DSci529: Security and Privacy In Informatics

Course Introduction

Prof. Clifford Neuman

Lecture 1
15 Jan 2021
Online

Course Identification

- DSci 529
  - Information Privacy
  - 4.0 units
- Class meeting schedule
  - Noon to 3:20PM Friday's
  - Online (and if we do transition to Hybrid, OHE100C)
- Class communication
  - bcn@isi.edu (for now)

General Course Information

- Professor office hours
  - Monday 1PM to 2:30-4:30PM in RTH-512
  - Other times by appointment
    Primary office in MDR at Information Sciences Institute
  - E-mail: bcn@isi.edu

- TA/Grader for the class
  - T.B.D.
  - Office Hours TBD
  - Email:

Guidelines for Students

- Class will be primarily lectures & individual study
- Student deliverables
  - Homework assignments
  - Spontaneous class participation
  - Individual project presentation
  - Midterm exam
  - Final exam
- Read the assigned readings before class!
  - Some readings assigned by e-mail as late as the day before lecture (if there is breaking news)
  - Responsible for content of assigned reading
  - Quizzes heavily focused on assigned reading

Guidelines for Students

- All assignments are to be submitted individually
  - Help each other understand concepts
  - Help each other understand assignments
  - Work should reflect your own efforts
- Academic integrity is taken very seriously
  - Libraries are a resource for USC academic standards

Grading Schema

Final: 25%
Mid-Term: 20%
Presentation: 25%
Current Event Presentations: 5%
Class Participation: 10%
Homework Assignments: 15%

Total 100%

Letter Grade Assignment

- A letter grade (or number on a 4 point scale) will be assigned for each assignment, project, or exam.
- The individual assignment scores are based on overall class performance (i.e. they may be curved) but I reserve the right to assign a higher average grade if in my opinion most students demonstrate solid understanding of the material.
- Course grade is determined by weighted calculation from the component grades and is not curved.

Privacy Course Multi-Context

- For security practitioners
  - Understand public policy and legal landscape
  - Understand the purpose and ethics behind privacy
- For data scientists and informaticists
  - Understand implications of your craft for privacy
  - Understand public policy and **changing** legal landscape
- For policy wonks
  - Understand the technical landscape
    - What is possible, what is not
  - Both in terms of protecting and destroying privacy
- From those approaching from the legal perspective
  - What is technically possible

Questions on Course Structure

Course Outline

- Overview of Security and Privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- Reasonable expectation of privacy
- Big Data – Technology and Privacy
- AI and Bias
- The Internet of Things and Security and Privacy
- Social Networks and the use of our Data
- Access to Data by Governments - Privacy in a Pandemic
- Privacy Regulation - GDPR, CCPA, CPRA
- Influence of Social Media – Free Speech – Disinformation
- CryptoCurrency - TOR - Privacy Preserving Technologies

What is Privacy?

- **Privacy is about Personally Identifiable Information**
  - **I may use the term sensitive information in discussions**
- **It is primarily a policy issue**
  - **Policy as a system issue**
    - **Specifying what the system should allow**
  - **Policy as in public policy**
    - **Same idea but less precise and must be mapped**

Privacy and Security

- **Privacy is a Security Issue**
  - **Security is needed to implement the policy**
  - **Compromise of the security of sensitive information compromises privacy.**
- **Do we trade privacy for Security**
  - **Franklin – "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither."**
  - **Security both depends on privacy, and can be improved by doing away with privacy.**
  - **The issue is private from whom**
    - **The policy issue again, but we know that our lack of security today stems from the inability to technically solve this policy problem.**

Security v. Privacy

- **Sometimes conflicting**
  - **Many security technologies depend on identification.**
  - **Many approaches to privacy depend on hiding ones identity.**
- **Sometime supportive**
  - **Privacy depends on protecting PII (personally identifiable information).**
  - **Poor security makes it more difficult to protect such information.**

Security and Privacy in The News

(Discussion by students):

Privacy in the News (Similar ideas keep resurfacing)

New York State's anti-encryption bill would force phone makers to add a backdoor -*By David Curry — January 14, 2016*

- **Smartphones sold inside New York might be less safe than the rest of the country, if a new encryption bill is passed in the state. The bill would force manufacturers or operating system providers to decrypt and unlock smartphones for law enforcement and other authorities, creating a backdoor to surpass the encryption.**

- **Introduced earlier this year, the bill would penalize manufacturers $2,500 for every device that does not comply with the law. New York State Assembly members who created the bill claim the it is in the best interests of New York State residents, citing terrorists and criminals who use encryption to avoid law enforcement as ample reason for the bill to be passed.**

- **"The fact is that, although the new software may enhance privacy for some users, it severely hampers law enforcement's ability to aid victims," notes on the bill say. "All of the evidence contained in smartphones and similar devices will be lost to law enforcement, so long as the criminals take the precaution of protecting their devices with passcodes. Of course they will do so. Simply stated, passcode-protected devices render lawful court orders meaningless and encourage criminals to act with impunity."**

California Bill Seeks Phone Crypto Backdoor

Written by Dennis Fisher on January 21, 2016 in Device Security, Privacy

- A week after a New York legislator introduced a bill that would require smartphone vendors to be able to decrypt users' phones on demand from law enforcement, a California bill with the same intent has been introduced in that state's assembly. On Wednesday, California Assemblyman Jim Cooper submitted a bill that has remarkably similar language to the New York measure and would require that device manufacturers and operating system vendors such as Apple, Samsung, and Google be able to decrypt users' devices. The law would apply to phones sold in California beginning Jan. 1, 2017. "This bill would require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or operating system vendor," the bill says.

- Like the New York bill, Cooper's measure would provide for a fine of $2,500 for each device that doesn't comply. However, the California bill isn't aimed at stopping terrorism, as the New York one ostensibly is. Cooper's bill is designed to address the problem of human trafficking, which the legislator and law enforcement officials say is a major problem in the state and almost always is accomplished through the use of smartphones. "You can get a warrant for pretty much anything and everything, but not for an iPhone or an iPad. That's just mind-boggling," Cooper, a former law enforcement officer, said during a press conference.

- "Ninety-nine percent of the public will never have their phone searched with a court order. Hopefully with this legislation we can do something about it and take it back and put the responsibility back on the tech industry." The California bill, like the New York one, could set up another battle in the long-running war between technology vendors and law enforcement agencies over the use of backdoors for encryption. Recent iPhones and Android devices have device encryption enabled by default and the vendors have told law enforcement agencies that they do not hold the encryption keys and can't decrypt users' devices, even with a court order. Privacy advocates and security experts have said consistently that any backdoor or key escrow system for encryption schemes will weaken them and make them targets for attackers of all stripes.

New York Times, July 23rd 2019

Barr Revives Encryption Debate, Calling on Tech Firms to Allow for Law Enforcement

The attorney general, reopening the conversation on security vs. privacy, said that encryption and other measures effectively turned devices into "law-free zones."

Previous Discussion

- **Suppose other countries demanded the same**
  - **They do**
  - **How can we judge them on a different basis than we judge ourselves.**
- **What are the procedures for utilizing the investigative procedures?**
  - **Can criminals exploit these backdoors**
  - **What about “insiders”**
- **If encryption is outlawed only outlaws will have encryption**

This Discussion Occurred BEFORE

NEWS RELEASE

For Immediate Distribution

February 16, 2016

Eileen M. Decker
United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
thom.mrozek@usdoj.gov
(213) 894-6947
www.justice.gov/usao-cdca
@CDCANews

Statement of United States Attorney Eileen M. Decker in Response to Court Order Directing Apple to Assist FBI in Accessing iPhone Used by Syed Rizwan Farook

"Since the terrorist attack in San Bernardino on December 2, 2015, that took the lives of 14 innocent Americans and shattered the lives of numerous families, my office and our law enforcement partners have worked tirelessly to exhaust every investigative lead in the case. We have made a solemn commitment to the victims and their families that we will leave no stone unturned as we gather as much information and evidence as possible. These victims and families deserve nothing less. The application filed today in federal court is another step – a potentially important step – in the process of learning everything we possibly can about the attack in San Bernardino."

Anti-hacking company gets hacked big time …The debate continues

Gary Robbins – San Diego Tribune – January 13 2017

There was a fresh reminder Thursday that virtually everyone is vulnerable to hackers — even a mobile forensics company that's familiar with all of their tricks. The Israeli firm Cellebrite, known for hacking mobile phones for police agencies around the world, confirmed that it suffered a 900GB data breach. That's roughly the amount of data contained in 177,000 emails.

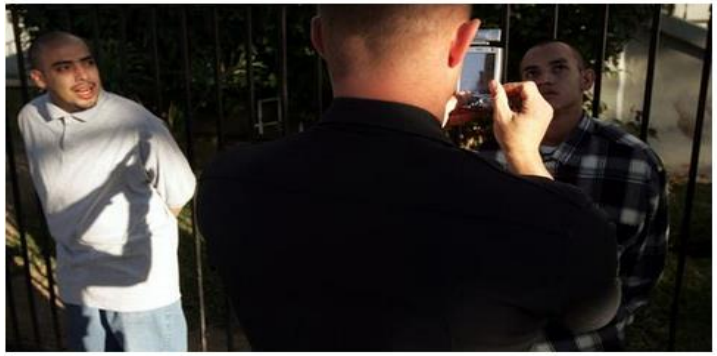
The hacker reportedly shared the data with Motherboard, a website that has been exploring whether Cellebrite's rapid phone-cracking technology has been used in questionable ways. …

"The real implication of the Cellebrite breach is related to the discussion regarding law-enforcement access to data in mobile (and other) devices, and whether systems must provide a technical means to obtain such data," said Clifford Neuman, director of the Center for Computer Systems Security at the University of Southern California.

"Those in favor of such mandated back doors will tell us that we should not be concerned about such capabilities because the data will only be accessible for legitimate law-enforcement purposes. This hack, and the potential unauthorized access to forensic data, highlights that such data might end up accessed for other than such purposes," Neuman said. "Additionally, disclosure of some of Cellebrite's customer organizations tells us who else might obtain such capability to access our protected data."

Disclosure of such technologies

California police would have to disclose the use of more surveillance devices under this proposed law



LAPD Officer Matthew Zeigler uses new facial recognition technology on suspects in a gang-related home invasion arrest on Rampart Boulevard in Los Angeles. (Damon Winter / Los Angeles Times)

By Jazmine Ulloa · Contact Reporter

JANUARY 6, 2017, 12:05 AM | REPORTING FROM SACRAMENTO

In what will likely become another battle over the balance between privacy and public safety, new legislation at the state Capitol would expand the list of electronic surveillance devices that California law enforcement agencies must disclose to the public.

The bill, introduced last month by state Sen. Jerry Hill (D-San Mateo), would require any local law enforcement agency in California that uses surveillance technology to submit a plan to local officials on how it uses the equipment and the information collected. Surveillance plans would have to be presented at an open hearing and would be required to include any facial recognition software, drones or even social media monitoring used by officers.

Data Breaches and Privacy

- **Personal Emails from Sony**
- **Credit card data and SSN's**
- **OPM breach – especially sensitive**
- **Celebrity Photo Hack**
- **Equifax data breach**

Public Records

- **Spokeo, etc**
- **Open Salary laws**
- **Voter records**
- **Implications of legislated data sharing**
  - **Why you might not want to give your phone number to the DMV**

Case Study: Motor Vehicle Records

California Elections Code Section 2194

- (a) The voter registration card information identified in subdivision (a) of Section 6254.4 of the Government Code:
- (1) Shall be confidential and shall not appear on any computer terminal, list, affidavit, duplicate affidavit, or other medium routinely available to the public at the county elections official's office.
- (3) Shall be provided with respect to any voter, subject to the provisions of Sections 2166.5, 2166.7, and 2188, to any candidate for federal, state, or local office, to any committee for or against any initiative or referendum measure for which legal publication is made, and to any person for election, scholarly, journalistic, or political purposes, or for governmental purposes, as determined by the Secretary of State.

Database of 191 million U.S. voters exposed on Internet - Jim Finkle and Dustin Volz – Reuters – Dec 28 2015

- An independent computer security researcher uncovered a database of information on 191 million voters that is exposed on the open Internet due to an incorrectly configured database, he said on Monday.
- The database includes names, addresses, birth dates, party affiliations, phone numbers and emails of voters in all 50 U.S. states and Washington, researcher Chris Vickery said in a phone interview.
- Vickery, a tech support specialist from Austin, Texas, said he found the information while looking for information exposed on the Web in a bid to raise awareness of data leaks.

Case Study: Conflict in Public Policy, Security Policy, and Privacy

- Third parties such as “Nationbuilder” aggregate this data for campaigns, but claim it was not their database that was found.

Could the Same Thing Happen for DMV Data?

DMV Privacy Policy

- The California Department of Motor Vehicles (DMV) is committed to promoting and protecting the privacy rights of individuals as enumerated in Article 1 of the California Constitution, the Information Practices Act of 1977, and other state and federal laws.
- DMV strives in each instance to tell people who provide personal information to DMV the purpose for which the information is collected. DMV tells persons who are asked to provide personal information about the general uses that DMV will make of that information. DMV does this at the time of collection. At the time of collection, DMV will provide information on the authority under which the request is made, the principal uses DMV makes of the information and the possible disclosures DMV is obligated to make to other government agencies and to the public.

Could the Same Thing Happen for DMV Data?

Access is Authorized:

- Request for Record Information (INF 70)
- A driver license/identification card (DL/ID) contains information obtained from an individual's DL/ID application, reportable abstracts of convictions, and reportable accidents. California Vehicle Code (CVC) Section 1808 describes this information as "public record."
- The Request for Record Information (INF 70) (PDF) form is used to request a DL/ID or VR record information on a one-time or occasional basis for:
  An individual's DL/ID or VR record information; other than your own.

Each request is reviewed to determine that the purpose of requesting the information is for a legitimate use and that the appropriate fee has been submitted.

California's new Voter registration

Melanie Mason – Los Angeles Times – October 16 2015

- California has received a lot of attention in recent days for its new voter registration law, which is intended to streamline the process of signing up to vote and encourage more participation in elections. Here's what we know — and don't know yet — about the new law:

- When people go to the DMV to obtain or renew a driver's license, or to get a state identification card, they'll be asked for the usual information in such transactions, such as their name, date of birth and address. They'll also be asked to affirm their eligibility to vote and will be given the choice of opting out of registering at that time. Information about anyone who does not decline registration will be electronically transmitted from the DMV to the secretary of state's office, where citizenship will be verified and names will be added to the voter rolls.

Sensitive data as toxic waste

- Ethical aspects of privacy
  - Do no evil
  - Definition of evil
- Business aspect of privacy
  - Motivations of some privacy initiatives by Apple, Google, etc.
  - Costs of compliance
  - Costs of non-compliance

Social Media

- Sensitive Information
  - Collection of biometric information at Facebook
- Business use of that Information
  - Sale and use of that information on behalf of other parties
- Third party use of that information
  - Facebook denies providing information to NSA
- Cambridge Analytica
- The Mueller Report
- Influence on other elections

Facebook lawsuit calls collection of biometrics data illegal

Justin Lee Biometricupdate.com April 6, 2015

- A new class action suit against Facebook alleges that the social media giant violated its users' privacy rights to acquire the largest privately held database of facial recognition data in the world, according to a report by Courthouse News Service. Lead plaintiff Carlo Licata, represented by attorney Jay Edelson, claims that Facebook first began violating the Illinois Biometric Information Privacy act of 2008 in 2010, in a "purported attempt to make the process of tagging friends easier."
- The lawsuit, recently filed in Cook County Court, relates to Facebook's "tag suggestions" program, which scans users' uploaded pictures and identifies any Facebook friends they may potentially want to tag. The facial recognition technology is taken from Israeli firm Face.com, which Facebook eventually acquired. The lawsuit argues that this method of data mining directly violates users' privacy laws, describing the facial recognition feature as a "brazen disregard for its users' privacy rights," through which Facebook has "secretly amassed the world's largest privately held database of consumer biometrics data."
- The tagging feature works by scanning the faces of Facebook friends in photos and extracting facial feature data to cross-match it against their "faceprint database," or what the company refers to as templates. However, Licata's lawsuit alleges that Facebook "actively conceals" this information from its user base, and "doesn't disclose its wholesale biometrics data collection practices in its privacy policies, nor does it even ask users to acknowledge them" – a practice that is illegal in Illinois.
- According to the Illinois Biometrics Information Privacy Act, it is unlawful to acquire biometric data without first providing the subject with a written disclaimer that details the purpose and length of the data collection, and without the subject's written consent.Additionally, the Federal Trade Commission also backs this same sentiment by suggesting that private companies should provide clear notice of how the technology works, what data they are collecting and for what reasons, and attain consent from the subject, before using biometric data.

Technical Means of Protection

Sensitive data must be protected in multiple places

- When it is in the hands of corporations
  - Traditional IT Security
  - Breaches in the news weekly
- On your devices
  - Encryption, access control
- On the servers you use
  - Access control for your data

Legal Protections

- Privacy policies and enforcement thereof
  - Especially when a company is sold
- Data breach disclosure requirements
  - Vary by state
- EU privacy protections and flow of information
  - GDPR – General Data Protection Regulations
  - Right to be forgotten
- Jurisdictional issues
- Coming Soon – Privacy by Ballot Initiative

Privacy Legislation by Initiative

On '18 ballots, data use could be a top issue

Los Angeles Times 26 Nov 2017 JOHN MYERS john.myers@latimes.com Twitter: @johnmyers

SACRAMENTO — There are pretty strong odds that California voters soon will be hearing a lot about how consumer data are bought and sold — products purchased, medical information, even religious affiliations — and are asked to do something about it.

The man behind the effort to start that conversation is a San Francisco real estate developer who started thinking a lot about the issue after a cocktail party conversation with a tech engineer.

"He said, 'If people just knew how much we knew about them, they'd be really worried,' " Alastair Mactaggart recalled of that chat with the engineer.

Some two years later, Mactaggart is poised to spend enough of his own money to ask Californians to consider a sweeping 2018 ballot measure that could shift the balance of power over data sharing to consumers and punish businesses that don't toe the line.

The initiative that he's introduced, now being circulated for voter signatures, would make two major changes to California law and perhaps set a powerful precedent in the national debate over consumer privacy.

First, the proposal would require significant new disclosure from companies that collect, buy or share the personal information of Californians. It would generally allow consumers to "opt out" once they know who's using their information while banning these large businesses from charging a higher price to those who make that choice.

Second, the ballot measure would give new power to prosecutors and average Californians to file civil lawsuits after a data breach or for selling personal information once a customer says "no" to sharing.

"Consumers would not have to prove that they suffered harm as a result of the violation to be awarded damages," a state fiscal analysis found.

It doesn't take a political insider to realize the business world sees things differently and is preparing to fight back should the initiative qualify for the ballot.

"Very few people are experts on what the consequences would be," said Allan Zaremberg, president of the California Chamber of Commerce. He wonders what would happen to state agencies or schools that share data, or whether a nonprofit credit union might be exempt from the new rules but a commercial bank would not be.

"The economy in California depends on data sharing," Zaremberg said.

Mactaggart, with no real political track record outside of donations to candidates, says he doesn't think the state will be hurt by the change. And he's got a pretty good inkling of what's coming if the privacy proposition makes the ballot.

"This is the wealthiest industry in the world that we're trying to regulate," he said.

A more limited consumer privacy proposal stalled during the final hours of the Legislature's session this year. And it's possible, under relatively new state initiative rules designed to allow for more compromise between lawmakers and activists, that a costly ballot box fight could be avoided.

At the outset, this has all the markings of a huge campaign in an election year where the list of statewide propositions almost certainly will be smaller than the long list of measures in 2016.

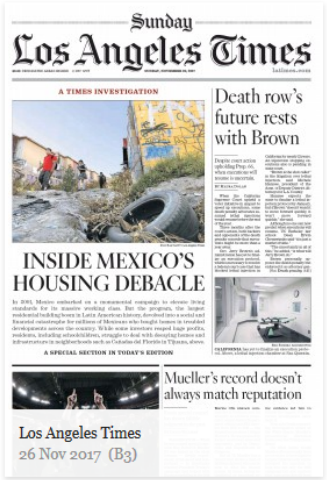
As with so many epic ballot battles, one side will insist that change is long overdue and the other will counter that the change could lead to unintended consequences.

And failing a compromise, the only ones who can sort all of that out, of course, will be the voters.

Write a comment...

Page View Share Comment Save More

Bump it Dump it


Sunday
Los Angeles Times
A TIMES INVESTIGATION
Death row's future rests with Brown
INSIDE MEXICO'S HOUSING DEBACLE
A SPECIAL SECTION IN TODAY'S EDITION
Mueller's record doesn't always match reputation
Los Angeles Times
26 Nov 2017 (B3)

Initially – California Privacy Act

The Act gives "consumers" (defined as natural persons who are California residents) four basic rights in relation to their personal information:

1. the right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;

2. the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in);

3. the right to have a business delete their personal information, with some exceptions;

4. the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

2020 – Ultimately CPRA

On '18 ballots, data use could be a top issue

Los Angeles Times 26 Nov 2017 JOHN MYERS john.myers@latimes.com Twitter: @johnmyers

SACRAMENTO — There are pretty strong odds that California voters soon will be hearing a lot about how consumer data are bought and sold — products purchased, medical information, even religious affiliations — and are asked to do something about it.

The man behind the effort to start that conversation is a San Francisco real estate developer who started thinking a lot about the issue after a cocktail party conversation with a tech engineer.

"He said, 'If people just knew how much we knew about them, they'd be really worried,' " Alastair Mactaggart recalled of that chat with the engineer.

Some two years later, Mactaggart is poised to spend enough of his own money to ask Californians to consider a sweeping 2018 ballot measure that could shift the balance of power over data sharing to consumers and punish businesses that don't toe the line.

The initiative that he's introduced, now being circulated for voter signatures, would make two major changes to California law and perhaps set a powerful precedent in the national debate over consumer privacy.

First, the proposal would require significant new disclosure from companies that collect, buy or share the personal information of Californians. It would generally allow consumers to "opt out" once they know who's using their information while banning these large businesses from charging a higher price to those who make that choice.

Second, the ballot measure would give new power to prosecutors and average Californians to file civil lawsuits after a data breach or for selling personal information once a customer says "no" to sharing.

"Consumers would not have to prove that they suffered harm as a result of the violation to be awarded damages," a state fiscal analysis found.

It doesn't take a political insider to realize the business world sees things differently and is preparing to fight back should the initiative qualify for the ballot.

"Very few people are experts on what the consequences would be," said Allan Zaremberg, president of the California Chamber of Commerce. He wonders what would happen to state agencies or schools that share data, or whether a nonprofit credit union might be exempt from the new rules but a commercial bank would not be.

"The economy in California depends on data sharing," Zaremberg said.

Mactaggart, with no real political track record outside of donations to candidates, says he doesn't think the state will be hurt by the change. And he's got a pretty good inkling of what's coming if the privacy proposition makes the ballot.

"This is the wealthiest industry in the world that we're trying to regulate," he said.

A more limited consumer privacy proposal stalled during the final hours of the Legislature's session this year. And it's possible, under relatively new state initiative rules designed to allow for more compromise between lawmakers and activists, that a costly ballot box fight could be avoided.

At the outset, this has all the markings of a huge campaign in an election year where the list of statewide propositions almost certainly will be smaller than the long list of measures in 2016.

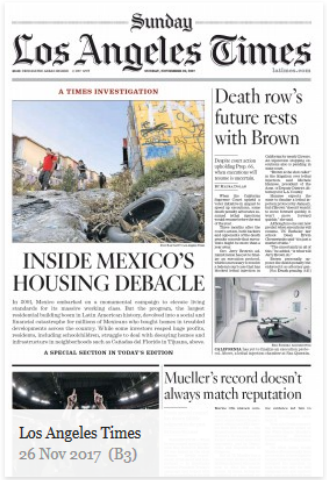
As with so many epic ballot battles, one side will insist that change is long overdue and the other will counter that the change could lead to unintended consequences.

And failing a compromise, the only ones who can sort all of that out, of course, will be the voters.

Write a comment...

Page View Share Comment Save More

Bump it Dump it


Sunday
Los Angeles Times
A TIMES INVESTIGATION
Death row's future rests with Brown
INSIDE MEXICO'S HOUSING DEBACLE
A SPECIAL SECTION IN TODAY'S EDITION
Mueller's record doesn't always match reputation
Los Angeles Times
26 Nov 2017 (B3)

Measuring Privacy

Information Theoretic approaches

Approaches based on assurance

Approaches based on assessment

Major Debate on Attribution

- **How much low level information should be kept to help track down cyber attacks.**
  - **Such information can be used to breach privacy assurances.**
  - **How long can such data be kept.**

Privacy not Only About Privacy

- **Business Concerns**
  - **Disclosing Information we think of as privacy related can divulge business plans.**
    - **Mergers**
    - **Product plans**
    - **Investigations**
- **Some "private" information is used for authentication.**
  - **SSN**
  - **Credit card numbers**

Why Should you Care?

- Aren't the only ones that need to be concerned about privacy the ones that are doing things that they shouldn't?
- Consider the following:
  - Use of information outside original context
    - Certain information may be omitted
  - Implications may be mis-represented.
  - Inference of data that is sensitive.
  - Such data is often not protected.
  - Data can be used for manipulation.

Old News - Shopper's Suit Thrown Out
Los Angeles Times – 2/11/1999 – Stuart Silverstein

A Vons shopper's lawsuit that raised questions about the privacy of information that supermarkets collect on their customers' purchases has been thrown out of court. Los Angeles Superior Court Judge David Horowitz tossed out the civil suit by plaintiff Robert Rivera of Los Angeles, declaring that the evidence never established that Vons was liable for damages.

The central issue in the case was a negligence claim Rivera made against Vons. It stemmed from an accident at the Lincoln Heights' Vons in 1996 in which Rivera slipped on spilled yogurt and smashed his kneecap.

Although that issue was a routine legal matter, the case drew attention because Rivera raised the privacy issue in the pretrial phase. Rivera claimed that he learned that Vons looked up computer records of alcohol purchases he made while using his club discount card and threatened to use the information against him at trial. Vons, however, denied looking up Rivera's purchase records and the issue never came up in the trial, which lasted two weeks before being thrown out by the judge Tuesday.

2009 current event

- New York Times – Miguel Helft – November 11 2008.

- SAN FRANCISCO — There is a new common symptom of the flu, in addition to the usual aches, coughs, fevers and sore throats. Turns out a lot of ailing Americans enter phrases like “flu symptoms” into Google and other search engines before they call their doctors.
  - link

Pandemics and Privacy

- There is a lot to discuss regarding the use of technology for “contact tracing”.
- Other impacts on privacy during a pandemic.

Aggregation of Data

- **Consider whether it is safe to release information in aggregate.**
  - **Such information is presumably no longer personally identifiable**
  - **But given partial information, it is sometimes possible to derive other information by combining it with the aggregated data.**

Anonymization of Data

- **Consider whether it is safe to release information that has been stripped of so called personal identifiers.**
  - **Such information is presumably no longer personally identifiable**
  - **But is it. Consider the release of AOL search data that had been stripped of information identifying the individual performing the search.**
    - **What is important is not just anonymity, but likability.**
    - **If I can link multiple queries, I might be able to infer the identity of the person issuing the query through one query, at which point, all anonymity is lost.**

Traffic Analysis

- **Even when specifics of communication are hidden, the mere knowledge of communication between parties provides useful information to an adversary.**
  - **E.g. pending mergers or acquisitions**
  - **Relationships between entities**
  - **Created visibility of the structure of an organizations.**
  - **Allows some inference about your interests.**

Information Useful for TA

- **Lists of the web sites you visit**
- **Email logs**
- **Phone records**
- **Perhaps you expose the linkages through web sites like linked in.**
- **Consider what information remains in the clear when you design security protocols.**

Obama's cell phone records breached Washington (CNN) 11/21/2008

- Records from a cell phone used by President-elect Obama were improperly breached, apparently by employees of the cell phone company, Verizon Wireless said Thursday.
- "This week we learned that a number of Verizon Wireless employees have, without authorization, accessed and viewed President-Elect Barack Obama's personal cell phone account," Lowell McAdam, Verizon Wireless president and CEO, said in a statement.
- McAdam said the device on the account was a simple voice flip-phone, not a BlackBerry or other smartphone designed for e-mail or other data services, so none of Obama's e-mail could have been accessed.
- Gibbs said that anyone viewing the records likely would have been able to see phone numbers and the frequency of calls Obama made, but that "nobody was monitoring voicemail or anything like that."

P3P DNT and Privacy Statements

- **Most commercial web sites provide a privacy statement.**
  - **Most are not worth the paper they are printed on**
    - **You probably view it on your screen**
    - **Many actually are illustrative, as they are written to say that "we can't control what happens to you data – so don't blame us".**
    - **Who reads them anyway.**
    - **How are they enforced**
      - **Some are certified by outside endorsers**

P3P, Do not Track

- **P3P was a protocol that was designed to allow users to specify their preferences, and to have these preferences negotiated by a browser when connecting to a site.**
  - **But it still doesn't provide any enforcement that the site follows it stated policy.**
  - **It doesn't ensure that the data held by the site is not compromised by outsiders.**
  - **You may still see support in some browsers, but it saw only brief adoption by web sites.**

Protecting Data in Place

- **Many compromises of privacy are due to security compromised on the machines holding private data.**
  - **Your personal computer or PDAs**
  - **Due to malware or physical device theft**
- **Countermeasures**
  - **For device theft, encryption is helpful**
  - **For malware, all the techniques for defending against malicious code are important.**
  - **Live malware has the same access to data as you do when running processes, so encryption might not be sufficient.**

Forensics

- **Tools are available to recover supposedly deleted data from disks.**
  - **Similar tools can reconstruct network sessions.**
  - **Old computers must be disposed of properly to protect any data that was previously stored.**
    - **Many levels of destruction**
  - **Tools like whole disk encryption are useful if applied properly and if the keys are suitably destroyed.**

Privacy – Retention Policies

- PII (personally identifiable information)
  - Is like toxic waste
  - Don’t keep it if you can avoid it
- Regulations
  - Vary by Jurisdiction
  - But if you keep it, it is “discoverable”

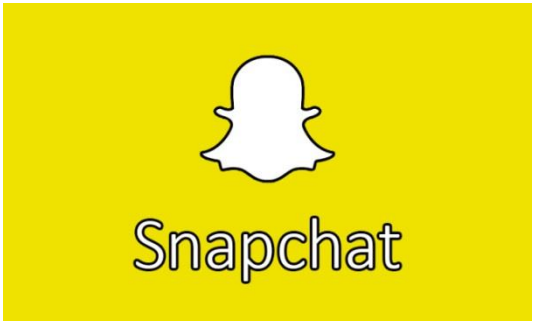
The future of Privacy

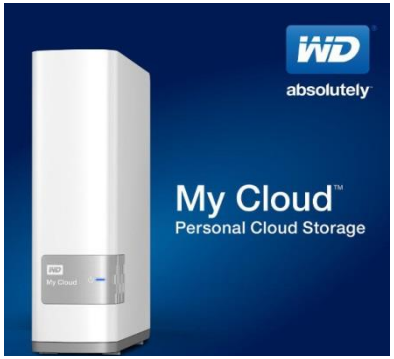
- Who's data is it anyway
  - Should PII carry tags that limit its use.
  - How do we enforce that such tagged policies are actually followed.

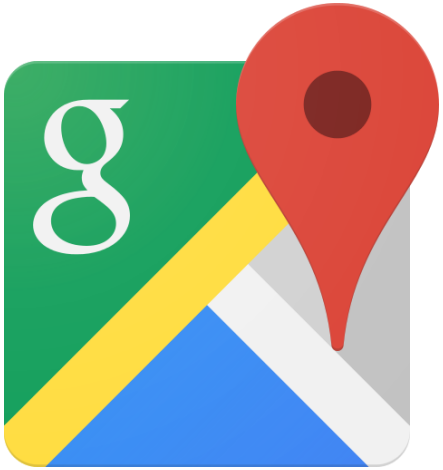
Some IT Background (today's systems)

- In the 1990's Sun Microsystems (now owned by Oracle) used the phrase the network is the computer.
  - We will talk about the kinds of data you can obtain from these parts of computers.
  - With cloud computing, many functions are no longer performed on a physical device, but are performed elsewhere on the network.

Examples of Cloud Services







Cloud Discussion

- What is stored in these and other services.
- How is this data protected.
- What kind of access can you get to this data.
- What you need to know before using.
- What are the implications.

More Background
You Are Being Tracked

- Location
  - From IP address
  - From Cell Phones
- Interests, Purchase History, Political/Religious Affiliations
  - From Transaction Details
  - From network and server traces
- Associates
  - From network, phone, email records
  - From location based information
- Health Information
  - From Purchases
  - From Location based information
  - From web history

Linkages – The Trail We Leave

- **Identifiers**
  - **IP Address**
  - **Cookies**
  - **Login IDs**
  - **MAC Address and other unique IDs**
  - **Document meta-data**
  - **Printer microdots**
- **Where saved**
  - **Log files**
  - **Email headers**
- **Persistence**
  - **How often does Ip address change**
  - **How can it be mapped to user identification**

Unlinking the Trail

- **Blind Signatures**
  - **Enable proof of some attribute without identifying the prover.**
  - **Application in anonymous currency.**
  - **Useful in voting.**
- **What about BitCoin**
  - **Contrary to popular belief, the flow of funds in bitcoin are completely public (public blockchain)**

Unlinking the Trail

- **Anonymizers**
  - **A remote web proxy.**
  - **Hides originators IP address from sites that are visited.**
  - **Usually strips off cookies and other identifying information.**
- **Limitations**
  - **You are dependent on the privacy protections of the anonymizer itself.**
  - **All your activities are now visible at this single point of compromise.**
  - **Use of the anonymizer may highlight exactly those activities that you want to go unnoticed.**

Onion Routing

- **Layers of peer-to-peer anonymization.**
  - **You contact some node in the onion routing network**
  - **Your traffic is forward to other nodes in the network**
  - **Random delays and reordering is applied.**
  - **With fixed probability, it is forwarded on to its destination.**
- **TA requires linking packets through the full chain of participants.**
  - **And may be different for each association.**

Forensics

- **Tools are available to recover supposedly deleted data from disks.**
  - **Similar tools can reconstruct network sessions.**
  - **Old computers must be disposed of properly to protect any data that was previously stored.**
    - **Many levels of destruction**
  - **Tools like whole disk encryption are useful if applied properly and if the keys are suitably destroyed.**

Deleted Files

- Usually remain on the storage system until overwritten with new data later
  - Until completely overwritten, these “partially removed” files can be partially or completely recovered using special forensic program tools that can read every sector and piece the old information together.
  - Different storage devices use different methods for removing these deleted files from the directory structure and sooner or later overwriting them.

Visibility of Addresses

- MAC or physical addresses seen only on the local network.
- IP Addresses visible to the endpoints and intermediate nodes.
- Private IP addresses behind NAT boxes (Network Address Translators) may not be visible
- IP addresses are often transient, assigned as needed through DHCP.
  - Attributing an action based on IP address requires knowing the IP address assignment at a particular point in the past.

Privacy – Retention Policies

- PII (personally identifiable information)
  - Is like toxic waste
  - Don’t keep it if you can avoid it
- Regulations
  - Vary by Jurisdiction
  - GDPR
  - But if you keep it, it is “discoverable”

Discussion of Data Sources

- De-Privacy by Sophia Catsambi from Yale News 18 January 2018

  "By clicking or navigating this site, you agree to allow our collection of information on and off Facebook through cookies." This was the message that greeted me when I opened my page on Monday evening. I promptly clicked "Agree" and rushed to meet a friend for dinner. The notification didn't catch my attention for more than the minimum amount of time required to dismiss it. Not for a second did I pause to think: "Wait, do I actually want Facebook to have access to my personal information, even when I'm engaging in activities that aren't even happening on its platform?"

Initial Homework Assignment
(A,B, or FAIL - due 21 January 2021)

- What sensitive information is available about you through Google, Apple, Amazon, Facebook, TikTok, WeChat and other tools (including your phones)?

  (You should pick two of the providers described above based on the tools/providers you are most familiar with. (you don't need to cover all of them)
  - Enumerate the data
  - Where is it stored?
  - To whom is this data available and under what conditions?
  - How long is the data retained and how (or) can you remove it?
  - What can be done with this data?

  (where to find this – EULA's, Websites, Privacy Policies)

Semester Project

All students are expected to prepare and present a 20 minute lesson on a topic related to privacy that is of interest to them.

- If on a topic that is already in the syllabus, your presentation will be made in the week that the topic is covered in class. The class website shows the topics that are to be presented each week of the semester. Your title/topic should be smore specific than just the title/topic of the lecture.
- If on a topic that is not already in the syllabus, I will assign a week from your presentation, based on available time in lecture, and based on relevance.
- Please send me proposed topics for your class presentation by Thursday the 21st. I will create a drop box entry in D2L through which you can submit your proposal. You can suggest multiple topics if you like... if so let me know your order of preference. All that you need is a short title and a one sentence description. Topics may be chosen from among the topics listed in the syllabus for the class, or you may propose topics around any particular problem domain (e.g. type of system, type of business, type of activity) for which you will provide a thorough discussion of privacy (or privacy invading) technology and policy.
- Group presentations are acceptable, in which case your team would receive 20 minutes per team member to present on a topic.

Weekly Current Event Assignment

Beginning 1/22/2021 students should find a current event regarding security or privacy (preferably privacy) in the news and send me a URL, title, and three sentence write-up which we will discuss in class. The write-up should be sent to me before 7AM the morning of our lecture. We will present these weekly, but all students are expected to submit at least one such event description for every two lectures. Please your writeup with the subject "529 Current Event for Lecture X" to inf529@csclass.info.

The body of your message should be HTML formatted as follows:

<A HREF="{link to news story}">Your one line title (which may be the headline for the story)</A> - Author(e.g. name of write), Source(e.g. New York Times) Date
<UL>
Your three sentence summary of the story in your own words – Your name
</UL>

We will discuss all submissions in class and you will be called on to provide additional information about your submission.

Example of how it will look on the class web page:
Google's Art Selfie App Offers A Lesson In Biometric Privacy Laws – John Smith - NPR 1/18/18
Story explains why the Art Selfie app is not available to users in Illinois or Texas. Explains the unintended consequences of privacy legislation.

This year's most current events

Each year the focus of our discussion changes because of particular current breaking news. Here I list a few of the major current discussions that may be covered this semester, and we can briefly discuss them here:

- GDPR
- California Consumer Privacy Act
- California Privacy Rights Act
- Facebook (and others') use of private data
- Social media and political influence
- China's Social Credit Scoring
- Access and use of DNA databases
- IoT and privacy