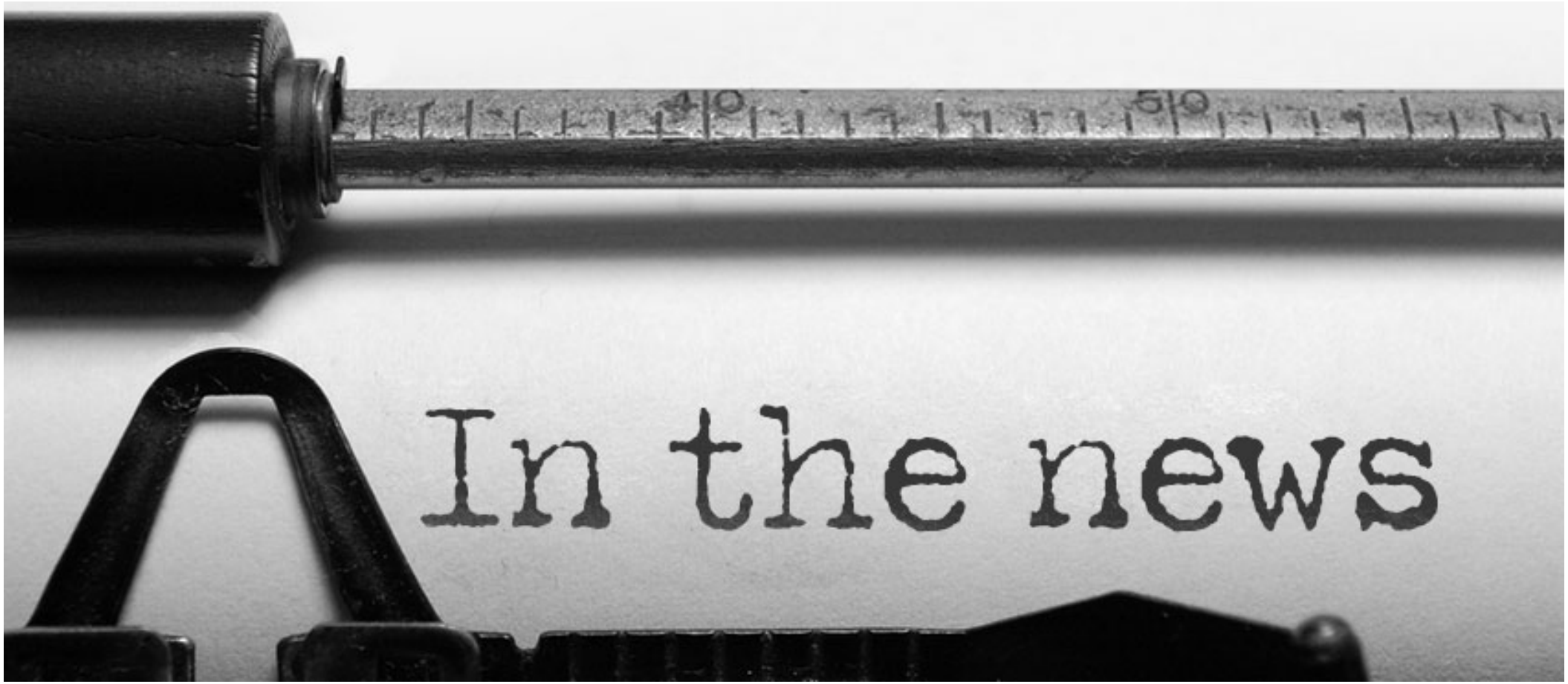
INFO 350

INFO Policy, Law, and Ethics



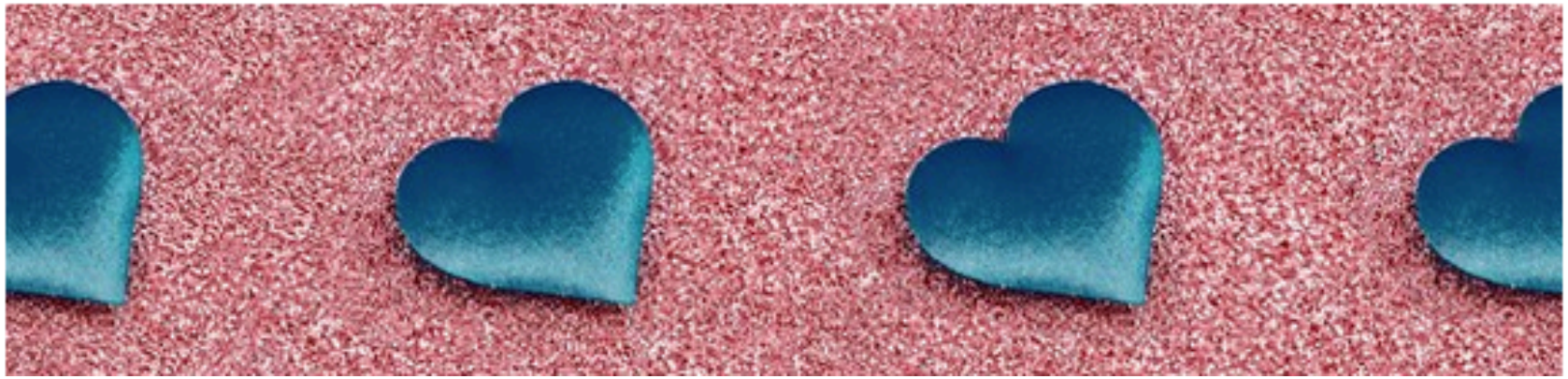
Facebook's Zuckerberg announces privacy overhaul: 'We don't have the strongest reputation'

At annual F8 developer conference, CEO focuses on 'sense of intimacy' and unveils plans for payments tools

- The Facebook founder and chief executive repeatedly broke out in laughter as he announced a product roadmap for his company's new "privacy-focused social platform" at its annual developer conference, F8, in San Jose on Tuesday.
- "Now look, I get that a lot of people aren't sure that we're serious about this," Zuckerberg said, through skittish guffaws. "I know that we don't exactly have the strongest reputation on privacy right now, to put it lightly. But I'm committed to doing this well."

LOUISE MATSAKIS BUSINESS 04.30.19 01:30 PM

FACEBOOK WANTS TO CONNECT YOU WITH YOUR 'SECRET CRUSH'



“Facebook wants to know who you want to sleep with”

- Here’s how it’s supposed to work. If someone adds you to their Secret Crush list, Facebook will send you a notification saying “A friend added you as a secret crush.” If you then pick the same person for *your* list, Facebook will match you together and reveal your names. If the feelings are only one-sided, the unrequited lover’s identity remains secret. The object of their affection is then left to wonder who may have a crush on them, with no way to find out.

- It’s not hard to imagine how Secret Crush could go wrong. You could easily prank or even bully someone by adding them to your crush list under false pretenses. One WIRED staffer who used [something similar] in college reported they and their best friend “spent a full semester fucking with another friend through this service.” But Secret Crush **will likely be great for engagement purposes**. Using Facebook to scroll through baby photos may be a snooze, but who doesn’t want to find out that someone has a crush on them?

In-lecture reflection question – May 2nd

- How would you describe Facebook's business model? How do they make money?
- What are the biggest privacy risks for Facebook users?
- Offer some ideas about how to reduce these risks that would still make Facebook profitable…

Privacy and the Law

US Constitution…on Privacy?

- All US law is based on (or contested by) the constitution.
  - So, where is privacy in the constitution?
- **First Amendment:** Association without monitoring, anonymity and speaking your mind
- **Third Amendment**: Housing soldiers in the home
- **Fourth Amendment**: “Unreasonable searches and seizures…”
- **Fifth Amendment:** Right against self-incrimination
- Also argued from the **9th** and **14th** amendments (enumeration and due process clauses)

The Fourth Amendment

The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

—4th Amendment, U.S. Constitution

The Fourth Amendment

- Sets limits on **government's** rights to search our homes and businesses and seize documents and other personal effects. Requires government provide probable cause.
- Only applies to government – usually law enforcement.
- Two key problems arise from new technologies:
  - The home is now porous. We store data in the cloud. Our devices (phones, IoT…) send out personal data constantly.
  - New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge.

Privacy Law in the United States

- We do have privacy laws
  - **The Privacy Act (1974)–** mainly covers specific government agencies
    - Notably does not affect companies – this was intentional
  - **HIPAA** – healthcare privacy
  - **FERPA** – education privacy
  - Many other laws - banking, veterans affairs, etc.
  - Consumer protection – the **Federal Trade Commission (FTC)** is probably the strongest enforcer of commercial privacy

- But most of the action has been in Supreme Court decisions…

A brief history of Fourth Amendment law

Telephone

- *Olmstead v. United States* (1928)
- Supreme Court allowed the use of wiretaps on telephone lines without a court order.
- Interpreted the Fourth Amendment to apply only to *physical* intrusion and only to the search or seizure of material things, not conversations.
- Privacy of telecommunications is not assured…

Congress responds (eventually)

- 1934 Communications Act prohibited interception of messages

Supreme Court Decisions and Expectation of Privacy

- *Katz v United States* (1967)
  - **Reasonable Expectation of Privacy**
  - Supreme Court reversed its position in *Olmstead* and ruled that the Fourth Amendment *does* apply to conversations.
  - Court said that the Fourth Amendment protects **people**, not places. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order.
  - This is (probably) the single most important Fourth Amendment privacy decision in Supreme Court history

Supreme Court Decisions and Expectation of Privacy

- *U.S. v. Miller (1976)*
  - **Third party doctrine**
  - Information provided willingly to one party can be shared with government without a warrant.
  - Banking records case: Miller's rights were not violated when a third party - his bank - transmitted information that he had entrusted them with to the government.
  - Later applied to telecommunications – i.e. cell phone co.s
  - Dramatic blow to informational privacy.

Supreme Court Decisions and Expectation of Privacy

- *U.S. v. Jones (2012)*
  - Court ruled that a GPS device surreptitiously hidden on a car and used for tracking was a “trespass”
    - Notably – court found that Jones *did not* have an expectation of privacy (driving on public streets), so sort of upholds *Katz*.
    - Upheld lower court’s ruling "prolonged surveillance generates individual pieces of information that constitute a Fourth Amendment search when aggregated."
  - **Five justices appeared to be poised to reconsider the "expectation of privacy" doctrine from Katz as not sufficient.**

Supreme Court Decisions and Expectation of Privacy

- *Riley v. California (2014)*
  - **Cell phone privacy**
  - Warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional.
  - "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." –*Justice Roberts*

Supreme Court Decisions and Expectation of Privacy

- *Carpenter v. United States (2018)*
  - **Cell phone records privacy**
  - Cell site records access constitutes a fourth amendment search. Extends *Riley* and seems to chip away at *Miller* and third party doctrine, at least for cell phones.
  - "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."

Foreign Intelligence Surveillance Act

- 1978: FISA provides judicial and congressional oversight of covert surveillance of foreign governments and agents
- Allows electronic surveillance of foreign nationals for up to one year without a court order
- Amended in 2007 to allow government to wiretap communications to/from foreign countries without oversight by FISA Court

PRISM Program

- Documents provided by Edward Snowden revealed NSA had obtained access to servers at Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL, and Apple
- PRISM program enabled NSA to access email messages and monitor live communications of foreigners outside US
- All companies contacted by the *Guardian* denied knowledge of the PRISM program

Electronic Communications Privacy Act

- Passed by Congress in 1986
- Allows police to attach two kinds of surveillance devices to a suspect's phone line
  - Pen register: displays number being dialed
  - Trap-and-trace device: displays caller's phone number
- Court order needed, but prosecutors do not need to show probable cause
- Allows police to do roving wiretaps (following suspect from phone to phone)

Stored Communications Act

- Part of Electronic Communications Privacy Act
- Government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old
- Advent of cloud computing raises new privacy concerns
- Digital Due Process organization (nearly 50 companies and privacy rights organizations) lobbying Congress to change law

Communications Assistance for Law Enforcement Act (aka CALEA)

- Passed in 1994
- Designed to ensure police can still do wiretapping as digital networks are introduced
- FBI asked for new abilities, such as ability to intercept digits typed by caller after phone call placed
- Federal Communications Commission included these capabilities in its guidelines to phone companies
- Privacy-rights advocates argued that new capabilities went beyond Congress's intent

6.6 USA PATRIOT Act

USA PATRIOT Act

- Provisions
  - Greater authority to monitor communications
  - Greater powers to regulate banks
  - Greater border controls
  - New crimes and penalties for terrorist activity
- Critics say Act undermines 4th Amendment rights
  - Pen registers on Web browsers
  - Roving surveillance
  - Searches and seizures without warrants
  - Warrants issued without need for showing probable cause

National Security Letters

- FBI can collect Internet, business, medical, educational, library, and church/mosque/ synagogue records without showing probable cause
- Issues a National Security Letter stating the records are related to an ongoing investigation; no approval from judge needed
- Gag orders prevent recipients (e.g., libraries) from disclosing receipt
- FBI issued 50,000 National Security Letters a year between 2003 and 2006

Tribune Media Services TMS Reprints

Patriot Act Successes

- Charges against 361 individuals
  - Guilty pleas or convictions for 191 people
  - Shoe-bomber Richard Reid
  - John Walker Lindh
- More than 500 people removed from United States
- Terrorist cells broken up in Buffalo, Seattle, Tampa, and Portland (“the Portland Seven”)

Patriot Act Failure

- March 11, 2004 bombings in Madrid Spain
- FBI makes Brandon Mayfield a suspect
  - Claims partial fingerprint match
  - Conducts electronic surveillance
  - Enters home without revealing search warrant
  - Copies documents and computer hard drives
- Spanish authorities match fingerprint with an Algerian
  - Judge orders Mayfield released
  - FBI apologizes
- Civil rights groups: Mayfield was targeted for his religious beliefs

Patriot Act Renewal

- Nearly all provisions have been made permanent
- Four-year sunset clause on two provisions
  - Roving wiretaps
  - FBI ability to seize records from financial institutions, libraries, doctors, and businesses with approval from secret Foreign Intelligence Surveillance Court

NSA Access to Telephone Records

- Edward Snowden leaked documents to the *Guardian* newspaper
- *Guardian* revealed Foreign Intelligence Surveillance Court had ordered Verizon to provide NSA with all of its telephone metadata for 3-month period in 2013 (date, time, location, and length of call, but not contents of call)
- *Guardian* critique: NSA's mission now "focuses increasingly on domestic communications"
- May 2015: Federal court ruled NSA's program was illegal
- June 2015: Congress passed a reform, called the USA Freedom Act, requiring agencies to obtain a court order before accessing metadata

6.7 Regulation of Public and Private Databases

Genesis of Code of Fair Information Practices

- 1965: Director of Budget asked committee of economists to look at problems caused by decentralization of statistical data across federal agencies
- Committee recommended creation of a National Data Center
- Citizens and legislators expressed concerns about possible abuses of such a system
- Another group formed to draft guidelines for government databases

Code of Fair Information Practices

- No secret databases
- People should have access to personal information in databases
- Organizations cannot change how information is used without consent
- People should be able to correct or amend records
- Database owners, users responsible for reliability of data and preventing misuse

Privacy Act of 1974 Falls Short

- Applies only to government databases
- Only covers records indexed by a personal ID
- No federal employee responsible to enforcing Privacy Act provisions
- Allows agencies to share records with other agencies

Legislation for Private Institutions

- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- Financial Services Modernization Act

Fair Credit Reporting Act

- Promotes accuracy and privacy of information used by credit bureaus
- Major credit bureaus: Equifax, Experian, Trans Union
- Negative information kept only 7 years
- Exceptions
  - Bankruptcies: 10 years
  - Criminal convictions: indefinitely

Fair and Accurate Credit Transactions Act

- Passed in 2004
- Requires three major credit bureaus to provide consumers a free copy of their credit report every 12 months
- Not automatic: consumers must request credit reports
- Provisions to reduce identity theft

Financial Services Modernization Act

- Also called Gramm-Leach-Bliley Act of 1999
- Creates “financial supermarkets” offering banking, insurance, and brokerage services
- Privacy-related provisions
  - Privacy policies must be disclosed to customers
  - Notices must provide an opt-out clause
  - Companies must develop procedures to protect customers’ confidential information

6.8 Data Mining by the Government

Telecommunications Records Database

- Created by National Security Agency after 9/11
- Contains phone call records of tens of millions of Americans
- NSA analyzing calling patterns to detect terrorist networks
- Phone records voluntarily provided by several major telecommunications companies
- *USA Today* revealed existence of database in May 2006
- Several dozen class-action lawsuits filed
- August 2006: Federal judge in Detroit ruled program illegal and unconstitutional
- July 2007: US Court of Appeals overturned ruling, saying plaintiffs did not have standing to bring suit forward

Predictive Policing

- Criminals behave in a predictable way
  - Times of crimes fall into patterns
  - Some areas have higher incidence of crimes
- Predictive policing: use of data mining to deploy police officers to areas where crimes are more likely to occur
- Police in Santa Cruz and Los Angeles saw significant declines in property crime

Potential Harms of Profiling

- Government security agencies supposed to protect nation from harm
- What if an erroneous profile characterizes an innocent citizen as a potential terrorist?
- May be impossible to explain how an algorithm has put someone on the watch list
- US government’s terrorist watch list now contains 1.5 million names
- How can innocent people clear their names?

Other Challenges to Privacy Involving Government…

Government Systems

Public Records: Access vs. Privacy:

- Public Records – records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)

- In Washington, The **Public Records Act** (PRA) is especially generous to people seeking information
  - RCW 42.56*

*https://apps.leg.wa.gov/RCW/default.aspx?cite=42.56

Government Systems

- Identity theft using public records is a significant risk
- Data discrimination also a significant risk
- Most public records laws did not anticipate digital access to databases, ease of publication, sharing.
  - Government agencies may lack skills and resources to protect data and prevent predation by information businesses (WA has a Chief Privacy Officer now)
- How should we control access to sensitive public records?
  - Balance legitimate desire for transparency with privacy?