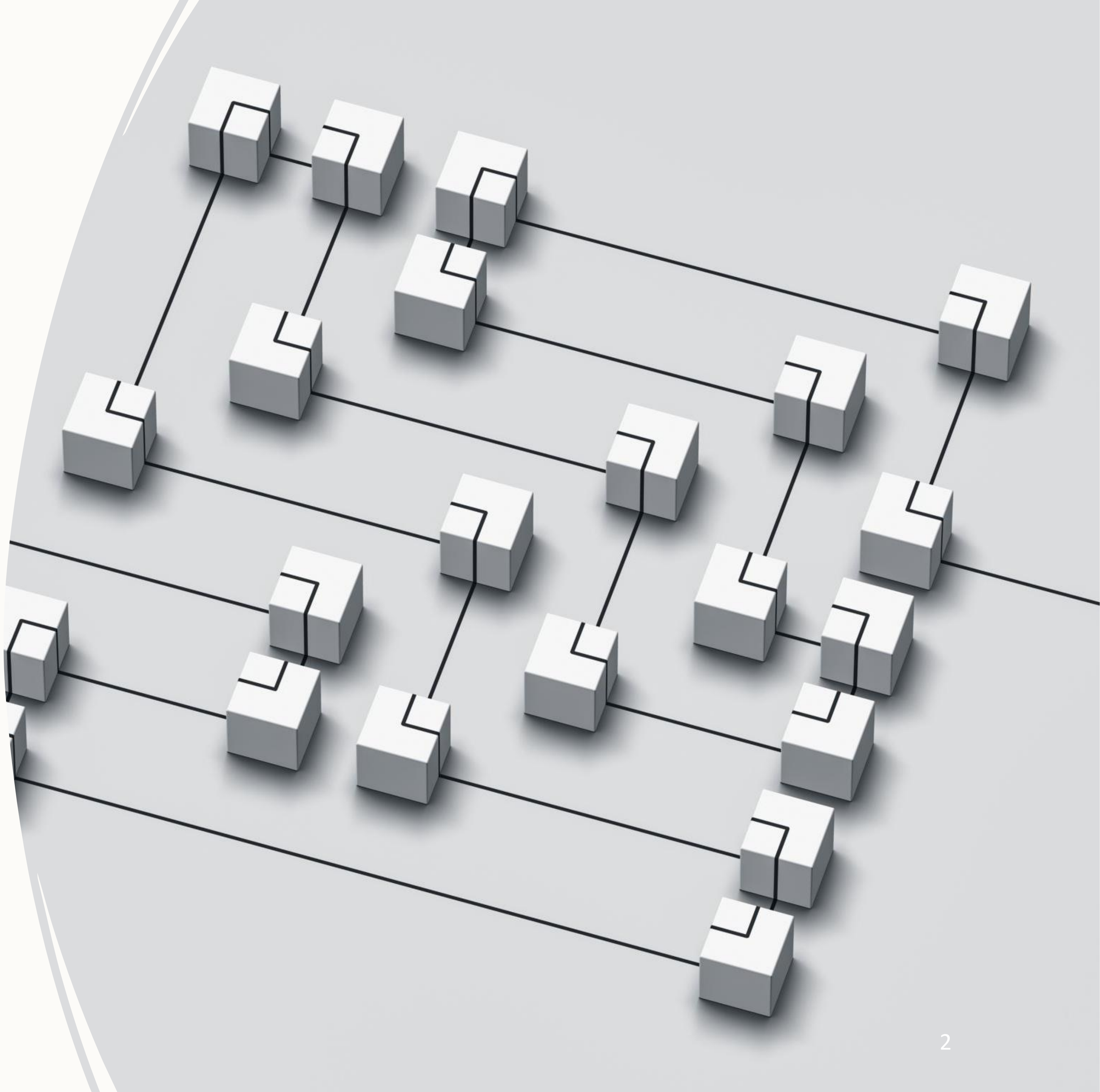
Week 7 Privacy

Learning outcomes

- ➢Perspectives on privacy
  - Dimensions of privacy
  - Threats and principles
  - Trade-offs and rights

- ➢Theories of privacy
  - Definitions and views
  - Solove’s Taxonomy

- ➢Different Opinions on Privacy



Additional Reading

Books

- Chapter 3 of the book Ethics in a Computing Culture (Brinkman & Sanders, 2013)
- Chapter 2 of Sara Baase (2013), A gift of fire: social, legal, and ethical issues of computing technology.

Articles

- I’ve Got Nothing to Hide and Other Misunderstandings of Privacy. Daniel J. Solove, San Diego Law Review, Vol. 44, pp. 745—772, 2007.
- Can You Engineer Privacy? Seda Gurses. Communications of the ACM, Vol. 57, No. 8, pp. 20-23, August 2014.
- Security and Privacy of Augmented Reality Systems. Franziska Roesner, Today Oshi Kohno, and David Molnar. Communications of the ACM, Vol. 57, No. 4, pp.88-96, April 2014.

Articles are available on Moodle.

University of Nottingham
UK | CHINA | MALAYSIA

Perspectives on Privacy

What does privacy mean to different people?

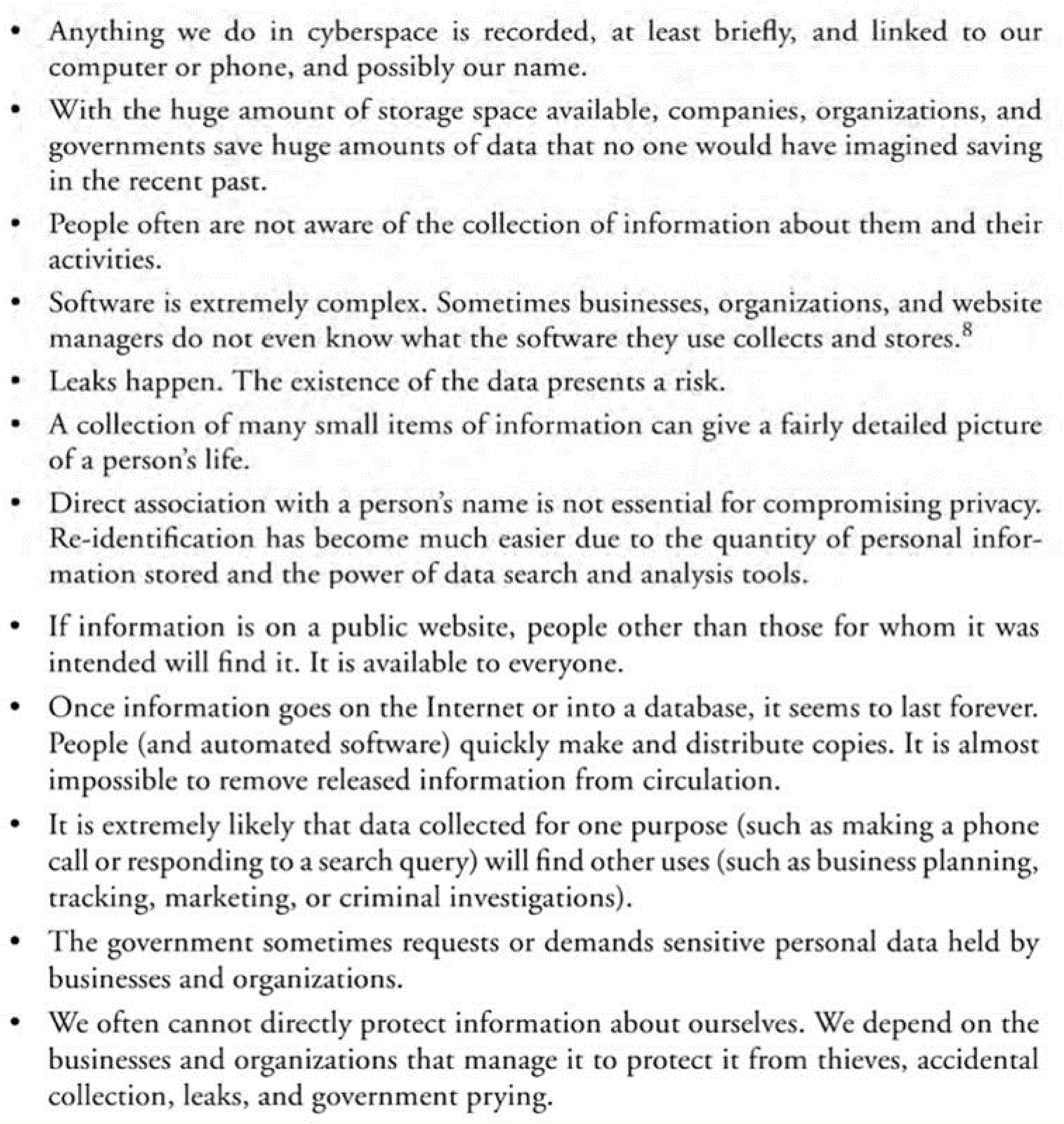
Student assignment – an example

- Professor Blake teaches computer security. In that module, he teaches students how easy it is to intercept e-mail and instant messages. As an assignment, students are required to intercept e-mails and instant messages from the University’s network and post them to the class blog.
- Jessica - one of the students on the module – objects to the assignment on the grounds that it constitutes an invasion of privacy. Professor Blake disagreed for the following two reasons...
  - It is very easy to intercept e-mail, so emails cannot be considered private.
  - The email accounts are on University servers, the contents of which are actually public, so reading them is not a privacy violation.
- **Identify important questions that arise from this scenario.**

Student assignment – some questions

- Expectations of privacy?
- Reasonable to expect e-mail to be private?
- Making information public without knowledge?
- Making information accessible?
- Difference between morality, ethical, and privacy issue?
- Sensibility about the content an the authorship?
- Gaining consent eliminates the problem?
- Secrecy, intrusion, control, surveillance: who is to blame?
- Role of computing professionals?

A summary of privacy risks



- Anything we do in cyberspace is recorded, at least briefly, and linked to our computer or phone, and possibly our name.
- With the huge amount of storage space available, companies, organizations, and governments save huge amounts of data that no one would have imagined saving in the recent past.
- People often are not aware of the collection of information about them and their activities.
- Software is extremely complex. Sometimes businesses, organizations, and website managers do not even know what the software they use collects and stores.[8]
- Leaks happen. The existence of the data presents a risk.
- A collection of many small items of information can give a fairly detailed picture of a person's life.
- Direct association with a person's name is not essential for compromising privacy. Re-identification has become much easier due to the quantity of personal information stored and the power of data search and analysis tools.
- If information is on a public website, people other than those for whom it was intended will find it. It is available to everyone.
- Once information goes on the Internet or into a database, it seems to last forever. People (and automated software) quickly make and distribute copies. It is almost impossible to remove released information from circulation.
- It is extremely likely that data collected for one purpose (such as making a phone call or responding to a search query) will find other uses (such as business planning, tracking, marketing, or criminal investigations).
- The government sometimes requests or demands sensitive personal data held by businesses and organizations.
- We often cannot directly protect information about ourselves. We depend on the businesses and organizations that manage it to protect it from thieves, accidental collection, leaks, and government prying.

Baase (2013), A gift of fire: social, legal, and ethical issues of computing technology, pp. 55-56.

A list of privacy risks & threats

A. Intentional use or release
B. Unauthorised use or release
C. Inadvertent leakage or careless loss
D. Search query data
E. Re-identification of individuals
F. Smartphone data
G. Massive data storage (i.e., the cloud)
H. Complexity of software
I. Surveillance and recognition
J. Unintended use
K. Difficult to control or protect (*e.g. autonomous systems such as AI*).

Baase (2013), A gift of fire: social, legal, and ethical issues of computing technology, pp. 55-56.

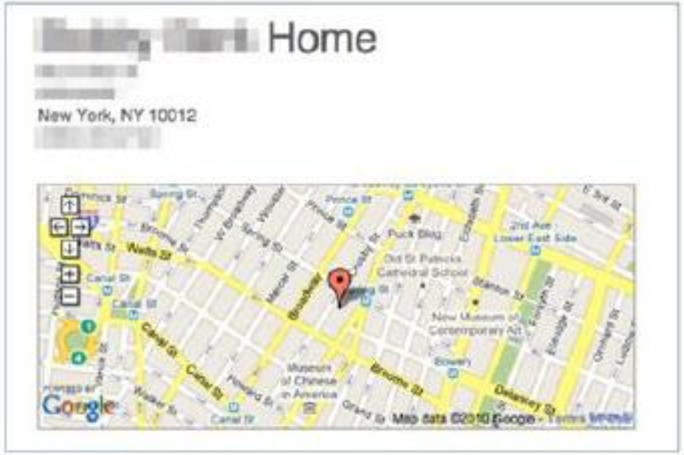
(A) Intentional Use or Release

PLEASE ROB ME
Raising awareness about over-sharing
Check out our guest blog post on the CDT website.

Hey, do you have a Twitter account? Have you ever noticed those messages in which people tell you where they are? Pretty annoying, eh_ Well, they're actually also potentially pretty dangerous. We're about to tell you why.

Don't get us wrong, we love the whole location-aware thing. The information is very interesting and can be used to create some pretty awesome applications. However, the way in which people are stimulated to participate in sharing this information, is less awesome. Services like Foursquare allow you to fulfill some primeval urge to colonize the planet. A part of that is letting everyone know you own that specific spot… You get to tell where you are and if you're there first, it's yours.

(*website no longer available)*



Foursquare

(C) Inadvertent Leakage or Careless Loss

•©IRE

•HACK BRIEF: YAHOO BREACH

•IIITS HALF A BILLION USERS

https://www.wired.com/2016/09/hack-brief-yahoo-looks-set-confirm-big-old-data-breach/

The Hack

Yahoo chief information security officer Bob Lord wrote in a statement on Yahoo's Tumblr site that the company had been the victim of a hacker intrusion in late 2014 that accessed at least 500 million accounts and retrieved a bounty of information, including user names, email addresses, telephone numbers, dates of birth. security questions and answers, arid passwords—albeit passwords protected by cryptographic hashing. "We have confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor," Lord writes. "An increasingly connected world has come with increasingly sophisticated threats. industry, government and users are constantly in the crosshairs of adversaries,"

Earlier Thursday Recode reported that Yahoo was expected to confirm a data breach that affects hundreds of millions of users. The site referenced a collection Of 200 million of Yahoo's user names, birthdates, email addresses and hashed passwords that's been offered for sale on the dark web marketplace The Real Deal since at least August. In June, WIRED interviewed the hacker known as Peace or Peace of Mind, who's behind the data sale on Real Deal. Peace claimed to be a former member of a team of Russian cybercriminal hackers. He or she later sent WIRED a sample of the purported Yahoo data, but when WIRED sent test messages to the email addresses, half of them were invalid.

But Yahoo's announcement suggests a different breach. The timing, scale and Yahoo's claim of state involvement indicate it may be distinct from the one that surfaced data on the dark web and could also be significantly more serious.

(E) Re-identification of Individuals

- Data can be anonymized by removing directly identifiable fields such as name, personal ID, or mobile phone number.

- However, often individuals may be re-identifiable by secondary data such as postal code (zip code), data of birth, and gender.
  https://www.isaca.org/resources/news-and-trends/industry-news/2024/reidentifying-the-anonymized-ethical-hacking-challenges-in-ai-data-training

- Indeed, for individuals with infrequent characteristics, they may be identified even from other characteristics by linking data sets.
  https://www.fuqua.duke.edu/duke-fuqua-insights/jiaming-xu-does-data-anonymization-really-hide-your-identity

- Therefore, the anonymization process requires careful consideration.

(F) Smart Phone Data

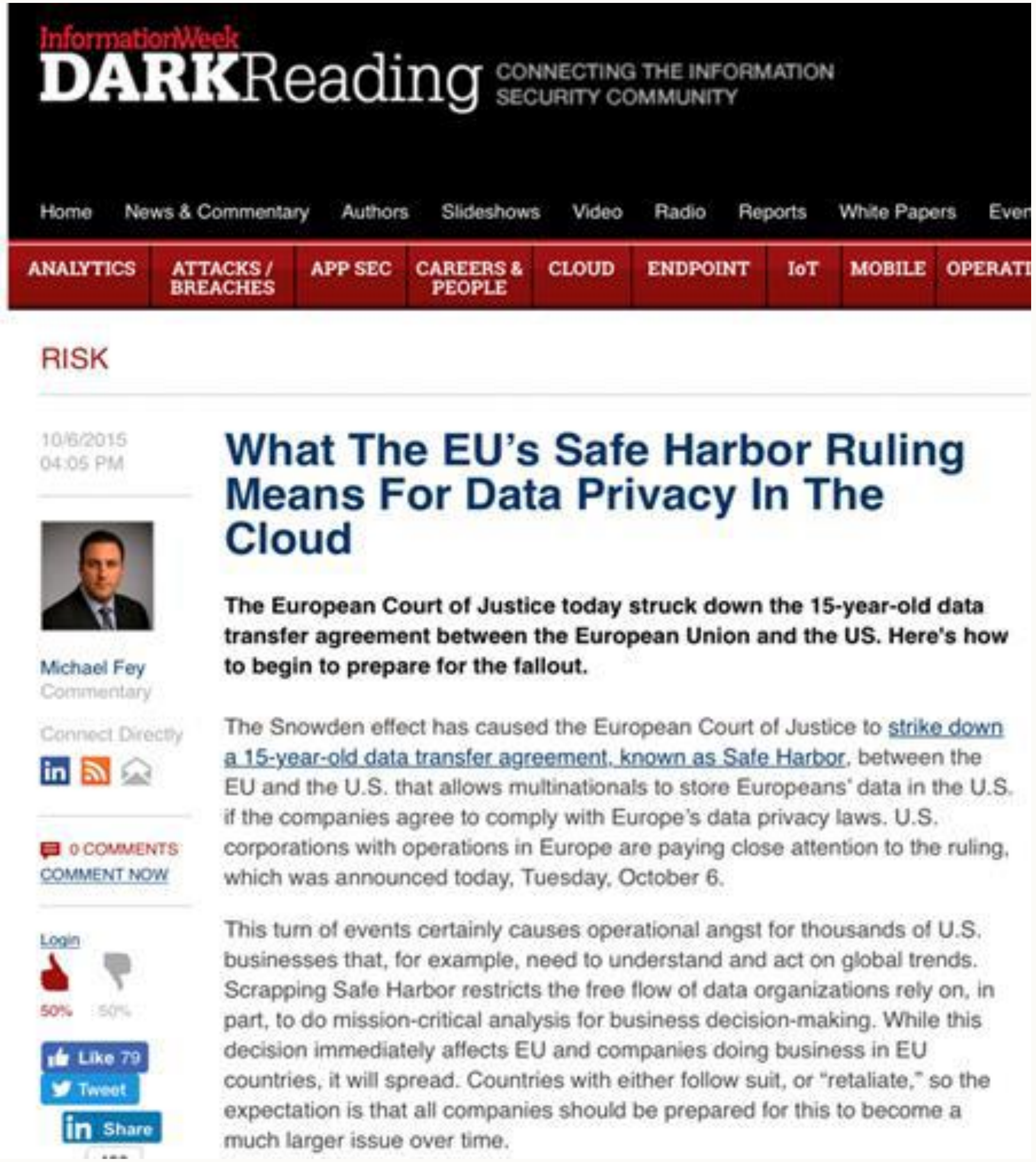
Report: Porsche Opts for CarPlay Over Android Auto (October 2015)

Porsche has reportedly opted for Apple's rival CarPlay system over Android Auto due to privacy concerns.

- Porsche's 2017 911 sports car will have a number of new features, but Android Auto won't be one of them.
- That's because automakers that sign up to install Google's car infotainment system are required to collect and send back certain data to the company -- such as a vehicle's speed, RPMs and coolant temperatures, according to Motor Trend… That's information that Porsche isn't keen on sharing. In comparison, Apple CarPlay only checks to see whether a vehicle is in motion.

https://www.pcmag.com/news/report-porsche-opts-for-carplay-over-android-auto.

(G) Massive Data Storage (the Cloud)



RISK

10/6/2015
04:05 PM

Michael Fey
Commentary

0 COMMENTS
COMMENT NOW

What The EU's Safe Harbor Ruling Means For Data Privacy In The Cloud

The European Court of Justice today struck down the 15-year-old data transfer agreement between the European Union and the US. Here's how to begin to prepare for the fallout.

The Snowden effect has caused the European Court of Justice to strike down a 15-year-old data transfer agreement, known as Safe Harbor, between the EU and the U.S. that allows multinationals to store Europeans' data in the U.S. if the companies agree to comply with Europe's data privacy laws. U.S. corporations with operations in Europe are paying close attention to the ruling, which was announced today, Tuesday, October 6.

This turn of events certainly causes operational angst for thousands of U.S. businesses that, for example, need to understand and act on global trends. Scrapping Safe Harbor restricts the free flow of data organizations rely on, in part, to do mission-critical analysis for business decision-making. While this decision immediately affects EU and companies doing business in EU countries, it will spread. Countries with either follow suit, or "retaliate," so the expectation is that all companies should be prepared for this to become a much larger issue over time.

http://www.darkreading.com/risk/what-the-eus-safe-harbor-ruling-means-for-data-privacy-in-the-cloud/a/d-id/1322512.

October 2015

Privacy Risks: Homework

Find other examples of privacy risks under each category A to K.

University of
Nottingham
UK | CHINA | MALAYSIA

Theories of Privacy

What do we mean by privacy?
Warren & Brandeis’s argument
Solove’s Taxonomy

Definitions of Privacy

- Three dictionary definitions of privacy:

  1. Seclusion (*being set apart, or out of view*)
  2. Secrecy or concealment
  3. Freedom from intrusion

Scenario: You post your phone number on an online forum and shortly afterwards you start to receive harassing calls.

- Question: Harassing calls are immoral, but do they violate your privacy?
  - If privacy is seclusion or secrecy, then perhaps not - it was your responsibility to keep your phone number secret.
  - If privacy is freedom from intrusion, then harassing calls are invading your privacy.

The Right to Privacy

> “Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual… the right “to be let alone”. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house tops.”

The Right to Privacy. Samuel. V. Warren and Louis D. Brandeis. Harvard Law Review, Vol. 4. No. 5, (Dec. 15, 1890), pp. 193-220.

https://www.jstor.org/stable/1321160

The Right to Privacy

UN Declaration of Human Rights

Article 12: Right to privacy

You have the right to protection if someone tried to harm your good name, enter your home without permission or interfere with your correspondence.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

UNDHR is signed by most countries including China, USA and UK.

https://www.ohchr.org/en/universal-declaration-of-human-rights/illustrated-universal-declaration-human-rights

Warren & Brandeis’s argument

- Opponents state that “privacy” derives from other rights:
  - **Implicit contract**:

    e.g., a department store that video records you in the changing rooms is violating an implicit contract with you not to record, rather than violating a separate right to privacy.
  - **Intellectual property**:

    e.g., your friend posts an embarrassing picture of you on WeChat and tags you – this violates your intellectual property rights to your pictures of yourself and not a violation of your privacy.
- Warren & Brandeis debunked this; i.e., “Privacy” is not protected by contracts and intellectual property.
  - Using counter-argument of private letters published against wishes of the author to another person. The private letters are not covered by contract or intellectual property protection.

Solove’s Taxonomy of Privacy

“Using the traditional method – seeking to define privacy’s essence or core characteristics ... [results in] endless disputes over what falls inside or outside the domain of privacy”

"I've Got Nothing to Hide" and Other Misunderstandings of Privacy – Daniel J. Solove

Bottom Up approach:

- Impossible to adequately define “privacy” in a “top-down” way that covers all instances.
- Identify instances of clear violations of privacy, and build up from there: *a hierarchical Taxonomy* of Privacy.

Solove's Taxonomy of Privacy

Four categories of privacy violation:

- Information collection
- Information processing
- Information dissemination
- Invasion

Let's look at each in turn.

Information Collection

- **Surveillance**: Monitoring continuously, usually via audio, visual, or computer technology.

- **Interrogation**: “Pressuring... individuals to divulge information”

The 2017 model of the Porsche 911 will come with Apple CarPlay support. Photo: Simon Maina/AFP/Getty Images

Information Processing

- **Aggregation**: Collecting many small pieces of information about a person and linking them together, to create new information.

- **Identification**: “Connecting information to individuals”.

- **Insecurity**: Inadequately safeguarding collections of personal data against theft.

- **Secondary Use**: Using data that people willingly gave for one purpose for some other purpose they did not approve.

- **Exclusion**: Failing to notify individuals that their data is being collected, or failing to provide a way for individuals to view or correct such data.

PLEASE ROB ME
Raising awareness about over-sharing
Check out our guest blog post on the CDT website.

Information Dissemination

- **Breach of Confidentiality**: Breaking a contractual … duty to keep someone else’s information private.
- **Disclosure**: Publishing private, but true, information in a way that damages the reputation of the subject.
- **Exposure**: Publicly displaying certain physical or emotional attributes of another that are normally considered private, especially if such as display is humiliating or embarrassing.
- **Increased Accessibility**: Making records that are technically available to the public easier to access.
- **Blackmail**: Exerting power over another by threatening to reveal damaging information about that person.
- **Appropriation**: Using someone else’s identity for one’s own ends.
- **Distortion**: “Manipulat[ing] ... the way a person is perceived or judged by others” .

mugshots.com

Invasion

- Intrusion: Communicating with people in a way that disturbs their peace or makes them feel uncomfortable.
    - E.g. Phishing: a cybercrime that uses fake emails, websites, or messages to trick people into sharing personal or financial data.

- Decisional Interference: Intruding into an individual's decision making regarding their private affairs.
    - Mobile game Pokemon Go tracks user locations and “leads” players to establishments of businesses that paid the company to lead the players there.
      https://privacy.wiki/Pokemon_Go_Mobile_Game

University of Nottingham
UK | CHINA | MALAYSIA

Different Opinions on Privacy

Different Opinions on Privacy

- The ***“Nothing to Hide”*** argument: Richard Posner believes privacy as a social good is greatly overrated.

  http://bigthink.com/videos/judge-richard-posner-privacy

- Juan Enriquez on “*Your Online Life, Permanent as a Tattoo”*

  https://www.ted.com/talks/juan_enriquez_your_online_life_permanent_as_a_tattoo

- Alessandro Acquisti on *“What Will a Future Without Secrets Look Like?”*

  http://https://www.ted.com/talks/alessandro_acquisti_what_will_a_future_without_secrets_look_like

- Glenn Greenwald on *“Why Privacy Matters?”*

  - http://https://www.ted.com/talks/glenn_greenwald_why_privacy_matters