DSci529:
Security and Privacy In Informatics

Continued Discussion
Technical Means of Protection
Containment Architecture
(then)
Expectations of Privacy

Prof. Clifford Neuman

Lecture 5
12 February 2021
Online

Course Outline

- Overview of informatics privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- **The right of or expectation of privacy**
- Social Networks and the social contract
- Measuring Privacy
- Big data – Privacy Considerations
- Criminal law, National Security, and Privacy
- Civil law and privacy
- International law and conflict across jurisdictions
- The Internet of Things
- The future – What can we do

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec5-ce.html

Presentations

- Most students have submitted their proposed topics and I have organized them into groups based on the dates that we cover similar topics in lecture.
- If you submitted your topic through D2L and have not received specific feedback, that means your topic is approved (if you listed several topics, I approved one of them).
- You will receive more feedback as I complete the assignment to lectures.
- But, some topics are much earlier in the semester than others, so let's discuss assignments for some topics now.

The right of or expectation of privacy

- We will provide our lectue this week, but the student presentations will occur on February 19th.
  - Emily Christiansen – CyberSecurity v. Constitutionally Protected Rights
  - Tian Yang – Expectations and Understanding of Privacy
  - (total 20 minutes across both presenters)

- I recognize this is much earlier than other students will present, and I will consider that factor in my assessment of your presentations.

Big Data – AI and Privacy

- I would also like to cover this on February 19th, since it is the official topic of class on that date.
  - Lingyu Ge – Big Data and Discrimination
  - Tingyi Guo – Big Data Security and implication in Healthcare and the Cloud
  - Kung-hsiang Huang – Secure Neural Network Inference
  - Supreet Kaur Randhawa – Eavesdropping and Data Breaches in Big Data
  - Zheyu Ren – Big Data and Privacy
  - (50 minutes across all presenters)
- I recognize this is much earlier than other students will present, and I will consider that factor in my assessment of your presentations.

Internet of Things

- This topic will likely be covered on March 5th.
- The students proposing on Internet of Things related topics are:
  - Pratheek Athreya
  - Arzu Karaer
  - Bolong Pan
  - Danielle Sim
  - Haipeng Yu
  - Xihao Zhou
  - Jinyu Zhao
  - Pu Zhao
  - Junbo Sheng
- This group will have one hour 30 minutes to present.

Social Media

- This topic will likely be covered on March 19thth.
- The students proposing on Social Media topics are:
  - Addison Allred
  - Yixiang Cao
  - Lei Gao
  - Brianna Hefferin
  - Mingliao Xu
  - Shengwang Zhang
  - Zixin Zheng
  - Hehan Xie
  - Chengyuan Zhou
- This group will have one hour and 30 minutes to present.

The Pandemic (and other government use of data)

- This topic will likely be covered on March 26th.

- The students proposing on pandemic related topics: (40 min)
  - Yuemeng Gao
  - Tanmay Ghai – Privacy Preserving Contact Tracing
  - Yi Lin – Use of Big Data in China related to the COVID Pandemic
  - Gan Xin – Health QR Code in China

- Other government use of data (50 min)
  - Yi Jin – How countries (eg US and China) collect and use personal data
  - Congrui Li
  - Michelle Muldoon – Law Enforcement and Privacy w.r.t. Data Brokers
  - Griffin Weinhold – Decentralized Search and Search Histories in Court
  - Xihao Zhou – Use of Data by Governments

Privacy Related to Healthcare

- I have not determined the optimal date for this presentation.

- The students proposing on healthcare related topics (excluding the pandemic) are:
  - Vartan Batmazyan
  - Tingyi Guo
  - Phuong Ngo
  - Sharad Sharma (DNA Databases)
  - Ye Zheng - Fitness apps

- This group will have 50 minutes to present.

Privacy and Security Regulation

- This topic will likely be covered on April 2nd .
- Several Students have Proposed on these topics:
  - Jia Yu Lee
  - Yansong Wang
  - Kaifan Lu – Assessing China's Cybersecurity Law

Free Expression - Disinformation

- This topic will likely be covered on April 9th.
- The students proposing on this are:
  - Adriana Nana – Deep Fakes and Privacy
- This group will have 10 minutes to present.

Privacy and Finance

- This topic will likely be covered on April 16th..

- Two students proposing on Financial Topics
  - Jonathan De Leon – Privacy in Finance
  - Sidong Wang – History and Technologies for Cryptocurrencies

Secure Communication – Privacy Preserving Technologies

- This topic will likely be covered on April 16th..

- Several Students have Proposed on these topics:
  - Zihuan Ran – Privacy Preserving Database Technologies
  - Aziza Saulebay – 5G and Data Privacy
  - Carol Varkey – Messaging Application Privacy
  - Francisco Ventura – Encryption Technologies and implications
  - Zixin Zheng – Privacy Preserving Technologies

Other Security Topics

- I have not settled on a date for these topics.

- Several Students have Proposed on general security technologies or issues:
  - Yo-Shuan Liu – User experience and Multi-Factor Authentication
  - Philana Williams – Security for Web App Development
  - Haonan Xu – Privacy issues in Cloud Computing
  - Pratishtha Singh – Card privacy Concerns in India

DSci529:
Security and Privacy In Informatics

Continued Discussion
Technical Means of Protection
Containment Architecture
(then)
Expectations of Privacy

Prof. Clifford Neuman

Lecture 5
12 February 2021
Online

Containment Architecture Action PLAN

Conduct an Inventory – of data

- What Kinds of Data do you have in your business
- How is it handled and where is it handled
- Who needs access to this data
- Which systems need access to this data
- How is it protected in transit, and in situ

Containment Architecture Action PLAN

Conduct an Inventory – of physical assets

- What Kinds of systems do you have
  - E.g. POS terminals, servers, network hardware
- Understand the access to each system
  - Employees, customers, etc
- How are the different classes of systems protected from one another
  - Network zones, etc
- How do you contain breaches to particular zones.

COLLECT BASLINE INFO ON ALL ASSETS

Software and system checksums
- Used to detect changes to the system
- To identify which assets are affected
- To enable recovery – reinstall those affected systems

Baseline data communication from all assets
- In you network infrastructure, use this to identify anomalous flows
- As they happen to block exfiltration
- From Logs to identify where data went and how much, and over what time periods

This much PREPARATION CHANGES THE STORY

From:
XYZ corporation is the latest company to report that the personal information of 70M customers may have been compromised.
TO:
XYZ corporation reports that users of its beach city store between October 1st and 3rd may have been affected by …

What Technology should I deploy

- Audit and intrusion detection
- Encryption throughout the systems
  - Data in transit and data on disk
  - As close to the source as possible
- System mapping/configuration tools
  - Align with your containment architecture
- Effective identity and policy management
- Configuration management systems

Addressing Data Compromise

Don’t collect the data
- If you don’t need it
- Design systems so you don’t need it

Don’t use the data for authentication
- Why do we use public information for authentication:
  - Mothers maiden name
  - Password reset information
  - SSN

Why such poor practices

Internet services require scalability to be viable.
Automation provides that scalability.
Effective Customer service does not.

It is all about avoiding personal contact with the customer, which would require more staff.

Course Outline

- Overview of informatics privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- **The right of or expectation of privacy**
- Social Networks and the social contract
- Measuring Privacy
- Big data – Privacy Considerations
- Criminal law, National Security, and Privacy
- Civil law and privacy
- International law and conflict across jurisdictions
- The Internet of Things
- The future – What can we do

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec4-ce.html

INF529:
Security and Privacy
In Informatics

Advance Slides
(if time permits)

Expectations of Privacy

Prof. Clifford Neuman

Lecture 5
12 February 2021
Online

Course Outline

- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- **The right of or expectation of privacy**
- Government and Policing access to data – Feruary15th
- Social Networks and the social contract – March 1st
- Criminal law, National Security, and Privacy – March 22nd
- Big data – Privacy Considerations – March 8th
- Civil law and privacy – March 29th (also Measuring Privacy)
- International law and conflict across jurisdictions – April 5th
- The Internet of Things – April 12th
- Technology – April 19th
- The future – What can we do – April 26th

What is Privacy – One Definition

Broadly speaking, privacy is ***the right to be let alone*****.**

- **Itallics US Supreme Court Justice Louis Brandeis in 1890 Harvard Law Review (before he was a Supreme Court Justice).**

– **There is no right to privacy specifically spelled out in the US Constitution, but there are many specific rights that support interpretations providing such rights.**

Expectation of Privacy

4th amendment to US Constitution

- The right of the people to be secure in their persons, 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.
- This statement applies to actions by Government

Today's discussion is not about the 4th amendment, but rather the meaning of the term "Unreasonable".

And thus the topic is neither US, nor government centric

When do we not have an expectation

- 3rd Party Doctrine
  - Holds that people who voluntarily give information to third parties are not protected by a reasonable expectation of privacy

Reasonable Expectation of Privacy

- To have a reasonable expectation of privacy you need 2 things:
  - Individual needs to exhibit an actual expectation of privacy, meaning “he seeks to preserve something as private”
    - “plain view test”
  - Is the individual’s expectation of privacy one that society is prepared to recognize as ‘reasonable’?

3rd Party Doctrine

- Also known as the “Privacy Doctrine”
- Many court rulings uphold the idea that right to privacy is waived when signing up for a service.
- Original purpose was to allow police to question gang members without needing a warrant.
- Over time, the doctrine grew to allow warrantless searches of telephone metadata and financial bank records.

Standing

- The right of an individual to contest the illegality of a search and seizure

- Almost like a “catch 22”.
  - Only the person whose rights are being violated has “standing”. Therefore, to challenge an alleged governmental constitutional violation, you have to claim ownership of the evidence being submitted.

Katz v. United States (1967)

- Situation:
  - Government agents had intercepted the contents of a telephone conversation of a man suspected of illegal gambling
  - This was done by installing a listening device on the outside of a public telephone booth.
- Ruling:
  - Court rejected the argument that a “search” can occur only when there has been a “physical intrusion” into a “constitutionally protected area”

Implications of Katz v United States

- Refined interpretation of the unreasonable search and seizure clause of the 4th Amendment to include immaterial intrusion with technology as a search.

- Extends the 4th Amendment right to “protect people, not property”

Smith v. Maryland (1979)

- Situation:
  - Man robbed a store and for a couple weeks after, the man would call the owner of the store and threaten her.
  - Police installed a pen register (device that records numbers that a phone dials), this showed that the man suspected of robbing the store was the one placing the phone calls
  - This data led to a search warrant, where they found more evidence in the man's home.
  - Smith wanted all evidence thrown out that was a result of the pen register.
- Court Ruled:
  - The pen register was not a breach of "reasonable expectation to privacy", therefore the evidence remained
  - ***This predated the ECPA***

Justification for Smith v. Maryland

- Activity in question:
  - Installing and using the pen register
- Who's property?
  - Since the pen register was installed on the telephone company's property, the defendant cannot claim his "property" was invaded or that police intruded.
- What about "protecting the person" not "protecting the property"?

Other Implications of Exposed Metadata

- Think of ISP and Social Media
- What could be determined from our metadata?
- **What is being determined from our metadata?**

United States v. Knotts (1983)

- Situation:
  - Officers followed a car containing a beeper, relying on the beeper signal to determine the car's final destination.
- Ruling:
  - Court unanimously held that since the use of such a device did not violate a legitimate expectation of privacy; there was no search and seizure and thus allowed without a warrant.

Implications of United States v. Knotts

- A person traveling in public has no expectation of privacy in one's movements.

- Will Google Maps and Apple Maps be allowed to work in tandem with the police force?

- ***Again, note that there have been recent laws and ruling that limit this kind of collections.***

Bringing Things Up to Date

Real expectations vs legal fictions

- No expectation of privacy for actions performed in public
- No expectation of privacy for material in plain sight
- But technology changes to nature of the information

Expectation of Privacy from Whom

- 4th amendment US Centric and applies to government.
- What about industry, neighbors, etc.

Where else are there laws related to privacy expectations

Actions Performed in Public

- What are our expectations:
  - When our actions can be observed
    - Then – Witnesses can describe what they saw
    - Now – ubiquitous surveillance cameras may record us
      - (certain locations have privacy expectations)
    - We might be identified after the fact
      - Ones activities creates the motivation to obtain data
    - Our loss of privacy/anonymity occurs after the act
      - And based on information we expect to be “public”

New Technologies

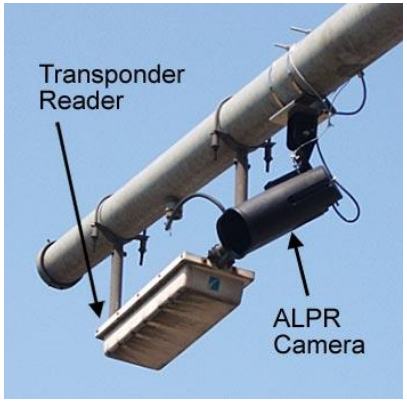
We are constantly identified and the stream of indivually "public" data is now invasive.

- ALPR – Automatic License Pate Readers
  - Similarly, when location data is centralized, we can track movement of individual vehicles.
- Facial recognition
  - When combined with central clearing of identification
  - Allows one to track the movements of individuals

Automatic License Plate Readers

ALPR devices are popping up all over the place, from toll roads to parking garages, to the entrances to the USC Campus.

Many private ALPR systems are managed by organizations that aggregate the data and sell it for commercial purposes such as repossessions.



LAPD automatic license plate readers pose a massive privacy risk, audit says, LA Times, 2/13/2020

An automated license plate reader is mounted to the back of a Washington, D.C., police vehicle. (Jim Lo Scalzo / EPA)

By PATRICK MCGREEVY | STAFF WRITER FEB. 13, 2020 | 1:07 PM

SACRAMENTO — The Los Angeles Police Department and three other California law enforcement agencies have not provided sufficient privacy protections for the hundreds of millions of images collected by automated license plate readers and shared with other jurisdictions, the state auditor said Thursday.

Most of the images collected by the devices are unrelated to criminal cases. The audit found that 99.9% of the 320 million images the LAPD stored came from vehicles that were not on a list of those involved in criminal investigations when the image was made by the automated license plate readers, or ALPR.

We are Part of the Problem

https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive

University of Southern California
USC had far fewer ALPR cameras exposed than those in Louisiana—only four of what is likely a 60-plus camera network. However, these four cameras were even more vulnerable than the Louisiana cameras, since their controls were hosted on public university pages, with obvious URLs such as pipscam9.usc.edu.

Pipscam9 was particularly problematic. Located on "Fraternity Row" (see it here) and directly across from the Pi Kappa Phi house, the ALPR camera was completely unprotected. One could not only see the license plates passing down the street, but also watch a live video feed (below) of people crossing the street.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM

OCTOBER 28, 2015 | BY DAVE MAASS AND COOPER QUINTIN

License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech

Law enforcement agencies around the country have been all too eager to adopt mass surveillance technologies, but sometimes they have put little effort into ensuring the systems are secure and the sensitive data they collect on everyday people is protected.

Case in point: automated license plate recognition (ALPR) systems.

Earlier this year, EFF learned that more than a hundred ALPR cameras were exposed online, often with totally open Web pages accessible by anyone with a browser. In five cases, we were able to track the cameras to their sources: St. Tammany Parish Sheriff's Office, Jefferson Parish Sheriff's Office, and the Kenner Police in Louisiana; Hialeah Police Department in Florida; and the University of Southern California's public safety department. These cases are very similar, but unrelated to, major vulnerabilities in Boston's ALPR network uncovered in September by DigBoston and the Boston Institute for Nonprofit Journalism.

After five months of engagement with these entities, we are releasing the results of our research and the actions these offices undertook in response to our warnings.

Texas ALPR to Collect Fines

https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and

The problem with License Plate Readers is the aggregation of the data. While the location of our vehicle on a public street is visible and we have no expectation of privacy, when the information is collected over a period of time, it now exposes our transportation history, and we at least EXPECT some level of privacy regarding that.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM

JANUARY 26, 2016 | BY DAVE MAASS

"No Cost" License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners

Vigilant Solutions, one of the country's largest brokers of vehicle surveillance technology, is offering a hell of a deal to law enforcement agencies in Texas: a whole suite of automated license plate reader (ALPR) equipment and access to the company's massive databases and analytical tools—and it won't cost the agency a dime.

Even though the technology is marketed as budget neutral, that doesn't mean no one has to pay. Instead, Texas police fund it by gouging people who have outstanding court fines and handing Vigilant all of the data they gather on drivers for nearly unlimited commercial use.

ALPR refers to high-speed camera networks that capture license plate images, convert the plate numbers into machine-readable text, geotag and time-stamp the information, and store it all in database systems. EFF has long been concerned with this technology, because ALPRs typically capture sensitive location information on all drivers—not just criminal suspects—and, in aggregate, the information can reveal personal information, such as where you go to church, what doctors you visit, and where you sleep at night.

Vigilant is leveraging H.B. 121, a new Texas law passed in 2015 that allows officers to install credit and debit card readers in their patrol vehicles to take payment on the spot for unpaid court fines, also known as capias warrants. When the law passed, Texas legislators argued that not only would it help local government with their budgets, it would also benefit the public and police. As the bill's sponsor, Rep. Allen Fletcher, wrote in his official statement of intent:

> [T]he option of making such a payment at the time of arrest could avoid contributing to already crowded jails, save time for arresting officers, and relieve minor offenders suddenly informed of an uncollected payment when pulled over for a routine moving violation from the burden of dealing with an impounded vehicle and the potential inconvenience of finding someone to supervise a child because of an unexpected arrest.

Surveillance for Hire

http://www.theblaze.com/news/2014/03/06/surveillance-for-hire-would-you-take-money-to-record-fellow-drivers/

Once again, we see the value to companies of data about your locations. In this case, data could be accessed by private investigators and others. The value is in the aggregation of the data, rather than in the localized snapshot of ones current location.

theblaze News Channels MyVoice Radio TV

Surveillance For Hire: Would You Take Money to Record Fellow Drivers?

Elizabeth Kreft Mar 6, 2014 8:02 am

90 Follow

SHARE TWEET

If you could mount a camera on your car that simply scanned license plates as you drove — and earned you $200 to $400 each time it registered a stolen or repossessed car — would you do it?

License plate readers on a civilian vehicle. (Image source: YouTube)

That's the gig several repo men have lined up across the country: selling location information they gather to companies like Texas-based Digital Recognition Network. The Fort Worth company typically adds 8,000 plate scans to their huge database from "spotters" like Manny Sousa.

BetaBoston reported that repossession companies like Sousa's New England Associates Inc. in Bridgewater, Mass., mount automatic readers to spotter cars that constantly take pictures of every license plate it passes while the drivers are working a repossession route.

ICE Accesses a Massive Amount of License Plate Data. Will California Take Action?

ELECTRONIC FRONTIER FOUNDATION

BY DAVE MAASS | JANUARY 29, 2018

The news that Immigrations & Customs Enforcement is using a massive database of license plate scans from a private company sent shockwaves through the civil liberties and immigrants' rights community, who are already sounding the alarm about how mass surveillance will be used to fuel deportation efforts.

The concerns are certainly justified: the vendor, Vigilant Solutions, offers access to 6.5 billion data points, plus millions more collected by law enforcement agencies around the country. Using advanced algorithms, this information—often collected by roving vehicles equipped with automated license plate readers (ALPRs) that scan every license plate they pass—can be used to reveal a driver's travel patterns and to track a vehicle in real time.

ICE announced the expansion of its ALPR program in December, but without disclosing what company would be supplying the data. While EFF had long suspected Vigilant Solutions won the contract, The Verge confirmed it in a widely circulated story published last week.

In California, this development raises many questions about whether the legislature has taken enough steps to protect immigrants, despite passing laws last year to protect residents from heavy-handed immigration enforcement.

But California lawmakers should have already seen this coming. Two years ago, The Atlantic branded these commercial ALPR databases, "an unprecedented threat to privacy."

Vigilant Solutions tells its law enforcement customers that accessing this data is "as easy as adding a friend on your favorite social media platform." As a result, California agencies share their data wholesale with hundreds of entities, ranging from small towns in the Deep South to a variety of federal agencies.

An analysis by EFF of records obtained from local police has identified more than a dozen California agencies that have already been sharing ALPR data with ICE through their Vigilant Solutions accounts. The records show that ICE, through its Homeland Security Investigations offices in Newark, New Orleans, and Houston, has had access to data from more than a dozen California police departments for years.

At least one ICE office has access to ALPR data collected by the following police agencies:

- Anaheim Police Department
- Antioch Police Department
- Bakersfield Police Department
- Chino Police Department
- Fontana Police Department
- Fountain Valley Police Department
- Glendora Police Department
- Hawthorne Police Department
- Montebello Police Department
- Orange Police Department
- Sacramento Police Department
- San Diego Police Department
- Simi Valley Police Department
- Tulare Police Department

California says no, you can't cover your license plate

Proposed legislation that would allow California residents to cover their license plates while parked, has been tabled under pressure from law enforcement groups.

Previous: Deepfakes AI porn GIFs purged from Gfycat p... Next: Adobe warns of Flash zero-day, patch to come nex...

by Lisa Vaas

Under pressure from police lobbyists, California state senators have killed a bill that would have made it harder for data-aggregators-on-wheels to automatically snap photos of parked cars' license plates.

Senate bill SB-712, which had bipartisan support, would have tweaked a law that says you can't cover your car's license plate.

In California, it's currently legal to cover your entire vehicle when it's parked, including the license plate, to protect the car from the weather, as long as the cover is easy enough to pull up to get a look at the license plate.

However, it's illegal to cover *just* the license plate when it's parked, which you may very well want to do to protect your privacy from automated license plate readers (ALPRs). As of Tuesday, the bill is dead, and it's still illegal to cover just your license plate.

The bill, which was endorsed by the Electronic Frontier Foundation (EFF), was meant to protect location data privacy from the spying electronic eyes of ALPRs. As the EFF notes, ALPR data can reveal where you live, where you work, where you worship and where you drop your kids at school. From the EFF:

Facial Recognition

https://www.engadget.com/2006/02/28/biobouncer-facial-recognition-system-for-bars-clubs/

While we're aware of the occasional incident "in da club" featuring a firearm-bearing-celebrity, we've been blissfully ignorant of the fact that clubbing these days has apparently gotten so dangerous that a market has sprung up for nightlife-specific biometric security solutions.

Well Wired is reporting that besides the fingerprint recognition system that a company called Food Service Solutions is pitching to alcohol retailers, an even more ambitious facial recognition system is about to be deployed in U.S. bars and clubs by a 24-year-old entrepreneur named Jeff Dussich. Dussich's company, JAD Communications and Security, is promoting its BioBouncer package as a way for communities to identify habitual troublemakers by using a Vegas-like database of blacklisted individuals that is shared among local establishments. BioBouncer costs $7,500 for the initial hardware, software, and setup, and $6000 per year for support, which presumably means access to the networked "rogue's gallery." Not surprisingly, privacy groups such as the EFF are opposed to BioBouncer and similar systems,citing both their questionable accuracy and potential for misuse.

BioBouncer facial recognition system for bars, clubs

Evan Blass
02.28.06

0
Shares

While we're aware of the occasional incident "in da club" featuring a firearm-bearing-celebrity, we've been blissfully ignorant of the fact that clubbing these days has apparently gotten so dangerous that a market has sprung up for nightlife-specific biometric security solutions. Well Wired is reporting that besides the fingerprint recognition system that a company called Food Service Solutions is pitching to alcohol retailers, an even more ambitious facial recognition system is about to be deployed in U.S. bars and clubs by a 24-year-old entrepreneur named Jeff Dussich. Dussich's company, JAD Communications and Security, is promoting its BioBouncer package as a way for communities to identify habitual troublemakers by using a Vegas-like database of blacklisted individuals that is shared among local establishments. BioBouncer costs $7,500 for the initial hardware, software, and setup, and $6000 per year for support, which presumably means access to the networked "rogue's gallery." Not surprisingly, privacy groups such as the EFF are opposed to BioBouncer and similar systems,citing both their questionable accuracy and potential for misuse.

From Whom is Information Private

Business Records

- 3rd party doctrine tells us that we have no expectation of privacy for records that are maintained in the normal course of business (including things like call logs, etc).
- Specific legislation my dictate that certain kinds of records not be disclosed.
- Privacy policies or contractual requirements may do the same.

Expectation of Privacy implications

Not that information can-not be obtained, but rather the conditions under which it may be obtained.

Privacy of Electronic Mail

from the 2012 Version of FBI Domestic Investigations and Operations Guide, which the ACLU got through a FOIA request:

> In enacting the ECPA, Congress concluded that customers may not retain a "reasonable expectation of privacy" in information sent to network providers. . . **[I]f the contents of an unopened message are kept beyond six months or stored on behalf of the customer after the e-mail has been received or opened, it should be treated the same as a business record in the hands of a third party, such as an accountant or attorney.** In that case, the government may subpoena the records from the third party without running afoul of either the Fourth or Fifth Amendment.

Privacy of Electronic Mail

https://www.wired.com/2017/02/trump-power-email-privacy-act-never-urgent/

New proposed legislation changes this.

The email privacy act could require government agencies to obtain a warrant before seizing criminal suspect's online communications that are more than 180 days old. Under the ECPA's existing logic, those older communications are considered abandoned, and thus not subject to a reasonable expectation of privacy. Amendment.

WIRED Passing the Email Privacy Act Has Never Been More Urgent

BUSINESS CULTURE DESIGN GEAR SCIENCE

SHARE

SHARE 750

TWEET

ANDY GREENBERG SECURITY 02.06.17 4:26 PM

PASSING THE EMAIL PRIVACY ACT HAS NEVER BEEN MORE URGENT

IT'S SAFE TO say that any digital privacy bill written more than three years before the invention of the World Wide Web is probably due for an overhaul. But the Electronic Communications Privacy Act has persisted intact for more than three decades, including its anachronistic loophole that allows the warrantless collection of emails from US citizens. Now, in its second attempt in two years, Congress is poised to reform the most outdated elements of ECPA. With Trump's incoming Justice Department, that reform seems more urgent than ever.

On Monday evening, the House of Representatives unanimously passed the Email Privacy Act, a bill that would reform ECPA were it to become law. In particular, it would newly require government agencies to obtain a warrant before seizing a criminal suspect's online communications that are more than 180 days old. Under the ECPA's existing logic, those older communications are considered abandoned, and thus not subject to a reasonable expectation of privacy.

Overriding Expectations

For business records and other items without an “expectation” of privacy, there is still criminal and civil procedure that must be applied to obtain such records.

Three classes:

- What is truly considered public
  - Investigators ask witnesses, look at public records, or other material considered public.
- Items like business records or information held by third parties
  - Investigators issue subpoenas or other forms of process for specific records. Though arrangements have been entered into for direct access. Such arrangements are troublesome.
- If there is an legislated or legal expectation of privacy
  - Investigators must obtain a search warrant, which has a higher burden of probable cause than for subpoenas.

Can Public Tweets be used by LE

https://www.engadget.com/2016/12/15/twitter-stops-dataminr-from-sharing-tweets-with-police-hubs/

Should Law Enforcement and intelligence agencies really be stopped from using information that is published to the rest of the world.
Twitter thinks yes.

engadget 3 related articles

Latest in Culture

Snapchat is getting a reality TV show from A+E

Twitter won't share tweets with law enforcement data hubs

Its partner Dataminr can't contribute information to surveillance-friendly fusion centers in the US.

Twitter is still determined to avoid facilitating mass surveillance by spies and law enforcement. The company has told Dataminr, a firm it partly owns, to stop sharing tweets with the 77 law enforcement fusion centers (that is, data hubs where agencies share info and make connections) in the US. This doesn't prevent police from sifting through Twitter posts, but it certainly makes their work harder. The centers won't have ready access to "billions" of tweets they can pass on to the federal government for spying purposes, according to the ACLU.

This doesn't mean that Dataminr is without government business. Rather, it's emphasizing a "focused" service that delivers breaking news to first responders, including police. The move should help with emergencies while preventing easy user profiling, geospatial analysis (say, where protesters are operating) and other forms of monitoring. Twitter and Dataminr aren't flouting the law, then. They just don't want to contribute to attempts to discourage free speech, whether it's a protest on the street or journalists who challenge political leaders.

Electonic Communication Privacy Act (1986)

https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515.

Many issues to be discussed.

CAL ECPA

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178

Senate Bill No. 178

CHAPTER 651

An act to add Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code, relating to privacy.

[Approved by Governor October 08, 2015. Filed with Secretary of State October 08, 2015.]

LEGISLATIVE COUNSEL'S DIGEST

SB 178, Leno. Privacy: electronic communications: search warrant.

(1) Existing law provides that a search warrant may only be issued upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing, or things and the place to be searched. Existing law also states the grounds upon which a search warrant may be issued, including, among other grounds, when the property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony, or when there is a warrant to arrest a person.

This bill would prohibit a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under specified conditions, except for emergency situations, as defined. The bill would also specify the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, or consent of the owner of the device. The bill would define a number of terms for those purposes, including, among others, "electronic communication information" and "electronic device information," which the bill defines collectively as "electronic information." The bill would require a search warrant for electronic information to describe with particularity the information to be seized and would impose other conditions on the use of the search warrant or wiretap order and the information obtained, including retention, sealing, and disclosure. The bill would require a warrant directed to a service provider to be accompanied by an order requiring the service provider to verify by affidavit the authenticity of electronic information that it produces, as specified. The bill would authorize a service provider to voluntarily disclose, when not otherwise prohibited by state or federal law, electronic communication information or subscriber information, and would require a government entity to destroy information so provided within 90 days, subject to specified exceptions. The bill would, subject to exceptions, require a government entity that executes a search warrant pursuant to these provisions to contemporaneously provide notice, as specified, to the identified target, that informs the recipient that information about the recipient has been compelled or requested, and that states the nature of the government investigation under which the information is sought. The bill would authorize a delay of 90 days, subject to renewal, for providing the notice under specified conditions that constitute an emergency. The bill would require the notice to include a copy of the warrant or statement describing the emergency under which the notice was delayed. The bill would provide that any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of its provisions, according to specified procedures. The bill would provide that a California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, wiretap order, or other order issued pursuant to these provisions.

ARTICLE 8 – European Convention on Human Rights

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Europe's GDPR

Extends privacy rights to corporate use of data.

Includes "Right to be Forgotten"

More on this later in the semester when we speak about regulations.

Right to be Forgotten (before GDPR)

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

- In 2010 a Spanish citizen lodged a complaint against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc. The citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results

Going Dark from a Law Enforcement Perspective

Those responsible for protecting us are not always able to access evidence and/or materials necessary for their job to prosecute crimes and prevent terrorism even when they have a lawful reason to do so. Examples:

- Monitoring Phone calls, e-mail, and live chat sessions of criminals and terrorists
- Recovering Data stored on the devices of criminals and terrorists, such as e-mail, text messages, photos, and videos

For this reason, they seek solutions (laws) that will enable such access.

  - In many cases, the laws they seek try to impose technical solutions to this problem.
  - Can there be technical solutions to the problem as defined above?

Post Snowden Distrust of Government

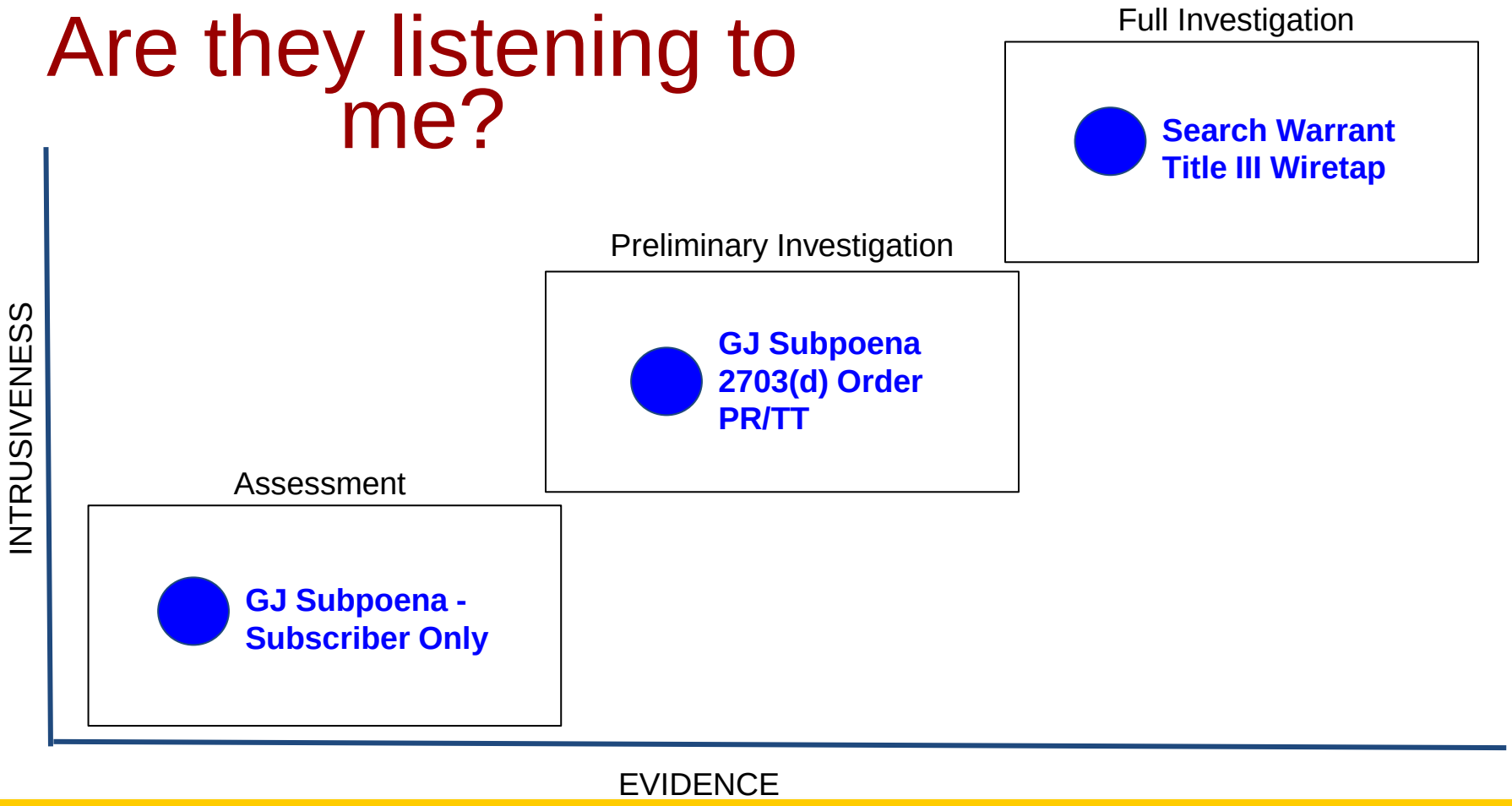
"The people of the FBI are sworn to protect both security and liberty. We care deeply about protecting liberty—including an individual's right to privacy through due process of law—while simultaneously protecting this country and safeguarding the citizens we serve." - FBI website

"In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true." - ex FBI Director James Comey.

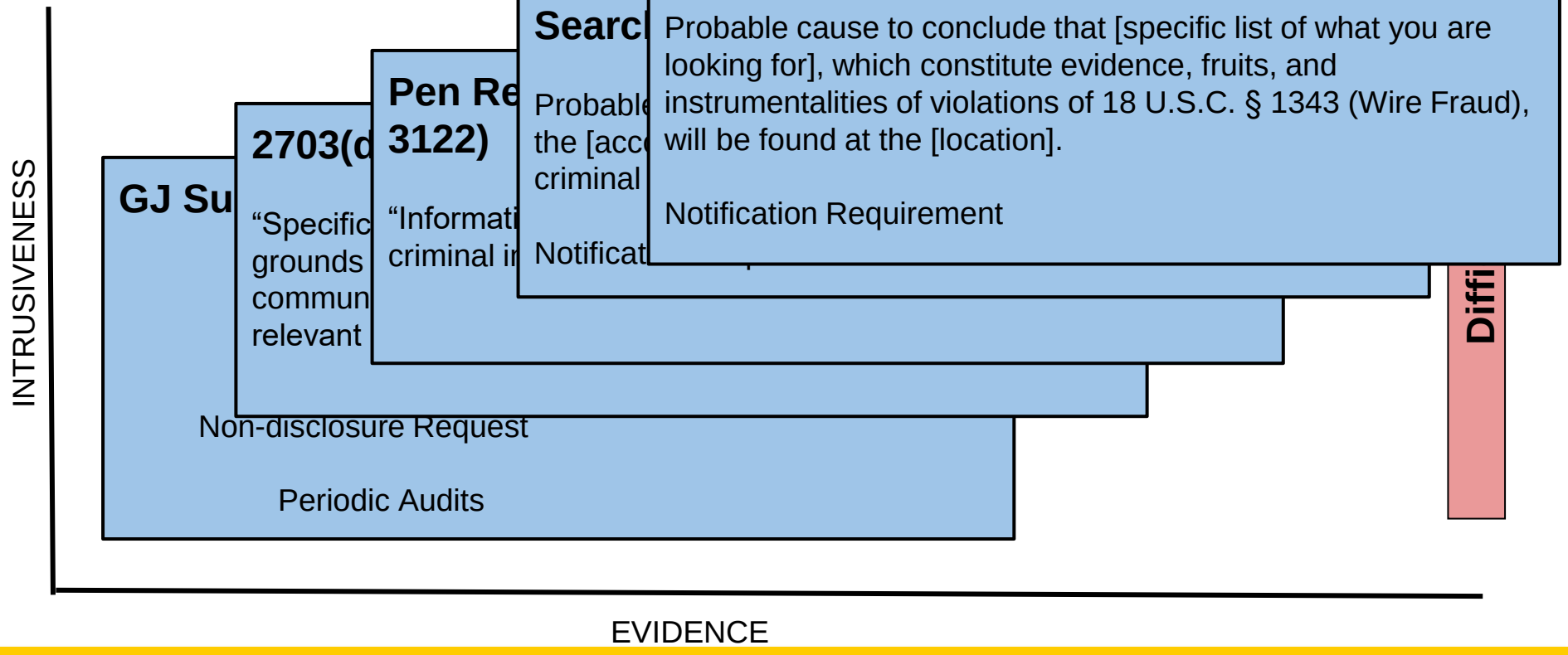
"Those of us in law enforcement can't do what we need to do without your trust and your support." - ex FBI Director James Comey

Distrust of Government is a good thing.

Are they listening to me?



How hard is it?



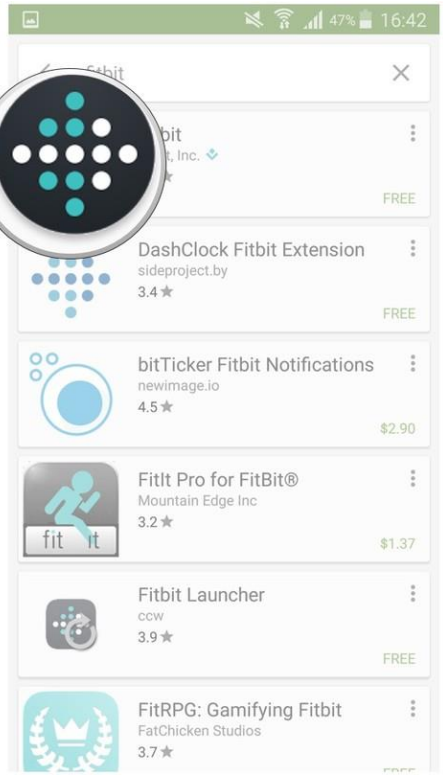
Communications Assistance for Law Enforcement Act (CALEA) - October 25, 1994

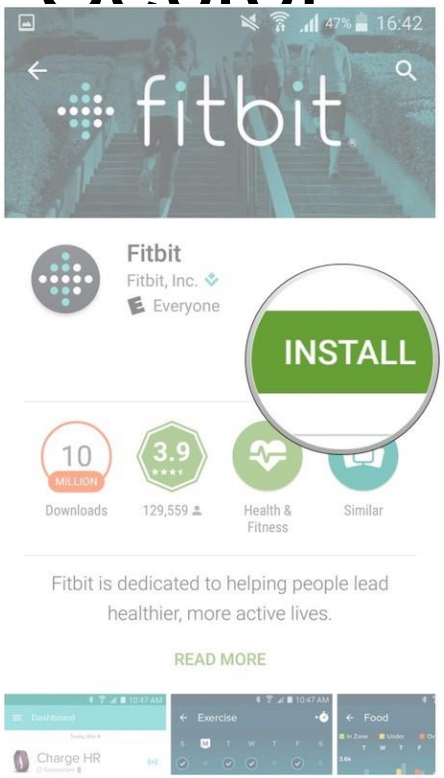
It requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information. - FCC

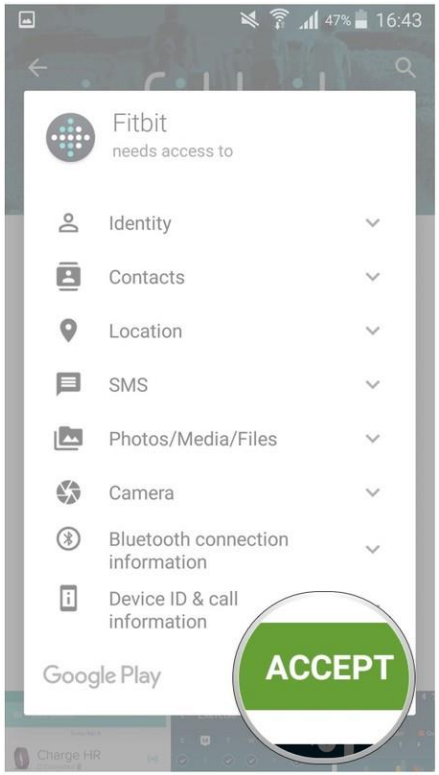
Currently thousands of companies provide some form of communication service, and most are not required by CALEA to develop lawful intercept capabilities for law enforcement. - FBI Website

As a result, many of today's communication services are developed and deployed without consideration of law enforcement's lawful intercept and evidence collection needs. - FBI Website

So What Does It Take for the Private Sector?







Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec5-ce.html

Privacy and Big Data

Required reading:

Big Data and the Future of Privacy
Epic.org

Will Democracy Survive Big Data and Artificial Intelligence?
Scientific American – 25 February 2017

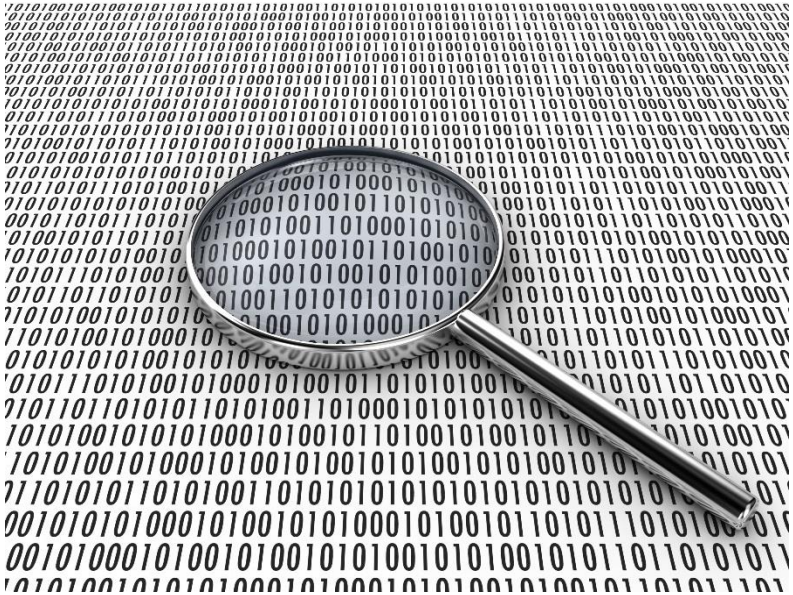
"Muslim registries", Big Data and Human Rights
Amnesty International – 27 February 2017.

What is Big Data

Processing of large and complex data sets.

- **Often with multiple structures.**
- **Data is mined to find trends, relationships, and correlations.**

- **Danger**
  - **By combining information from multiple sources more can be inferred than specifically disclosed.**



Inferences are imprecise

- **The algorithms learn discrimination**

What is Big Data

- Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves.
- Use of Big Data promotes
  - cost reductions
  - time reductions
  - new product development and optimized offerings
  - smart decision making

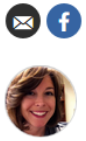
What Data Mining Can Tell Us

Quite a lot, and acting on that information can cause problems.

FEB 16, 2012 @ 11:02 AM 3,122,087 VIEWS

Forbes

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide FULL BIO

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +0.21%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant -- and loyal -- buyers of all things pastel, plastic, and miniature. He talked to Target

Who uses it

- Banking
  - finding new and innovative ways to manage big data
  - understand customers and boost their satisfaction
  - minimize risk and fraud
- Education
  - identify at-risk students
  - make sure students are making adequate progress
  - implement a better system for evaluation and support of teachers and principals
- Government
  - managing utilities
  - running agencies
  - dealing with traffic congestion
  - preventing crime
- Health Care
  - patient records
  - treatment plans
  - Prescription information
- Manufacturing
  - solve problems faster
  - make more agile business decisions
- Retail
  - the best way to market to customers
  - the most effective way to handle transactions
  - the most strategic way to bring back lapsed business

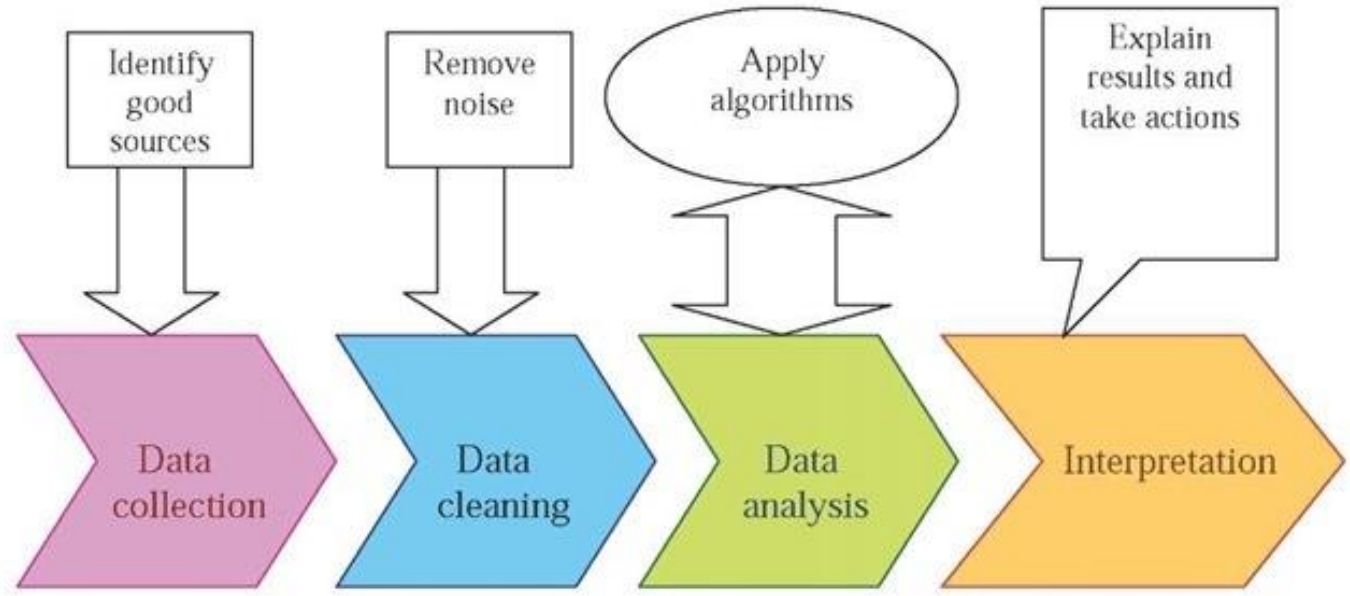
Who uses it

- Case study:

One classic example of the success of big data is the success of House of Cards. Netflix, the distributor of this TV show, collects data from its users and analyze those data. For example, they analyze what kind of show or movie did the users watch, share, and subscribe, therefore make inference about which type of show, which director and actors will be preferred by the users. That's how the director and actors of house of cards are decided. Then, they use algorithm to rank and recommend shows to the users, and most of the time, users will like it.

Steps of Data Mining

- The process of analyzing data from different perspectives and summarizing it into useful information.



Privacy Consideration

- Are users concerned?
  - According to a survey in 2017, about 49% of consumers are less willing to share their personal information. Many consumers are now aware of the dangers of sharing their personal information and the security issues involved by consenting to the sharing of their personal information online.

Privacy Consideration

- (Big data) breaches are big (data breaches).
- The more information used in big data, the more likely it includes personal or sensitive information.
- Sources of information vary greatly, allowing multiple opportunities for exfiltration.
- The distributed processing of big data (e.g. cloud services) increases the attack surface for this data.

Some Area for Risk

- **Personal data protection**
  - Existing methods for protecting identity might be thwarted by Big Data Analysis
- **Financial and legal liabilities**
  - The data you hold may now be more sensitive because of what can be derived through big data analysis.
  - Disovery requests
- **Ethical dilemmas**
  - New ethical dilemmas are being created by the analysis of Big Data

Bias in Big Data

- Confirmation bias
  - Relying on data to confirm a certain hypothesis
- Availability heuristic/availability bias
  - Relying on only data that is readily available or recent.
- Selection bias
  - Sample not representative of the general population
- Confounding variables
  - Relationship between variables is only true when combined with a third (overlooked) variable.

Examples of big data bias

"Predictive policing" in Chicago

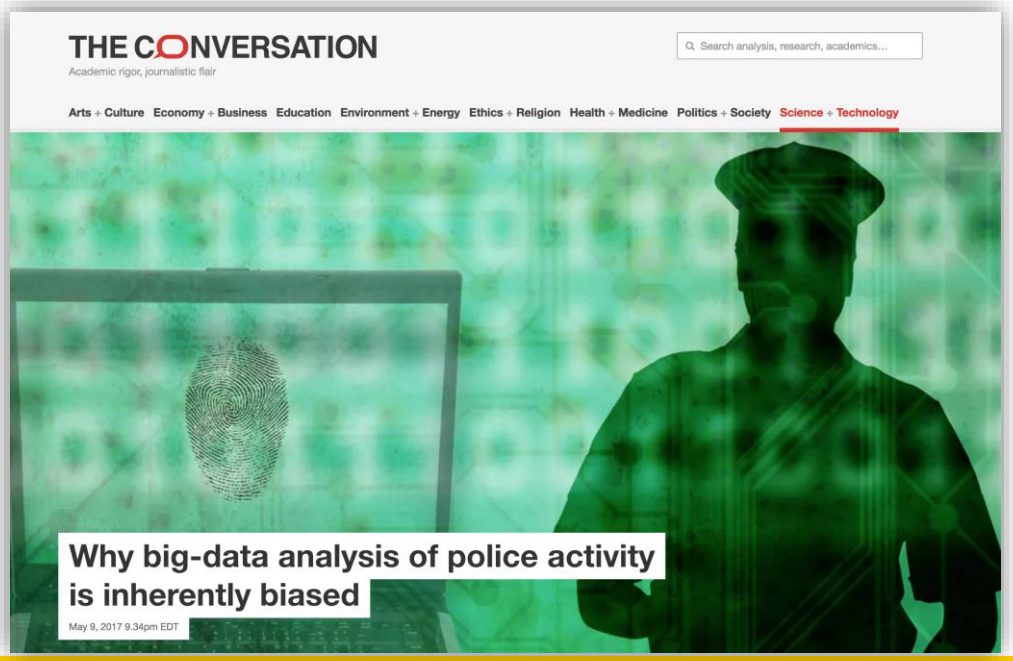
"The Chicago police will use data and computer analysis to identify neighborhoods that are more likely to experience violent crime, assigning additional police patrols in those areas. In addition, **the software will identify individual people who are expected to become – but have yet to be – victims or perpetrators of violent crimes**. Officers may even be assigned to visit those people to warn them against committing a violent crime."

Why big-data analysis of police activity is inherently biased, *The Conversation,* May 9, 2017

Examples of big data bias

Why big-data analysis of police activity is inherently biased, *The Conversation,* May 9, 2017

"Neighborhoods with lots of police calls aren't necessarily the same places the most crime is happening. They are, rather, where the most police attention is – though where that attention focuses can often be biased by gender and racial factors."



Can algorithms illegally discriminate

CNBC – and Whitehouse report

But when it comes to systems that help make such decisions, the methods applied may not always seem fair and just to some, according to a panel of social researchers who study the impact of big data on public and society.

The panel that included a mix of policy researchers, technologists, and journalists, discussed ways in which big data—while enhancing our ability to make evidence-based decisions—does so by inadvertently setting rules and processes that may be inherently biased and discriminatory.

The rules, in this case, are algorithms, a set of mathematical procedures coded to achieve a particular goal. Critics argue these algorithms may perpetuate biases and reinforce built-in assumptions.

Also

http://www.nextgov.com/big-data/2017/02/cfpb-wants-know-how-alternative-data-changes-credit-scores/135695/

Critics allege big data can be discriminatory, but is it really bias?

Pradip Sigdyal | @PSigdyal
Sunday, 8 May 2016 | 4:00 PM ET

CNBC

Getty | 187131740

Big data is increasingly viewed as a strategic asset that can transform organizations through its use of powerful predictive technologies.

But when it comes to systems that help make such decisions, the methods applied may not always seem fair and just to some, according to a panel of social researchers who study the impact of big data on public and society.