Privacy

Professional Ethics in Computing

Lecture 05

(largely based on material by J Cartlidge)

Teaching Week	Date	*Contents*
2	***26 Sep***	*Lecture 1: Introduction and Administration*
4	***8 Oct***	Lecture 2: Critical Reasoning and Moral Theory 1
5	***15 Oct***	Lecture 3: Critical Reasoning and Moral Theory 2
6	***22 Oct***	Lecture 4: Computing Professionals and Professional Ethics
7	***29 Oct***	Lecture 5: Privacy
8	***5 Nov***	Lecture 6: Intellectual and Intangible Property
9	***12 Nov***	Lecture 7: Critical Thinking
10	***19 Nov***	Lecture 8: Trust, Safety and Reliability
11	***26 Nov***	Lecture 9: How Computing is Changing Who We Are
12	***3 Dec***	Lecture 10: Computing and Vulnerable Groups
13	***10 Dec***	Lecture 11: Autonomous and Pervasive Technologies

1.	Theory	DONE
2.	Professional codes of conduct	DONE
3.	Real World issues	To do

Today…

- Perspectives on privacy
  - Dimensions of privacy
  - Threats and principles
  - Trade-offs and rights
- Theories of privacy
  - Definitions and views
  - Solove's Taxonomy
  - Panopticism
  - Legal

Additional Reading

- Chapter 3 of the book *Ethics in a Computing Culture* (Brinkman & Sanders, 2013)
- *I've Got Nothing to Hide and Other Misunderstandings of Privacy.* Daniel J. Solove, San Diego Law Review, Vol. 44, pp. 745—772, 2007. [on Moodle]
- *Can You Engineer Privacy?* Seda Gurses. Communications of the ACM, Vol. 57, No. 8, pp. 20-23, August 2014. [on Moodle]
- *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. [on Moodle]
- Foucault, Michel. "Panopticism." *Discipline and Punish: The Birth of the Prison.* New York: Vintage, 1977. 195-230. [available online]

"Anything else I should know about the Cybersecurity Law?
[This applies also on Data Protection Law]

Unfortunately, simply understanding the nature of the Cybersecurity Law, by itself, is not sufficient to determine the scope of a company's responsibilities under the law. **It is important to recognize that the Chinese legislative and legal systems are fundamentally different from their American counterparts, and how this fact impacts the law's interpretation and implementation**. Though a full review of the complexities of the Chinese legal system is outside the scope of this blog post, it is worth noting that, as with other laws in China, the text of the Cybersecurity Law (which currently is not available in the form of an official English translation) may not be the best determinant of its purpose or scope. Understanding the government's motivations and regulators' approach to enforcing the law is key, and the best way to develop that understanding is through communicating with regulators and sharing information about best practices with other professionals in the field. **Companies concerned about the Cybersecurity Law therefore should consider getting in touch with local counsel in China in order to gain the most up-to-date overview of the law's scope and requirements**".

By Courtney M. Bowman, Ying Li and Lijuan Hou on May 9, 2017
Posted in Cybersecurity, Data Privacy Laws, International, Privacy Law

Perspectives on Privacy

Scenario: 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

Possible 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?

Information: A summary of 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.

Pretty scary, isn't it!?

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

List of 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

List adapted from Baase (2013), *see previous page*

Does the following reinforce the importance of this module?

HOW MANY OF THESE THREATS HAVE OCCURRED (RECENTLY)?

(A) Intentional Use or Release

Mar 2012

This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's A Wake-Up Call About Facebook Privacy [Update]

BY JOHN BROWNLEE • 3:20 PM, MARCH 30, 2012

This app is meant to all be in good fun, but it's potentially a weapon in the hands of stalkers.

Girls Around Me

Girls Around Me's splash screen (left) and geo-maps interface (right). Lots of girls around the MFA.

The Girls of Girls Around Me. It's doubtful any of these girls even know they are being tracked. Their names and locations have been obscured for privacy reasons.

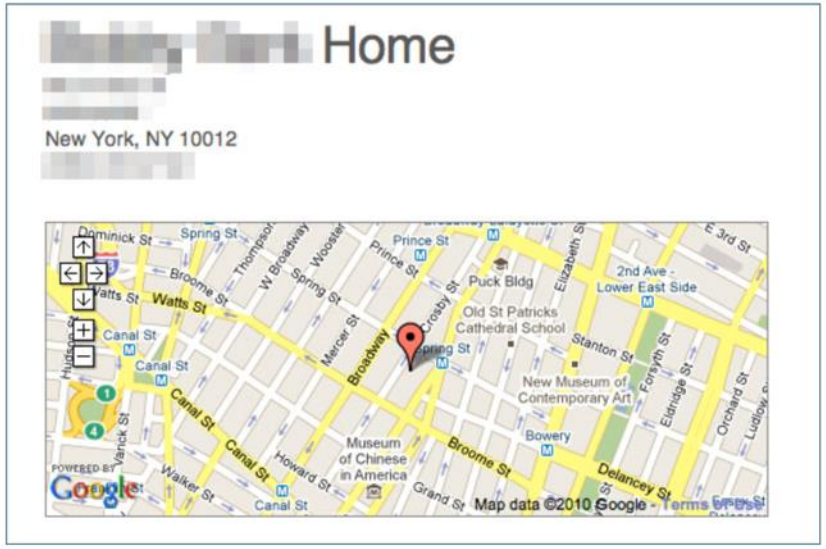
http://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/

2010

Why

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. O, and of course there's badges..



Foursquare

http://pleaserobme.com

(B) Unauthorised Use or Release

Sep 2013

The New York Times

Facebook Removes Dating Ads Featuring Photo of Dead Girl

By VINDU GOEL SEPTEMBER 18, 2013 3:26 PM

Rehtaeh Parsons was the target of cyberbullying because of online circulation of photos taken of her after an alleged gang rape. Andrew Vaughan/The Canadian Press, via Associated Press

Facebook has apologized for dating ads that recently appeared on its service that featured a photo of a Canadian teenager, Rehtaeh Parsons, who hanged herself in April.

Ms. Parsons's case has received much publicity in Canada because she had been the target of cyberbullying because of online circulation of photos taken of her after an alleged gang rape in 2011. Critics said the initial crime was poorly investigated by the police, who recently reopened the case.

http://bits.blogs.nytimes.com/2013/09/18/facebook-removes-dating-ads-featuring-photo-of-dead-girl/

(C) Inadvertent Leakage or Careless Loss

Sep 2016

WIRED

ANDY GREENBERG SECURITY 09.22.16 12:15 PM

HACK BRIEF: YAHOO BREACH HITS HALF A *BILLION* USERS

LISA WERNER/GETTY

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, and 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.

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

21 Privacy 101: Skype Leaks Your Location

MAR 13

Mar 2013

The events of the past week reminded me of a privacy topic I've been meaning to revisit: That voice-over-IP telephony service **Skype** constantly exposes your Internet address to the entire world, and that there are now numerous free and commercial tools that can be used to link Skype user account names to numeric Internet addresses.

The fact that Skype betrays its users' online location information is hardly news. For example, *The Wall Street Journal* and other news outlets warned last year about research showing that it was possible to coax Skype into revealing the IP addresses of individual Skype users. But I believe most Skype users still have no clue about this basic privacy weakness.

A Skype resolver service in action.

What's changed is that over the past year, a number of services have emerged to help snoops and ne'er-do-wells exploit this vulnerability to track and harass others online. For example, an online search for "skype resolver" returns dozens of results that point to services (of variable reliability) that allow users to look up the Internet address of any Skype user, just by supplying the target's Skype account name.

In the above screen shot, we can see one such service being used to display the IP address most recently used by the Skype account "mailen_support" (this particular account belongs to the tech support contact for Mailien, a Russian pharmacy spam affiliate program by the same name).

http://krebsonsecurity.com/2013/03/privacy-101-skype-leaks-your-location/

(D) Search query data

AOL search data leak

Aug 2006

From Wikipedia, the free encyclopedia

The **AOL search data leak** was the release, in August 2006, of detailed search logs by AOL of a large number of AOL users. The release was intentional and intended for research purposes; however, the public release meant that the entire Internet could see the results rather than a select number of academics. AOL did not redact any information, which caused privacy concerns since users could potentially be identified from their searches.

Contents [hide]

Overview [edit]

On August 4, 2006, AOL Research, headed by Dr. Abdur Chowdhury, released a compressed text file on one of its websites containing twenty million search keywords for over 650,000 users over a 3-month period intended for research purposes. AOL deleted the search data on their site by August 7th, but not before it had been mirrored and distributed on the Internet.

AOL did not identify users in the report; however, personally identifiable information was present in many of the queries. As the queries were attributed by AOL to particular user numerically identified accounts, an individual could be identified and matched to their account and search history by such information.[1] *The New York Times* was able to locate an individual from the released and anonymized search records by cross referencing them with phonebook listings.[2] Consequently, the ethical implications of using this data for research are under debate.[3][4]

AOL acknowledged it was a mistake and removed the data; however, the removal was too late. The data was redistributed by others and can still be downloaded from mirror sites.[5][6]

In January 2007, Business 2.0 Magazine on CNNMoney ranked the release of the search data #57 in a segment called "101 Dumbest Moments in Business."[7]

https://en.wikipedia.org/wiki/AOL_search_data_leak

(E) Re-identification of individuals

Aug 2006

Notable users [edit]

Although the searchers were only identified by a numeric ID, some people's search results have become notable due to various reasons.

Thelma Arnold [edit]

Through clues revealed in the search queries, the New York Times successfully uncovered the identities of several searchers. With her permission, they exposed user #4417749 as Thelma Arnold, a 62-year-old widow from Lilburn, Georgia.[9] This privacy breach was widely reported, and led to the resignation of AOL's CTO, Maureen Govern, on August 21, 2006. The media quoted an insider as saying that two employees had been fired: the researcher who released the data, and his immediate supervisor, who reported to Govern.[10][11]

User 927 [edit]

One product of the AOL scandal was the proliferation of blog entries examining the exposed data. Certain users' search logs were identified as humorous, disturbing, or even dangerous.[12][13]

Consumer watchdog website *The Consumerist* posted a blog entry by editor Ben Popken identifying the anonymous user number 927[14] as having an especially bizarre and macabre search history.[15] The blog posting has since been viewed nearly 4,000 times and referenced on a number of other high-profile sites.[16] In addition to sparking the interest of the Internet community, User 927 inspired a theatrical production, written by Katharine Clark Gray in Philadelphia. The play, also named *User 927*, has since been cited on several of the same blogs that originally discovered the real user's existence.[17] As time has passed, more artistic renderings of individual user logs have appeared. A series of movies on the web site Minimovies called "I Love Alaska" puts voice and imagery to User 711391 which the authors have labeled as "an episodic documentary".[18]

https://en.wikipedia.org/wiki/AOL_search_data_leak

The New York Times

A Face Is Exposed for AOL Searcher No. 4417749

Aug 2006

By MICHAEL BARBARO and TOM ZELLER Jr. AUG. 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

http://www.nytimes.com/2006/08/09/technology/09aol.html

May 2008

U are what U seek: new play sparked by AOL search query leak

What kind of person searches for both "pink camellia" and "cut into your ...

NATE ANDERSON - 5/23/2008, 9:38 AM

When AOL released "anonymized" search results from more than 500,000 users back in 2006, the resulting firestorm even blew into the mainstream media, which managed to track down and identify some of the "anonymous" users simply from their search queries. Now, two years later, a seedling emerges from those ashes as a Philadelphia theater company launches *USER 927*, a new play based on one user's rather unorthodox set of queries. Ars spoke to writer Katharine Clark Gray about the piece and what led her to create it.

From flowers to forced rape porn

A play about search queries might sound as enjoyable as listening to *Winnie Ille Pu* read entirely in Latin (I speak from experience), but AOL user 927 was no ordinary searcher. The *Consumerist* picked 927's queries from the complete archive and published them online in 2006, which inspired director Michael Alltop to pitch Gray on the idea of doing "a play about it."

http://arstechnica.com/uncategorized/2008/05/uare-what-u-seek-new-play-sparked-by-search-queries/

(F) Smart Phone Data

Jun 2015

TECHNOLOGY

Porsche Picks Apple CarPlay Over Android Auto Due To Privacy Concerns And Google Data Collection

BY **LUKE VILLAPAZ** ON 10/06/15 AT 9:23 AM

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

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.

http://www.ibtimes.com/porsche-picks-apple-carplay-over-android-auto-due-privacy-concerns-google-data-2128769

Data and computer security

Blackphone: privacy-obsessed smartphone aims to broaden its appeal

Oct 2015

Privacy company Silent Circle releases the second version of its phone, created by an encryption expert and a member of Navy Seal Team Six

Sam Thielman in New York

@samthielman

Thursday 1 October 2015 12.30 BST

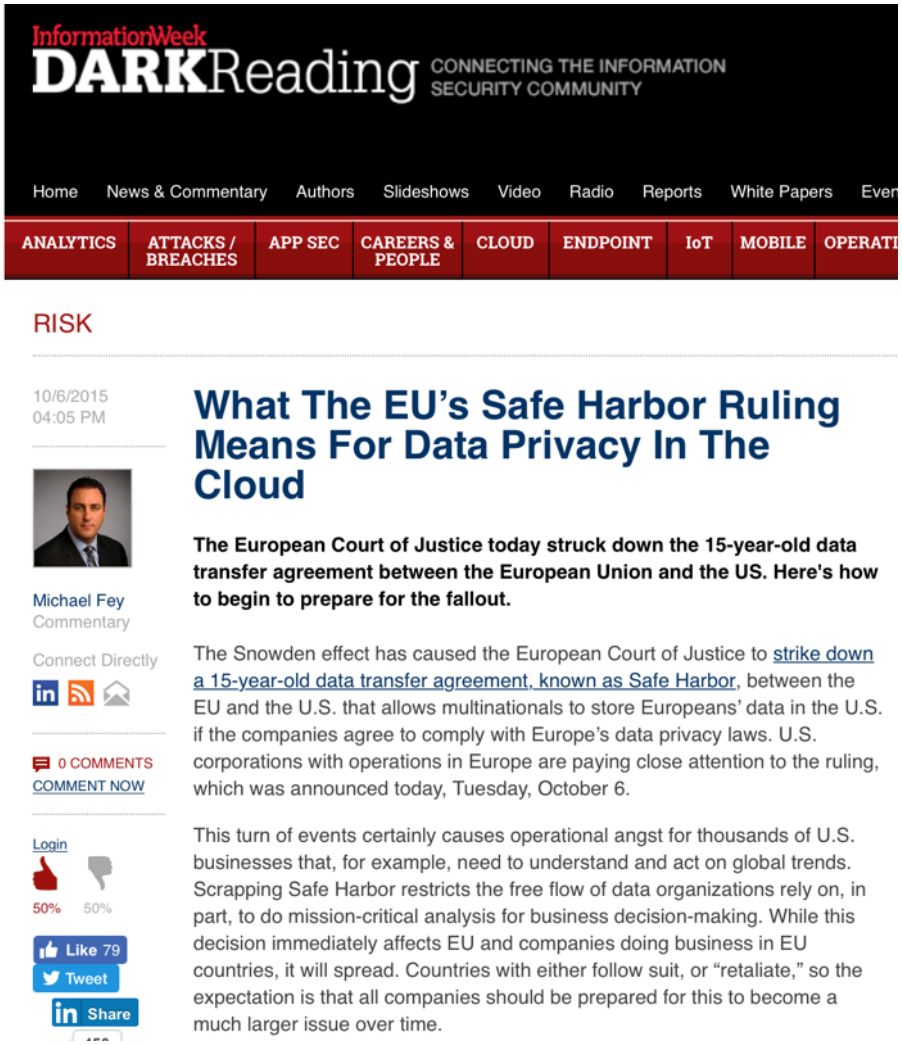
Phil Zimmermann is one of the phone's creators. Photograph: Frantzesco Kangaris for the Guardian

Can you hear me now? Not if you're eavesdropping on a Blackphone. Privacy company Silent Circle has released a second version of its signature handheld, a smartphone designed to quell the data scraping and web tracking that's become such an integral part of the digital economy in the last few years (and whose results might well end up with the NSA, if the Cybersecurity Information Sharing Act passes)

http://www.theguardian.com/world/2015/oct/01/blackphone-release-data-protection-privacy-surveillance

(G) Massive Data Storage (the Cloud)

Jun 2015



InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Even

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERATI

RISK

10/6/2015
04:05 PM

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.

Michael Fey
Commentary

Connect Directly

0 COMMENTS
COMMENT NOW

Login

50% 50%

Like 79
Tweet
Share

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

iCloud leaks of celebrity photos

Aug 2014

From Wikipedia, the free encyclopedia

On August 31, 2014, a collection of almost 500 private pictures of various celebrities, mostly women, and with many containing nudity, were posted on the imageboard 4chan, and later disseminated by other users on websites and social networks such as Imgur and Reddit. The images were believed to have been obtained via a breach of Apple's cloud services suite iCloud,[1][2][3] but it later turned out that the hackers could have taken advantage of a security issue in the iCloud API which allowed them to make unlimited attempts at guessing victims' passwords.[4][5]

The event, which media outlets and Internet users referred to under names such as "**The Fappening**" (a portmanteau of the words "fap"—a slang term for masturbation—and the word "happening"[6][7][8]) and "**Celebgate**", was met with a varied reaction from the media and fellow celebrities. Critics felt that the distribution of the images was a major invasion of privacy for their subjects, while some of the allegedly depicted subjects questioned their authenticity. The leak also prompted increased concern from analysts surrounding the privacy and security of cloud computing services such as iCloud—with a particular emphasis on their use to store sensitive, private information.

https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

(H) Complexity of software

Oct 2013

Google's terms and conditions are less readable than Beowulf

October 17, 2013 4.52pm AEDT

Twelve winters of grief for Hrothgar, for he had clicked 'agree' without reading to the end. Helen Stratton

http://theconversation.com/googles-terms-and-conditions-are-less-readable-than-beowulf-19215

(I) Surveillance and recognition

PRISM (surveillance program)

Jun 2013

From Wikipedia, the free encyclopedia
(Redirected from PRISM surveillance)

"PRISM" redirects here. For other uses, see Prism (disambiguation).

PRISM is a clandestine[1] surveillance program under which the United States National Security Agency (NSA) collects internet communications from at least nine major US internet companies.[2][3][4] Since 2001 the United States government has increased its scope for such surveillance, and so this program was launched in 2007.

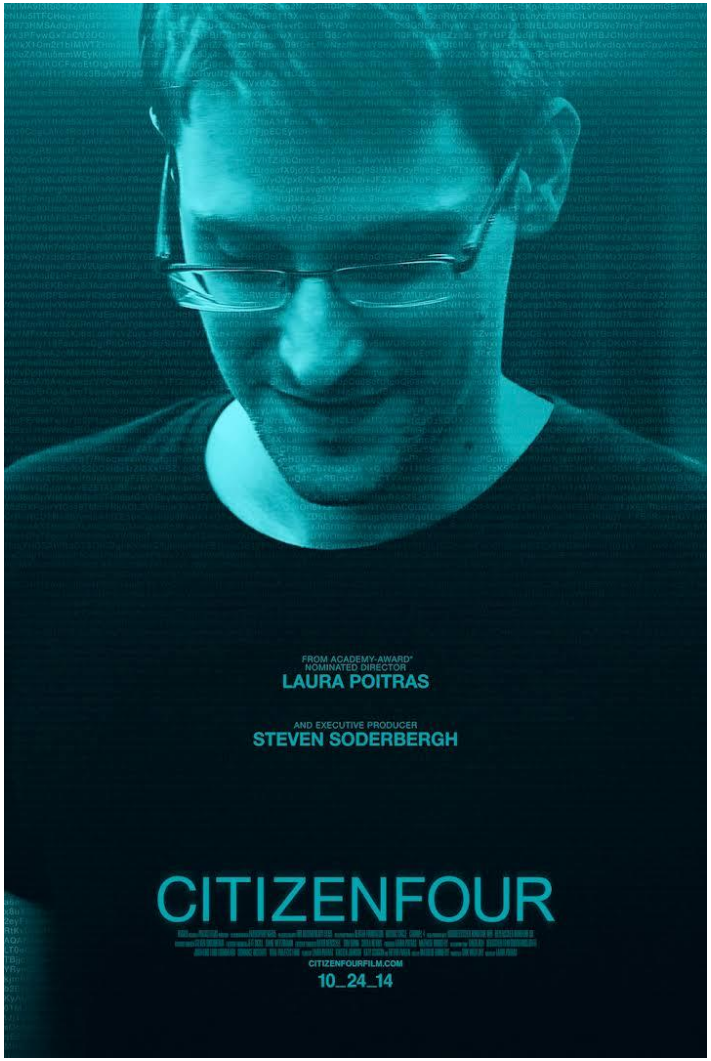
PRISM is a government code name for a data-collection effort known officially by the SIGAD US-984XN.[5][6] The PRISM program collects stored internet communications based on demands made to internet companies such as Google Inc. under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms.[7] The NSA can use these PRISM requests to target communications that were encrypted when they traveled across the internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier,[8][9] and to get data that is easier to handle, among other things.[10]

PRISM began in 2007 in the wake of the passage of the Protect America Act under the Bush Administration.[11][12] The program is operated under the supervision of the U.S. Foreign Intelligence Surveillance Court (FISA Court, or FISC) pursuant to the Foreign Intelligence Surveillance Act (FISA).[13] Its existence was leaked six years later by NSA contractor Edward Snowden, who warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities.[14] The disclosures were published by *The Guardian* and *The Washington Post* on June 6, 2013. Subsequent documents have demonstrated a financial arrangement between NSA's Special Source Operations division (SSO) and PRISM partners in the millions of dollars.[15]

Documents indicate that PRISM is "the number one source of raw intelligence used for NSA analytic reports", and it accounts for 91% of the NSA's internet traffic acquired under FISA section 702 authority."[16][17] The leaked information came to light one day after the revelation that the FISA Court had been ordering a subsidiary of telecommunications company Verizon Communications to turn over to the NSA logs tracking all of its customers' telephone calls.[18][19]

U.S. government officials have disputed some aspects of the *Guardian* and *Washington Post* stories and have defended the program by asserting it cannot be used on domestic targets without a warrant, that it has helped to prevent acts of terrorism, and that it receives independent oversight from the federal government's executive, judicial and legislative branches.[20][21] On June 19, 2013, U.S. President Barack Obama, during a visit to Germany, stated that the NSA's data gathering practices constitute "a circumscribed, narrow system directed at us being able to protect our people."[22]

https://en.wikipedia.org/wiki/PRISM_(surveillance_program)



A good documentary film to watch: ***many*** **privacy issues raised**

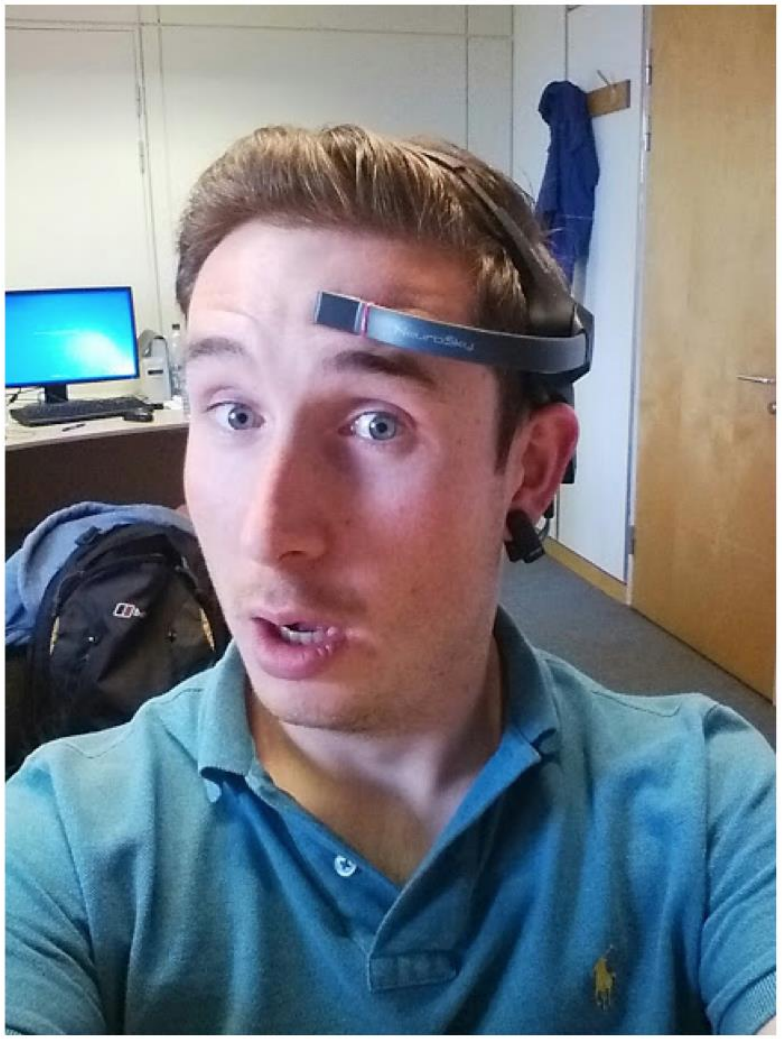
…maybe have a CPU showing?

https://www.youtube.com/watch?v=QSg8N2BGTGw

Interesting discussion: European Court in Brussels, Belgium [1:36:13 – 1:39:55]

(J) Unintended Use

Oct 2016



Would you Trust this researcher with your Data?

(K) Difficult to control or protect

Ongoing …

These are not isolated incidents; personal data threats occur all the time!

SO, THAT'S ALL OF THEM!

Qu: Can you give other examples? What category do they fall in?

Principles About Privacy

- **The Principles**
  - Informed consent (opt out vs. opt in)
  - No invisible information gathering
  - No secondary use
  - No covert data mining, matching, or profiling
  - Only collect as needed
- **Violations in Examples?**
  - Search data
  - PRISM
  - Brain Data
  - AOL
  - PRISM

Principles About Privacy (cont.)

- **The Principles**
  - Accuracy and security
  - Policy for responding to data requests
  - Constitutional protection and laws
  - Right to be forgotten
  - Responsible use of public records
- **Upheld in Examples?**
  - Yahoo
  - PRISM
  - PRISM
  - AOL
  - Girls Around Me / Please Rob Me

Definitions of Privacy

- Three *dictionary* definitions of privacy:
  - Seclusion (being set apart, or out of view)
  - Secrecy or concealment
  - Freedom from intrusion
- **Scenario: You post your phone number on an online forum and shortly afterwards you start to receive harassing calls.**
- **Qu: 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

2 Attempts to Define Privacy

1. "***Right to be left alone***" argument
    1. Freedom from intrusion
    2. Warren & Brandeis
    3. Privacy is a natural right
2. "***I have nothing to hide***" argument
    1. Privacy as concealment
    2. Judge Richard Posner
    3. People do not really value personal 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.

http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

(The Right to Privacy)

Warren & Brandeis's argument

- Opponents state that "*privacy*" derives from other rights:
  - **Implicit contract:** e.g., a department store that videotapes you in the changing rooms is violating an implicit contract with you not to videotape (rather than violating supposed 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 argument of private letters published against wishes of the author (not covered by contract or intellectual property protection)

Privacy as Concealment

*"**As a social good** … **I think privacy is greatly overrated, because privacy basically means concealmen**t. People conceal things in order to fool other people about them. They want to appear healthier than they are, smarter, more honest… [it is] what economists call a superior good; the demand for it rises as people become wealthier. Because it has this instrumental value, you want to control information about yourself; that will enable you to make advantageous transactions personally, professionally, and commercially with other people."*

Judge Richard Posner (2007), Video Interview.
http://bigthink.com/videos/judge-richard-posner-privacy

(Privacy as Concealment)

Posner's argument

- Pre-modern peoples had little or no privacy
  - therefore it is natural to have no privacy
- Contemporary people willing to give up private information in return for convenience or small financial incentives
  - therefore we do not value individual privacy
- Concealment is most useful for criminals, and least useful to honest people
  - therefore, privacy is mostly a social harm, not a social good

Can be use, e.g., to support introduction of the USA PATRIOT Act, 2001, which gave the government the ability to inspect library records without a warrant.

Posner agrees that everyone has a right to conceal their bodies by wearing clothes, etc. But denies a right to conceal personal information except in very limited situations. He argues we should stop using term "privacy" altogether.

SOLOVE'S TAXONOMY OF PRIVACY

Taxonomy of Privacy (Daniel Solove)

“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”

[Solove’s objective / rationale for creating the privacy taxonomy]

"I've Got Nothing to Hide" and Other Misunderstandings of Privacy –

Daniel J. Solove

[Moodle Link]

Solove's Taxonomy of Privacy

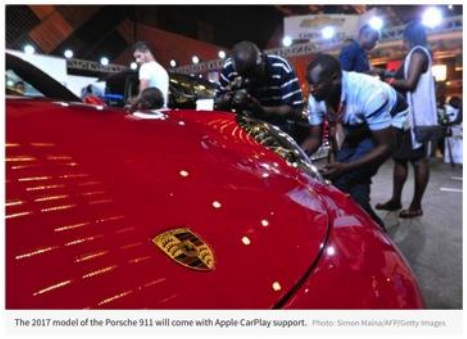
- **Bottom Up approach:**
  - Impossible to adequately define "privacy" in a "top-down" way that covers all instances
  - Identify instances of clear violations of privacy, and build up from there: a hierarchical Taxonomy of Privacy
- **4 categories:**
  - Information collection
  - Information processing
  - Information dissemination
  - Invasion

Solove's Taxonomy of Privacy

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

Solove's Taxonomy of Privacy

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

Qu: Any non-obvious ones?

Solove's Taxonomy of Privacy

Information Dissemination

- **Breach of Confidentiality:** Breaking a contractual or fiduciary 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

Qu: What about these? Any non-obvious ones?

Solove's Taxonomy of Privacy

Invasion

- **Intrusion:** Communicating with people in a way that disturbs their peace or makes them feel uncomfortable

- **Decisional Interference:** Controlling (usually by authority of the government) what one is allowed to do in one's private life

Aggregation & Accessibility

- Both involve processing or disseminating information that is already publicly available
  - **Aggregation:** When analysed, data reveals new facts about a person that she did not expect would be known about her when the original, isolated data was collected. E.g., PleaseRobMe creates a much greater privacy risk than the individual social networking sites (Twitter, Foursquare, Facebook, Flickr, …) do in releasing the data. A robber could do this process manually, but unlikely (too time consuming)
  - **Increased Accessibility:** E.g., in USA, since 1964 (Civil Rights Act) it is usually illegal to reject job applicants based solely on arrest records. One could do this manually by searching local newspapers, but is time consuming and may arouse suspicion. Now a quick Google search will do the job

Disclosure vs Exposure

- **Exposure:** public display of certain highly private aspects of a person's body or emotions (e.g., autopsy images of dead celebrity; "revenge porn" photographs)
- **Disclosure:** Revealing facts, not taboo images (e.g., autobiographical book about extramarital affair with prominent politician)

Solove's main idea: Rather than endlessly debate what is or is not "privacy", we ought to get on with the business of solving privacy problems – i.e., a ***pragmatic approach***

PRIVACY AND SOCIETY

A ***reasonable expectation*** of privacy

- Private life, work and public spaces
  - A ***reasonable expectation*** of privacy (4th Amendment)
  - Whether or not the person whose privacy is infringed actually had a reasonable expectation of privacy in that case.
- New technologies change our expectations of privacy
  - E.g., high-power zoom lens photography on drones: should we expect privacy in our own back garden?
  - E.g., E-mails reside on a 3rd part server: should we expect the same privacy as telephone calls? Should we expect our e-mails to be private?

Panopticism

- “Panopticism” essay by Michel Foucault (1977) explores influence of persistent surveillance on society
- Modern society and the modern prison
- Panopticon concept invented by English Philosopher Jeremy Bentham (1748-1832)

Panoptic Structure: Key Ideas

- Central authority control over some aspects of people's lives
- People are kept in small groups and separated from each other
- Everything is observed by the authority
- A person can never be sure whether or not they are being observed
- Awareness of the possibility of surveillance causes self-discipline (a *chilling effect*)

Chilling Effect

- The term *chilling effect* is used to refer to a situation in which one feels pressure not to do something, even though it is legal to do so, because of fear of prosecution.

Example: Blogs and technologies such as Twitter blur the lines between "journalist" and "citizen", and enable people from different countries to interact. If you are able to be prosecuted under the law of another country (e.g., for libel), there may be a severe chilling effect on free speech.

Different Opinions on Privacy

[Video Links]

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***"

http://www.ted.com/talks/juan_enriquez_how_to_think_about_digital_tattoos

Alessandro Acquisti on "***What Will a Future Without Secrets Look Like***?"

http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters

Glenn Greenwald on "***Why Privacy Matters?***"

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

Legal issues on Data Protection - China

Processing private data

Key principles

Transparency
Lawful basis for processing
Purpose limitation
Data minimisation
Proportionality (scope)
Retention of personal data

Individual rights

Error rectification
Right to deletion/be forgotten
Object to processing
Data portability
Withdraw consent
Object to marketing
Complain to relevant authority

https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

(The documents at that site are copyrighted, OK to view, no copying)

Different (overlapping) interpretations in different countries

To do

- For workshop on *Wednesday*:

  Before

  - Look at the reading materials and video links on Moodle.
  - Prepare one slide presentation before the workshop and hand to the Group Helper. Group Helpers will collate the slides and send to Nikolaj before the workshop.

  - **In workshop**, we will be applying Solove's taxonomy to a real world scenarios, have one presentation for each scenario (3 min) and critical discussion (3 min)

  - **After workshop**, a 400 words report to be submitted by each group to Vladimir by email, deadline Thursday 5 pm.

[END]