INF529: Security and Privacy in Informatics

Criminal law, National Security, and Privacy

Prof. Clifford Neuman

Lecture 10
22 March 2019
OHE 100C
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 – February 15th
• Mid-term, Then more on Government, Politics, and Privacy
• Social Networks and the social contract – March 1st
• Big data – Privacy Considerations – March 8th
• **Criminal law, National Security, and Privacy** – March 22nd
• 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
Homework 2: Big Data, Due 25 March

Consider the articles that have been assigned as readings in the past three weeks (from the website, and from the lecture slides). Based on these readings, and discussions in class, please answer the following question.

Explain how machine learning, data mining, and statistical inference methods can use “big data” about us in ways that are against our personal well-being. How can these techniques uncover (or discover) possibly incorrect information, and how do they create or reinforce profiles and stereotypes that society has long sought to abolish.

Your answer should be roughly four pages in length (about 1600 to 2000 words), but this is not a strict limit. Please submit your answers before noon on Monday 25 March sending your submissions to inf529@csclass.info.
This week - Policing, National Security

- Dewaine Redish – National Security and Privacy
- Andrew Carmer - History of Government Surveillance
- Gene Zakrzewski – NSA Surveillance Programs
March 29 - Civil Law and Privacy

- Arjun Raman – CCPA and related

Also Measuring Privacy

- Sevanti Nag – Measurement of Privacy in Social Media

Monetization of PII
- Ahmed Qureshi
Privacy and National Security
The affects of privacy protections and privacy breaches on the U.S. Department of Defense

Dewaine Reddish
Inf 529
March 2019

“The appearance of U.S. Department of Defense visual information does not imply or constitute DOD endorsement.”
Lesson Objective

- Provide an understanding of how privacy breaches can damage national security. Reinforce with scenarios related to the US DOD.
- Provide an understanding of how privacy legislation and protections can damage national security.

“Security both depends on privacy, and can be improved by doing away with privacy.”
-Lecture 1, INF 529
Agenda

• Background
  • DOD mission statement and composition
  • What is important to the DOD?
  • How important data is protected

• Privacy Breaches & OPSEC Failures
  • OPSEC Primer
  • Geo-location
  • OPM breach
  • Big Data

• Privacy Protection and Legislation
DOD Mission Statement

• The mission of the Department of Defense is to provide the military forces needed to deter war and to protect the security of our country.
What is important to the DOD?
(a) military plans, weapons systems, operations
(b) foreign government information
(c) intelligence activities (including covert action), intelligence sources or methods including cryptology
(d) foreign relations or foreign activities of the United States including confidential sources
(e) scientific, technological, and economic matters relating to the national security
(f) United States Government programs for safeguarding nuclear materials or facilities
(g) vulnerabilities and capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
(h) the development, production, and use of weapons of mass destruction*

*[Ref 1, E.O. 13526, Jan 2010]*
How is DOD information protected?

• Mandatory protection measures/mechanisms
  • NISPOM
  • DoDM
  • RMF / NIST 800-series
  • FIPS

• Restricting number of trusted individuals with access
  • Classification
  • Special Access Programs / Compartments

• Operational Security (OPSEC)

• Trust
  • Individuals eligible to access classified information (as of 2017)
    (Up to Secret) 2,720,832
    (Up to Top Secret) 1,309,793
    (Total) 4,030,625*

*[Ref 4, Office of the Director of National Intelligence, 2018]*
Agenda

• Background
  • DOD mission statement and composition
  • What is important to the DOD?
  • How important data is protected

• Privacy Breaches & OPSEC Failures
  • OPSEC Primer
  • Geo-location
  • OPM breach
  • Big Data

• Privacy Protection and Legislation

*[Ref 5 – US Navy, retrieved Mar 2019]*
Operations Security

- OPSEC is a process that identifies critical information, outlines potential threats and vulnerabilities, assesses risk, and develops countermeasures to safeguard critical information.
Critical Information

Information an adversary would need to do you harm that must be protected

- Names and photos of you, your family and co-workers
- Usernames, passwords, network details
- Job title, location, salary
- Home security systems, internet service provider
- What kind of pets and how many

- Position at work, certifications
- Physical limitations, medical information
- Family routines
- Vacation and travel itineraries
- Social security number, credit cards, banking information
- Hobbies, likes, dislikes, etc.
OPSEC in Social Networking

• What do you display in your social networking profiles?
  – Where you work
  – Where you are
  – Where you have been
  – What you are doing right now
  – Everything that you have done
  – What you like and don’t like
  – Your birthday
  – Your favorite pet
  – Your relationships
  – Your loved ones
  – The people you trust
Data Aggregation

• Information collected from multiple sources
• Open source information collected and analyzed can provide our adversaries with a significant amount of intelligence
• Manchester Document: According to Al 'Qaeda, 80% of their information is collected legally through open sources
  – Internet
  – Trash
  – Media
• Small or seemingly insignificant details pieced together can provide the big picture
What are they looking for?

• Present/future operations
  – Times of operational events
  – Participating units
  – Projected locations

• Information about military facilities
  – Location
  – Number of personnel
  – Ammo depot locations
  – Dates and times of operations

• Technology
  – Development timelines
  – Capabilities and limitations
Geo-location

• Strava user-provided geo-location data exposes US army bases in Afghanistan. *

Nathan Ruser, an analyst with the Institute for United Conflict Analysts, first noted the lapse. The heatmap “looks very pretty” he wrote, but is “not amazing for Op-Sec” – short for operational security. “US Bases are clearly identifiable and mappable.”

“In Syria, known coalition (ie US) bases light up the night,” writes analyst Tobias Schneider. “Some light markers over known Russian positions, no notable colouring for Iranian bases … A lot of people are going to have to sit through lectures come Monday morning.”
Geo-location

- Geo-location device memo was issued on Aug 3, 2018.

- Aims to reduce exposure of sensitive DOD plans and operations.

- "Effective immediately, DoD personnel are prohibited from using geolocation features and functionality on both non-government and government-issued devices, applications, and services while in locations designated as operational areas (OAs)."

* [Ref 2 – Deputy Secretary of Defense, Aug 2018]
Be Vigilant!

- Ensure troop safety
- Avoid compromise and tracking of sensitive locations
- Protect National security
- Protect America

Think OPSEC!
(Operations Security)

- Know your devices’ features and capabilities
- Configure settings to secure your information
- Read manufacturer fine print (i.e., licensing and user agreements)
- Consider opting out for sharing information
- Do not share sensitive information in the wild

Seek and follow local Commander’s guidance

Mobile device tracking can:
- Geolocate you
- Display your location
- Record location history
- Activate by default

Wearable and Mobile
GPS-Enabled Devices

Operations Security
Vigilance

Don’t Let the Enemy
Track You!

DoD 5205.02E, July 2012, DoD Operations Security (OPSEC) Program

“OPSEC. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems.....”

Remember to...
STOP & THINK before you wear or use a mobile device!
Risk?

Risks of GPS mobile and wearable devices

While drilling or exercising at sensitive, forward-deployed military bases, for example, location information may be gathered and transmitted into the wild (i.e., the Internet), providing intercepting adversaries the ability to map activity and locations.

Vulnerabilities?

When you use a mobile device such as a smartphone, fitness monitor, or even an electronic watch, disclosure of your location information is at risk.

Either the mobile device itself, an application on it, or both may be tracking your location!

Things to be aware of:

- Insecure default settings
- Unintentional data sharing
- Untrusted network connections
- Unaware users

Why Should You Care?

GPS-enabled devices make it possible to track individuals as they move while walking, running, or in vehicles. This data by itself may not reveal much; however, when the collected data is aggregated, it could be possible to pick out military installations or troop movements and patterns in places such as the Middle East or other sensitive locations.

Heavily trafficked areas are revealed through data gathered from many individual personal and wearable GPS-enabled devices used in and around these sensitive locations.

U.S. installations that might not have been disclosed previously may be discovered through this aggregated data analysis.

The ENEMY is tracking you
They want to know where you are
KEEP IT TO YOURSELF
Geo-location conclusions

• The need for this memo highlights wide-spread failure of OPSEC programs.
• OPSEC programs are a restriction on national security employee freedoms
OPM Breach

- Approximately 21.5 million records stolen on or before 2014.
- Full SF-86 background investigation data likely exfiltrated.
- FBI Director James Comey stated: [the OPM breach is] “... a very big deal from a national-security perspective and a counterintelligence perspective.” *

*[Ref 7 – Mercury News, July 2015]*
OPM Breach

**Assessment Methods**
- Extensive background investigations
  - Polygraph (TS/SCI)
  - Peer-reported and self-reported adverse information
- Periodic reinvestigations
  - 10 yr for Secret
  - 5 yr for TS or SAP eligibility

**Adverse Information**
- Debt / Affluence
- Foreign Travel
- Foreign Ties / Finances
- Ideology / Patriotism
- Criminal activity
- Extra-marital affairs
OPM Breach conclusions

- Breach likely provided foreign intelligence agencies ability to:
  - Identify targets for coercion
  - Identify targets to hire as informants
  - Identify regions where more sensitive data is being processed (location concentration of T.S. clearance-holders)
  - Understand organizational structures
Big Data

• We’ve discussed how data aggregators and big data analytics have enabled companies to draw conclusions about very private issues.

• The same techniques can be used to identify people in national security positions who are susceptible to blackmail.

• This is available to U.S. adversaries!
Big Data

- Automated Continuous Evaluation System (ACES)
  - Developed by Northrop Grumman for DHS
  - Includes 40 (phase 2) data sources
    - Credit Reports
    - LexisNexis Accurint Reports
    - Federal and State Government Databases
  - Does not include data aggregators or social media input

The data collected is subjected to a set of pre-defined Business Rules, which are developed and refined based upon direction from DHS personnel security adjudicators and policymakers in coordination with DoD PERSEREC. The business rules are used by the system to determine whether or not issues of possible security concern are present. *

*[Ref 8 – DTIC, Nov 2013]*
Agenda

• Background
  • DOD mission statement and composition
  • What is important to the DOD?
  • How important data is protected

• Privacy Breaches & OPSEC Failures
  • OPSEC Primer
  • Geo-location
  • OPM breach
  • Big Data

• Privacy Protection and Legislation
Privacy Protection & Legislation

Protections and legislation impair counterintelligence operations

• Encryption w/o government backdoor
  • Enables covert foreign intelligence operations inside the U.S.
  • Also reduces risk of friendly data compromise

• 4th Amendment
  • National Security Letters
    • Used to gather meta-data on correspondence
    • Shifting legal history - ruled unconstitutional more than once
    • Patriot Act expansion
  • FISA Warrants
    • 948 warrants approved, 34 denied in 2017*

*[Ref 3 – FISA Warrants Issued, July 2015]
References
1 – Executive Order 13526, “Classified National Security Information”
Barack Obama, President of the United States of America, 2010

Patrick Shanahan, Deputy Secretary of Defense, Aug 2018

3 – FISA Court Orders 1979-2017
https://epic.org/privacy/surveillance/fisa/stats/default.html
Epic.org, retrieved Mar 2019

4 – Fiscal Year 2017 Annual Report on Security Clearance Determinations
Office of the Director of National Intelligence, Feb 2018
References

5 – OPSEC Briefing Material  

6 – Fitness Tracking App Gives Away Location of Secret US Army Bases  

7 – Government Hack Exposed 21 Million Social Security Numbers  

8 – The Evolution of the ACES for Personnel Security  
Questions?
Government Surveillance

ANDREW CARMER
INF529 SECURITY AND PRIVACY
MARCH 22, 2019
Topics

- Where did it all start
- 3 Main Techniques
- Court Cases
- 9/11 Events
- Acts
- Pros vs. Cons
- Things to Keep in Mind
Where did it all start?

- 1086 – Domesday Book
  - Ordered by King William I
  - Compilation of every individual and parcel of land in England
  - Served as the first Census
  - Was used mainly for tax purposes/determine what taxes were owed to the king
  - Was also used as a political weapon for any rebels
Wiretapping

- Late 1800’s
  - Union and Confederacy tapped into each others telegraph lines
  - They copied down every message being sent
  - Major Young of the Union Army, commandeered enemy captured telegraph lines to misdirect supply trains intended for General Lee’s army
  - Anyone with a portable key set and knew Morse code could listen to these messages
  - Invention of the telephone mitigated this as information was flowing too fast
Keystroke Logging

- Keylogging is the act of recording key presses on a keyboard, mainly used to snoop passwords and other sensitive information.
- Can be either software or physical that plug into a USB or PS/2 port.
- As early as 1970’s
  - Russian spies found a way to bug IBM Selectric typewriters used by US diplomats.
  - The keystrokes were transmitted via radio frequency signals.
  - 16 typewriters used from 1976-1984 at the US embassy in Moscow and Leningrad were found to have keyloggers.
- 2015
  - HP laptops were found to have an audio driver.
  - Keylogger was found embedded in GTAV.
Encryption Backdoors

- Allows an intruder to access the encrypted information without having the correct credentials
- 2007’s NIST Special Publication 800-90 included a secret backdoor on behalf of the NSA
- 800-90 describes four techniques for Deterministic Random Bit Generators (DRBG)
  - Hash functions, HMAC, block ciphers, and elliptic curves
- Researchers discovered constants used within the DUAL-EC-DRBG standard have a relationship with a secret set of numbers
- Anyone who knows these numbers can predict the output of the DRBG and break the encryption schemes
- NSA pushed hard to have the elliptic curve put into the standard even though it was substantially slower than the other 3
Black Chamber

- 1920’s
  - Considered to be the predecessor to the NSA
  - Consisted of Army codebreakers
  - Monitored international telegraphs for anything that could affect national security
  - Asked major telegraph companies for these telegraphs; Western Union happily obliged
  - Funding for this program ended in 1929
Tapping into Telephone Lines

- US Government routinely tapped phones in the early years of the technology (late 1800’s)
- During Prohibition, evidence that was gather mostly through wiretapping was used in the 1928 Supreme Court case Olmstead v. United States
- This case shutdown the largest bootlegging operations in the country
- Established that federal agents could legally wiretap private telephone conversations without judicial approval; this was overturned in 1967 in Katz v. United States
Olmstead v. United States (1928)

- The court reviewed whether the use of wiretapped private telephone conversations obtained by federal agents without judicial approval constituted as violation of Fourth and Fifth amendment rights.
- Roy Olmstead was convicted for alleged conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting, and selling alcohol.
- Roy was the GM of the entire operation of using sea vessels for transportation and running an underground storage facility in Seattle.
- Prohibition officers installed wiretapping equipment in the streets near the houses and in the basement of the large office building.
- This equipment intercepted messages by Roy Olmstead and his employees.
- Ruled by 5-4 that no laws were broken as the officers did not trespass on the homes or offices of the defendants.
Katz v. United States (1967)

- Landmark US Supreme Court case discussing the nature of the “right to privacy” as well as the legal definition of “search” in reference to electronic-based communications.

- Charles Katz used a public pay phone booth to transmit illegal gambling wagers from LA to Miami and Boston.

- The FBI attached an electronic eavesdropping device to the outside of the exterior of the phone booth which were recording conversations; he was convicted based on these recordings.

- Appealed the conviction, arguing it violated his Fourth Amendment rights which the Court of Appeals sided with the FBI because there was no physical intrusion into the phone booth itself.

- In the end, the court ruled 7-1 in favor of Katz stating whoever occupied a telephone booth, shuts the door behind them, and pays the tool that permits them to place a call is entitled to assumed their conversation will not be broadcast to the world.
Escalation after 9/11

- “We will come together to strengthen our intelligence capabilities to know the plans of terrorists before they act and to find them before they strike.” - President Bush September 20, 2001

- Bulk domestic spying in the US increased dramatically

- In an attempt to prevent future attacks, the Patriot Act was passed
  - Allows investigators to use the tools already available to investigate organized crime and drug trafficking
  - Facilitated information sharing and cooperation among government agencies
  - Updated laws to reflect new technologies and threats
  - Increased the penalties for those who commit terrorist crimes

- Defense Advanced Research Projects Agency (DARPA) initiated “Total Information Awareness” which was a surveillance program for recording and analyzing all digital information generated by all US citizens

- Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments of 2008 were driven by 9/11 as well
Foreign Intelligence Surveillance Act (FISA) of 1978

- Enacted in 1978 set forth procedures for physical and electronic surveillance and collection of foreign intelligence information
- Initially only addressed electronic surveillance but has been significantly amended
- FISA Amendments Act of 2008 added a new title concerning additional procedures for acquiring the communications of certain persons outside the United States
- Protections for Electronic Communication Service Providers
- Requires semiannual reports from the AG to the IC and judiciary committees
Mass Surveillance Disclosures

- 2013 is when whistleblowers started to come to light more
- The government aggressively tried to dismiss and challenge Fourth Amendment cases caused by these leaks such as: Hepting v. AT&T, Jewel v. NSA, Clapper v. Amnesty International
- The government was able to grant retroactive immunity to ISPs participating in domestic surveillance
- On December 26, 2013 US district court judge for DC, Richard Leon, declared that collection of metadata of Americans’ telephone records by the NSA probably violates the fourth amendment
USA Freedom Act (2015)

- Signed into law June 2, 2015 which is a day after certain provisions of the Patriot Act had expired
  - No longer are able to obtain a roving wiretap, they must obtain a new warrant for each device
- Mandated an end to bulk collection of phone call metadata by the NSA within 180 days
- Still allowed this collection of metadata by phone companies with access by the government with a case-by-case approval from the Foreign Intelligence Surveillance Court
Government Surveillance

- **Pros**
  - The ability to trace and check communications for criminals and terrorists can help avoid crimes and save lives
  - Implicit deterrance factor: terrorists/offenders find it difficult to plan and organize their crimes
  - Information collected can help understand different aspects of society

- **Cons**
  - “Big Brother” pushes the idea that the government can control the minds of citizens and remove privacy altogether
  - Data collected can be used for other purposes other than collecting; potential blackmail or have an unfair advantage in business deals
  - The programs are expensive meaning the governments resources could deviate from other beneficial policies
Things to Keep in Mind

- Mass surveillance is different from broad data collection
  - If a bomb goes off somewhere and officials are looking at videos around the area that it happened, this is due to an event that occurred
- It hasn’t been proven that mass surveillance has stopped any terrorist attacks
  - Umar Farouk Abdulmutallab’s father contacted the Embassy in Nigeria with concerns his son might be planning an attack; Abdulmutallab was able to board a plane and come to the United States with no issues
- In 2009, $146 million of taxpayer money went to funding a single program to buy new hardware, contract support, and make payments to phone companies for helping out; the program was abused for years and there is no evidence this program was able to stop terrorists
References

- https://www.ancient.eu/Domesday_Book/
- https://en.wikipedia.org/wiki/Katz_v._United_States
- https://en.wikipedia.org/wiki/Olmstead_v._United_States
- https://www.justice.gov/archive/ll/highlights.htm
- https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286
- https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/
INF529: Security and Privacy In Informatics

NSA Surveillance Programs

Gene Zakrzewski

Criminal law, National Security, and Privacy
March 22, 2019
Spy vs Spy

- When is it spying & when is it surveillance?
  - According to Wikipedia, “espionage or spying, is the act of obtaining secret or confidential information without the permission of the holder of the information. Spies help agencies uncover secret information.” usually for military purposes. [https://en.wikipedia.org/wiki/Espionage](https://en.wikipedia.org/wiki/Espionage)

  - According to Merriam-Webster, surveillance is close watch kept over someone or something (as by a detective); also : supervision. [https://www.dictionary.com/browse/surveillance](https://www.dictionary.com/browse/surveillance)

- Is the NSA guilty of spying?
Privacy and Security

• Credible accounts of NSA's domestic spying program can found in the media, official government statements and reports, and court actions. Leaked documents confirmed the domestic spying by the NSA. After Edward Snowden’s disclosure numerous bills have been written in order to restore public trust.

• According to Washington Post article published in 2013, “When it comes to allowing infringements on personal privacy to investigate terrorist threats, Americans now divide 57 percent for unfettered investigations and 33 percent on the side of sacrosanct privacy.”

The NSA is responsible for:

- global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT).

- protection of U.S. communications networks and information systems.

The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine.

The NSA does not publicly conduct human-source intelligence gathering.

In 2013, Snowden was hired by an NSA contractor, Booz Allen Hamilton, after previous employment with Dell and the CIA.

On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii, and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill.

Many members of Congress believed that in the wake of the Snowden disclosures, restoration of public trust would require legislative changes. Many bills have been written since the disclosures began with the goal of clarifying government surveillance powers.

The Foreign Intelligence Surveillance Court was established by Congress in 1978, aka *FISA Court*.

The Court entertains applications made by the United States Government for:
- approval of electronic surveillance,
- physical search and,
- certain other forms of investigative actions for foreign intelligence purposes.

https://www.fisc.uscourts.gov/
FISA: Protecting Americans from Domestic Spying

• In 1978, Foreign Intelligence Surveillance Act (FISA) Signed Into Law
  • Protecting Americans from Domestic Spying

• In 2006, FISA Court Approves First Section 215 Order Authorizing Mass Collection of Calling Records.
  • Foreign Intelligence Surveillance Court Okays Surveillance of Telephony Metadata for First Time Ever

• In 2008, FISA Amendments Act reauthorized similar expired provisions in Protect America Act of 2007
  ❖ Section 702: Allows the Attorney General and the Director of National Intelligence to authorize surveillance on “persons reasonably believed to be located outside the United States” for up to one year
  ❖ Sections 802 and 803: Provides legal immunity to telecom companies for assisting intelligence community
Patriot Act

• In 2001, USA PATRIOT Act is an Act of Congress signed into law by United States President George W. Bush
  • The Act's full title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001".
  • Many of the act's provisions were to sunset beginning December 31, 2005
• In 2005, the U.S. Senate passed a reauthorization bill
  • The bill has substantial changes to several of the USA PATRIOT Act sections, while the House reauthorization bill kept most of the act's original language.
• In 2011, President Obama signed the PATRIOT Sunsets Extension Act
  • A four-year extension of three key provisions in the Act: roving wiretaps, searches of business records, and conducting surveillance of "lone wolves"—individuals suspected of terrorist-related activities not linked to terrorist.

Wikipedia: The Patriot Act
Here are five key points about the PATRIOT Act:

1. It protects civil liberties and provides for the common defense.
2. Expectation of privacy is not unlimited.
3. The law provides significant safeguards.
4. It has passed constitutional muster.
5. Disagreements over the role of government are different from actual abuse.

The PATRIOT Act and the Constitution: Five Key Points
by Jena Baker McNeill, Feb 10, 2011
USA Freedom Act

- The USA Freedom Act (H.R. 2048, Pub.L. 114–23) is a U.S. law enacted on June 2, 2015 that restored in modified form several provisions of the Patriot Act, which had expired the day before.

- The bill was originally introduced in both houses of the U.S. Congress on October 29, 2013, following publication of classified NSA memos describing bulk data collection programs leaked by Edward Snowden that June.

- The title of the act originally was a ten-letter “backronym” that stood for Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act.

USA Freedom Act – things to know

• The NSA will be able to collect data for all the phone numbers in contact with the suspect number, and all the numbers in contact with those numbers.

• The expired provision including the **roving wiretap provision**, which allows the FBI to eavesdrop on espionage and terror suspects who discard cell phones frequently, will go back into effect, as will the **lone-wolf provision**, which has never been used.

• The new law gives **private companies more leeway** to publicly report information about the number of national security surveillance demands they receive. It requires declassification of FISA Court opinions.

• It addresses the most controversial program Edward Snowden revealed, the **domestic phone records collection**. But it does nothing to affect another major Snowden revelation: the NSA’s collection of foreign Internet content from U.S. tech companies, a program that sweeps up lots of American communications.

PBS NEWS HOUR- [https://www.pbs.org/newshour/politics/questions-answers-newly-approved-usa-freedom-act](https://www.pbs.org/newshour/politics/questions-answers-newly-approved-usa-freedom-act)
A chart prepared by the NSA underscores the breadth of the data it is able to obtain: email, video and voice chat, videos, photos, voiceover IP (Skype, for example) chats, file transfers, social networking details, and more.

http://www.theguardian.com/world/2013/jun/06/ustechgiantsnsadata
Glenn Greenwald and Ewen MacAskill
The Guardian, Thursday 6 June 2013
Some of the world's largest internet brands are claimed to be part of the information sharing program since its introduction in 2007.

- Microsoft – which is currently running an advertising campaign with the slogan "Your privacy is our priority" – was the first, with collection beginning in December 2007.
- It was followed by Yahoo in 2008; Google, Facebook and PalTalk in 2009; YouTube in 2010; Skype and AOL in 2011; and finally Apple, which joined the program in 2012.
- The program is continuing to expand, with other providers due to come online.

http://www.theguardian.com/world/2013/jun/06/ustechgiantsnsadata.

Glenn Greenwald and Ewen MacAskill
The Guardian, Thursday 6 June 2013
The NSA may end its controversial phone data surveillance program
Edward Snowden exposed the program

- The National Security Agency may shut down a controversial program that vacuums up hundreds of millions of call and text message records.

- A senior Republican aide who appeared on a Lawfare blog podcast said the Trump administration had let the program stagnate in recent months and was considering ending it altogether. The comments were first noted by The New York Times.

- As recently as last year, the program was still causing controversy. The NSA said at the time that it would delete a massive database of records after inadvertently gathering more data than it was authorized to receive.

The Verge, By Colin Lecher@colinlecher Mar 5, 2019, 10:00am EST
Other NSA Global Surveillance Programs

- **MYSTIC** is a former secret program used to collect the metadata as well as the content of phone calls from several countries.

- **DISHFIRE** is a covert global surveillance collection system and that collects hundreds of millions of text messages on a daily basis from around the world.

- **Bullrun** (decryption program) is a clandestine, highly classified program to crack encryption of online communications and data.

- **ECHELON** is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the US with the aid of four other signatory nations to the, also known as the Five Eyes.

- **XKeyscore (XKEYSCORE or XKS)** is a formerly secret computer system for searching and analyzing global Internet data.

Reference Wikipedia and the associated links
Pro NSA Surveillance

Washington Post columnist, Marc. A Thiessen, continues to argue that those who criticize the NSA program believing it to be “unacceptable,” need to acknowledge **there is no other effective way to protect the country.**

He explains that there are only three methods to “get information to prevent terrorist attacks:”

1. Interrogation (questioning)
2. Penetration (infiltration)
3. Intelligence (monitoring communications)

http://www.people.fas.harvard.edu/~stephaniecampbell01/ProsOfNSASurveillance.html
PRO NSA Surveillance

U.S. President Obama defends the NSA program by quoting specific congressional and federal judicial negligence by the Foreign Intelligence Surveillance Court (FISC), but Obama neglects to respond to the demands for increased transparency for the U.S. public from members of the senate and the house.

http://www.people.fas.harvard.edu/~stephaniecampbell01/ProsOfNSASurveillance.html,
Expanded Look – ‘Section 702’ Saves Lives, Protects the Nation and Allies

NSA
December 17, 2017

This law, NSA Section 702 has played both a unique and decisive role in national defense.

- reporting helped thwart the efforts of front companies seeking to obtain weapons probably bound for a rebel group in the Middle East.

- provided details concerning a hostile nation’s efforts to directly supply another hostile regime with war material and collection also revealed military training occurring between the nations.

- identify cybersecurity information relating to a hostile foreign government.

- proliferation of military communications equipment and sanctions-evasion activity by a sanctions-restricted country.

- obtain intelligence on a foreign government’s state-sponsored phone application that impacted cybersecurity and was not publicly known.

- received information from a partner nation concerning the activities of an extremist, who aspired to either travel to the Middle East in order to join an extremist group, or conduct a terrorist attack on European soil.
CON NSA Spying

• NSA incorrectly believes to have the right to record every phone call made by every U.S. citizen on any day; however, this violates:
  • Amendment IV of the U.S. Constitution that “prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned,” and
  • Amendment I that prohibits any law infringing on the “freedom of speech” of any U.S. citizen.

• The public is also not informed on how the Patriot Act is being used

• History has shown that powerful government surveillance tools are almost always abusively used

• Constitution makes it so the government should be transparent to the people, not vice versa.

http://www.people.fas.harvard.edu/~stephaniecampbell01/ConsOfNSASurveillance.html
Privacy and Surveillance

The American Civil Liberties Union

Privacy today faces growing threats from a growing surveillance apparatus that is often justified in the name of national security. Numerous government agencies—including the National Security Agency, the Federal Bureau of Investigation, the Department of Homeland Security, and state and local law enforcement agencies—intrude upon the private communications of innocent citizens, amass vast databases of who we call and when, and catalog “suspicious activities” based on the vaguest standards.

The government’s collection of this sensitive information is itself an invasion of privacy. But its use of this data is also rife with abuse. Innocuous data is fed into bloated watchlists, with severe consequences—innocent individuals have found themselves unable to board planes, barred from certain types of jobs, shut out of their bank accounts, and repeatedly questioned by authorities. Once information is in the government’s hands, it can be shared widely and retained for years, and the rules about access and use can be changed entirely in secret without the public ever knowing.

Our Constitution and democratic system demand that the government be transparent and accountable to the people, not the other way around. History has shown that powerful, secret surveillance tools will almost certainly be abused for political ends and turned disproportionately on disfavored minorities.

The ACLU has been at the forefront of the struggle to prevent the entrenchment of a surveillance state by challenging the secrecy of the government’s surveillance and watchlisting practices; its violations of our rights to privacy, free speech, due process, and association; and its stigmatization of minority communities and activists disproportionately targeted by surveillance.

https://www.aclu.org/issues/national-security/privacy-and-surveillance
In 1791 the Bill of Rights went into affect, the fourth amendment prohibits unreasonable searches and seizures along with requiring any warrant to be judicially sanctioned and supported by probable cause.

Fourth Amendment: *The right of persons 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.*

“Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither.”
The National Security Agency (NSA) is a national-level intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence. The NSA is responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT). The NSA is also tasked with the protection of U.S. communications networks and information systems. The NSA relies on a variety of measures to accomplish its mission, the majority of which are clandestine.

Originating as a unit to decipher coded communications in World War II, it was officially formed as the NSA by President Harry S. Truman in 1952. Since then, it has become the largest of the U.S. intelligence organizations in terms of personnel and budget. The NSA currently conducts worldwide mass data collection and has been known to physically bug electronic systems as one method to this end. The NSA has also been alleged to have been behind such attack software as Stuxnet, which severely damaged Iran’s nuclear program. The NSA, alongside the Central Intelligence Agency (CIA), maintains a physical presence in many countries across the globe; the CIA/NSA joint Special Collection Service (a highly classified intelligence team) inserts eavesdropping devices in high value targets (such as Presidential palaces or embassies). SCS collection tactics allegedly encompass "close surveillance, burglary, wiretapping, [and] breaking and entering".

Unlike the CIA and the Defense Intelligence Agency (DIA), both of which specialize primarily in foreign human espionage, the NSA does not publicly conduct human-source intelligence gathering. The NSA is entrusted with providing assistance to, and the coordination of, SIGINT elements for other government organizations – which are prevented by law from engaging in such activities on their own. As part of these responsibilities, the agency has a co-located organization called the Central Security Service (CSS), which facilitates cooperation between the NSA and other U.S. defense cryptanalysis components. To further ensure streamlined communication between the signals intelligence community divisions, the NSA Director simultaneously serves as the Commander of the United States Cyber Command and as Chief of the Central Security Service.
• In 2013, Snowden was hired by an NSA contractor, Booz Allen Hamilton, after previous employment with Dell and the CIA. On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii, and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill.

• Snowden came to international attention after stories based on the material appeared in The Guardian and The Washington Post. Further disclosures were made by other publications including Der Spiegel and The New York Times.

• NSA Director Keith Alexander initially estimated that Snowden had copied anywhere from 50,000 to 200,000 NSA documents. Later estimates provided by U.S. officials were on the order of 1.7 million.

• Many members of Congress believed that in the wake of the Snowden disclosures, restoration of public trust would require legislative changes. More than 20 bills have been written since the disclosures began with the goal of clarifying government surveillance powers.

Here are five key points about the PATRIOT Act:

1. **It protects civil liberties and provides for the common defense.** The Constitution requires the President and Congress to respect and defend individual civil liberties but also provide for the common defense.

2. **Expectation of privacy is not unlimited.** The Supreme Court has ruled that Americans enjoy a “reasonable” expectation of privacy; however, this is not an unlimited expectation of privacy.

3. **The law provides significant safeguards.** It ensures that national security investigators have the same tools at their disposal to investigate terrorists that law enforcement agents have to investigate and prosecute drug dealers and rapists. These tools come with significant procedural safeguards, oversight, and reporting requirements and are subject to routine and aggressive oversight by the FISA court and Congress.

4. **It has passed constitutional muster.** No single provision of the PATRIOT Act has ever been found unconstitutional.

5. **Disagreements over the role of government are different from actual abuse.** Mere expansion of executive authority in the context of national security investigations alone does not in itself create actual abuse. However, careful monitoring and vigilant oversight are oftentimes the answer to potential abuses of power—not all-out prohibition.

The PATRIOT Act and the Constitution: Five Key Points
by Jena Baker McNeill, Feb 10, 2011
USA Freedom Act – 6 things to know

Q: What happens with the phone records collection?

A: It will resume for six months, provided that the Foreign Intelligence Surveillance Court orders phone companies to turn over the records and that no court stops it under various pending lawsuits. During that period, the NSA will seek to work with providers to come up with a way to quickly query their records against known terrorist phone numbers, pursuant to a court order. It will be able to collect data for all the numbers in contact with the suspect number, and all the numbers in contact with those numbers. So the NSA will still be rooting around in Americans’ phone records, but it won't be collecting all of them.

Q: What about the American calling records the NSA has been collecting for years?

A: Obama administration officials have not said what they will do with those and whether they will continue to search them.

Q: What about the other surveillance provisions that expired?

A: The roving wiretap provision, which allows the FBI to eavesdrop on espionage and terror suspects who discard cell phones frequently, will go back into effect, as will the lone-wolf provision, which has never been used. The FBI will still be able to use Section 215 of the Patriot Act to collect a variety of business records in national security investigations. But the new law requires the government to limit the scope of its collection, prohibiting it from grabbing, for example, all information relating to a particular service provider or area code.

PBS NEWS HOUR- [https://www.pbs.org/newshour/politics/questions-answers-newly-approved-usa-freedom-act](https://www.pbs.org/newshour/politics/questions-answers-newly-approved-usa-freedom-act)
USA Freedom Act – 6 things to know

Q: What else will change under the USA Freedom Act?

A: The new law gives private companies more leeway to publicly report information about the number of national security surveillance demands they receive. And it requires declassification of FISA Court opinions containing significant legal decisions, or a summary if declassification is not possible. That is designed to prevent secret interpretations such as the one that allowed bulk collection of U.S. phone records.

Q: Does this legislation address the concerns raised by the disclosures of former NSA contractor Edward Snowden?

A: It addresses the most controversial program he revealed, the domestic phone records collection. But it does nothing to affect another major Snowden revelation: the NSA’s collection of foreign Internet content from U.S. tech companies, a program that sweeps up lots of American communications. And it doesn’t address the bulk of Snowden disclosures about foreign intelligence gathering and the NSA’s attempts to exploit technology, such as encryption, for the benefit of U.S. intelligence.

Q: Who are the political winners and losers coming out of this legislative fight?

A: Winners include Obama, who proposed this idea more than a year ago to assuage public concerns about surveillance, and congressional Democrats, who backed it. The biggest loser by any measure is Senate Majority Leader Mitch McConnell, R-Ky., who opposed the USA Freedom Act and thought he could force the House to accept a last-minute extension of current law.

PBS NEWS HOUR- https://www.pbs.org/newshour/politics/questions-answers-newly-approved-usa-freedom-act
Global Surveillance

• Systems

  “MYSTIC is a former secret program used since 2009 by the US National Security Agency (NSA) to collect the metadata as well as the content of phone calls from several countries. The program was first revealed in March 2014, based upon documents leaked by Edward Snowden.”
How the NSA can 'turn on' your phone remotely – CNN Money June 6 2014 - Jose Pagliery

Even if you power off your cell phone, the U.S. government can turn it back on. That's what ex-spy Edward Snowden revealed in last week's interview with NBC's Brian Williams. It sounds like sorcery. Can someone truly bring your phone back to life without touching it?

No. But government spies can get your phone to play dead. It's a crafty hack. You press the button. The device buzzes. You see the usual power-off animation. The screen goes black. But it'll secretly stay on -- microphone listening and camera recording.
Other Global Surveillance Programs

- According to Wikipedia, **ECHELON**, originally a secret government code name, is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the US with the aid of four other signatory nations to the UKUSA Security Agreement: Australia, Canada, New Zealand and the United Kingdom, also known as the Five Eyes.

- According to Wikipedia **XKeyscore (XKEYSCORE or XKS)** is a formerly secret computer system first used by the United States National Security Agency for searching and analyzing global Internet data, which it collects on a daily basis. The program has been shared with other spy agencies including the Australian Signals Directorate, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau, Britain's Government Communications Headquarters, Japan's Defense Intelligence Headquarters and the German Bundesnachrichtendienst.
Surveillance Devices

• According to Wikipedia, the **StingRay phone tracker** is an IMSI-catcher, a controversial cellular phone surveillance device, manufactured by Harris Corporation. Initially developed for the military and intelligence community, the StingRay and similar Harris devices are in widespread use by local and state law enforcement agencies across Canada, the United States, and in the United Kingdom. Stingray has also become a generic name to describe these kinds of devices.
NSA Surveillance Reports

- In 2001, the NSA’s classified domestic surveillance program, was implemented by President George W. Bush shortly after the 911 attacks.

- The New York Time in 2005 reported:
  - What the agency calls a "special collection program" began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda operatives overseas, including Abu Zubaydah, who was arrested in Pakistan in March 2002. The C.I.A. seized the terrorists' computers, cellphones and personal phone directories, said the officials familiar with the program. The N.S.A. surveillance was intended to exploit those numbers and addresses as quickly as possible, they said.
  - In the weeks after 9/11, President Bush authorized the National Security Agency (NSA) to conduct a range of surveillance activities inside the United States, which had been barred by law and agency policy for decades.
  - Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation. Under the special program, the agency monitors their international communications, the officials said. The agency, for example, can target phone calls from someone in New York to someone in Afghanistan.

The U.S. Intelligence Community relies on Section 702 of the Foreign Intelligence Surveillance Act in the constant hunt for information about foreign adversaries determined to harm the nation or our allies. The National Security Agency (NSA), for example, uses this law to target terrorists and thwart their plans.

In a time of increasing cyber threats, Section 702 also aids the Intelligence Community’s cybersecurity efforts.

Under Section 702, the government cannot target a U.S. person anywhere in the world, or any person located in the United States.

Under Section 702, NSA can target foreigners reasonably believed to be located outside the United States only if it has a basis to believe it will acquire certain types of foreign intelligence information that have been authorized for collection.

This law has played both a unique and decisive role in national defense. For example:

- NSA Section 702 reporting helped thwart the efforts of front companies seeking to obtain weapons probably bound for a rebel group in the Middle East that is hostile to U.S. interests. Information derived from Section 702 was shared with a European government, which prompted that government to prevent a nearly $1 million shipment of weapons and ammunition. This European government also revoked the export license of multiple arms companies based on the intelligence.
NSA – Section 702

- During 2016, Section 702 collection provided NSA unprecedented details concerning a hostile nation’s efforts to directly supply another hostile regime with war material. Section 702 collection also revealed military training occurring between the nations.
- In 2016, using Section 702, NSA was able to identify cybersecurity information relating to a hostile foreign government. NSA was able to identify the specific foreign individuals and observe their tactics, techniques and procedures. By identifying the actors and their tactics, NSA gained an understanding of the foreign adversary that would help NSA stop malicious cyberattacks if they were to be used against the United States.
- NSA uses Section 702 to develop a body of knowledge regarding the proliferation of military communications equipment and sanctions-evasion activity by a sanctions-restricted country. Additionally, Section 702 collection provided foreign intelligence information that was key to interdicting shipments of prohibited goods by the target country.
- In 2016, thanks in part to NSA’s Section 702 collection technique, NSA was able to obtain intelligence on a foreign government’s state-sponsored phone application that impacted cybersecurity and was not publicly known. Because of this discovery, the app was ultimately removed from the various phone application marketplaces.
- In late September 2015, NSA received information from a partner nation concerning the activities of an extremist, who aspired to either travel to the Middle East in order to join an extremist group, or conduct a terrorist attack on European soil. Based on that tip, NSA used Section 702 collection to acquire the communications of the extremist. Specifically, NSA obtained a number of the extremist’s communications, which allowed NSA to tip the partner nation to the individual’s plans to carry out an attack on a public area. This timely foreign intelligence information assisted partner nation authorities with pinpointing the extremist’s location and activities. NSA was credited by the partner with providing key information for the investigation, which resulted in the extremist’s overseas arrest.
- Section 702 collection is critical to understanding strategic plans and intentions of foreign adversary militaries and is extremely valuable when developing countermeasures to mitigate the threat posed by those adversaries. During 2015, NSA used Section 702 to gather unprecedented details concerning military weapon systems research, development and testing by a hostile foreign power. This information allows the U.S. military, if desired, to create a functional duplicate of the system, providing a significant strategic and tactical advantage.
NSA – Section 702

- NSA uses Section 702 to acquire extensive insight into the highest level decision-making of a Middle Eastern government. This reporting from Section 702 collection provided U.S. policymakers with the clearest picture of a regional conflict and, in many cases, directly informed U.S. engagement with the country. Section 702 collection provides NSA with sensitive internal policy discussions of foreign intelligence value.
- NSA, over a two-year period, used Section 702 to develop a robust body of knowledge about the personal network of an individual providing support to a leading terrorist in Iraq and Syria. This “leading terrorist” practiced strict operational security, and thus it was necessary to study the target by identifying key operatives throughout his network to understand not only the plans and intentions of the terrorist leader, but also to attempt to track his movements. Section 702 collection provided the necessary information for tactical teams to conduct a successful military operation, removing the terrorist from the battlefield. This information was critical to the discovery and disruption of this threat to the U.S. and its allies.
- NSA produced a body of reporting based on Section 702 collection highlighting the 2015 travel of several extremists from the Middle East to Europe, likely for the purpose of conducting terror attacks. One of these travelers was directed by and maintained contact with one of the planners of the 2015 Paris attacks, reporting the problems and difficulties he encountered throughout his journeys. NSA provided identifying information to foreign partners, who located and detained the individual who now faces terrorism charges.
- NSA used Section 702 collection to reveal the identities of the overseas terrorists responsible for a 2016 attack which resulted in more than 20 deaths. NSA’s Section 702 collection provided the necessary insight and reporting on the attack that refuted the terrorist organization’s denial of any involvement. Specifically, Section 702 collection provided a direct claim of responsibility from the terror group’s leaders and included a list of the terrorists trained for the operation. This reporting was crucial for supporting timely U.S. and coalition force planning and operations against terrorists in the region.
• In mid-to-late 2015, while monitoring terrorists and associates active in the Middle East, NSA used collection authorized under Section 702 to monitor an individual targeting specific U.S. and Western individuals. Section 702 allowed NSA to understand some of the plans and intentions of the operative, and it helped determine his whereabouts. This information was critical to the discovery and disruption of this threat to Americans and allies.

• Section 702 has been critical to monitoring the activities of potential suicide bombers who threaten U.S. forces in Afghanistan. For example, in June 2016, NSA's timely reporting based on Section 702 collection enabled U.S. and coalition forces to detain a potential suicide bomber and seize various IED components, disrupting planned attacks on U.S. convoys and a U.S. base in Northern Afghanistan.

• Section 702 enables NSA to protect U.S. government networks by providing unique cybersecurity insights. For example, Section 702 collection provided significant understanding of specific cybersecurity vulnerabilities of networks and infrastructure. This discovery helped to defend against these vulnerabilities.

• Section 702 collection allowed NSA to discover key cybersecurity information concerning actors who planned to use United States infrastructure to enable spearphishing techniques on multiple targets that could have resulted in the compromise of personal and sensitive information.

• Section 702 collection enables NSA to monitor the expansion of terrorist groups in Southeast Asia. During 2013 and 2014, Section 702 collection provided information that terror groups in Southeast Asia planned attacks against U.S. interests in the region and enabled warnings to be issued to the appropriate locations.

• NSA analysis of Section 702 collection discovered the communications of a member of a major terrorist group in the Middle East who was communicating with an extremist in Europe who was sharing ideas on how to commit a terrorist attack. Specifically, NSA discovered communications where the individual in Europe was discussing with the terrorist buying material to build a suicide belt. NSA shared this critical information with European partners in an attempt to disrupt further attacks against U.S. and allied interests.
CON NSA Spying

Under the patriot act, NSA incorrectly believes to have the right to record every phone call made by every U.S. citizen on any day; however, this right was not granted by Congress and also violates the Amendment IV of the U.S. Constitution that “prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned,” and Amendment I that prohibits any law infringing on the “freedom of speech” of any U.S. citizen.

The public is also not informed on how the Patriot Act is being used and in response to this, there are motions asking the NSA to release its opinions on the program and the use of collected citizen information.

This particular “invasion of privacy” is concerning because history has shown that powerful government surveillance tools are almost always abusively used, and also the Constitution makes it so the government should be transparent to the people, not vice versa.

The U.S. government succeeded in making major telecommunication companies, such as AT&T and Sprint, hand over the personal information and call logs of all their customers with the purpose of making a national call database. Next, NSA receive the green-light to install surveillance equipment in these major telecommunication companies which gave the government real time access to phone calls and messages. They did so by installing “fiber-optic splitters” in order to intercept communications between the sender and the receiver and send the message to the government as well as the receiver.

http://www.people.fas.harvard.edu/~stephaniecampbell01/ConsOfNSASurveillance.html
Social Media and Free Speech


Why is it difficult to block such content
What is the appropriate line to draw
How is social media used for radicalization
The role social media plays in events like this is that it amplifies the emotions and the reach of communication about the attack, and that plays into the hands of the those committing these crimes. Terrorists seek to create as much fear as they can and they also seek to recruit those that can be radicalized to their cause.

Social media provides a platform through which their communications have greater reach, and in this case they have learned how the use of certain keywords will further expand the reach of their ideology.

The technology of social media also increases the speed through which their message spreads, making it harder for the social media platform providers to block access, take down messages, or otherwise act upon the communications using their platforms.
Social Media and Free Speech

From a technology perspective, there is so much content communicated on the major social media platforms that it is difficult for them to catch all instances of inappropriate content. Perhaps one thing that might need to change is that filtering, perhaps even human review, might need to be added based on the expected reach of the communication, i.e. those items that will be widely viewed because they trigger widely used keywords, could receive greater attention.

This would still leave the free speech issues. There have been instances where accounts and communications from political campaigns and politician's have been blocked, and the social media companies have in most of those cases reversed their initial action. While I think we can all agree that blocking certain communications about the NZ attack was the correct action, where does one draw the line. Who gets to make that choice, and on what basis. That is a slippery slope toward censorship.
Social Media and Free Speech

It is also important to note that technological solutions are not perfect. The application of AI can be fooled, and it can generate false positives too (blocking items that should not be blocked). If it can be used to pick up on content that indicates an attack (or any other kind of harm) is imminent, it is still lacking a channel to make the observation actionable. We saw this problem with the Parkland shooting where statements by the shooter in advance of the shooting were reported, but not sufficiently followed up.

In summary, there are many issues surrounding the role of social media in offensive speech and action and there needs to careful consideration of actions we expect the platforms to take. These actions need to balance free speech rights of innocent individuals against the incitement and indoctrination of terrorist groups. In the end, we need to decide whether the "amplification" provided by social media platforms is a good things or a bad thing.
What is Civil Law

- Civil law is concerned with private relations between parties rather than criminal complaints by a government against an individual.
  - This is in contrast to criminal law.
  - Includes contract law.
  - Includes tort law.

- If a tort (wrong) is committed we may be able to settle or litigate over actual, punitive, or stipulated damages, for “specific performance”, or injunctive relief.
Civil Law and Privacy

- Contracts and privacy and security
  - Privacy policy statement
- Discovery and Privacy
- Laws protecting privacy of consumers
  - HIPAA
  - FERPA (Buckley Amendment)
  - Fair Credit Reporting Act
  - Others
  - Regulations by FTC (and at one point FCC)
  - Data Breach Notification Laws
Contracts and Privacy

We enter into contracts all the time
  Signing contracts for services or good
  Consenting to terms of use on websites
  Installing software (EULAs)
Such agreements set the terms of our activity
  We can give away some rights to privacy
  They may spell out what our “expectations” are
  They can limit the damages we can collect
  They can determine how and where to litigate
Certain terms can still be found unenforceable for a variety of reasons.
Enforcement of Contracts

Probably easier against the writer of such agreements, if acceptance was “implied”.

- But usually the terms with respect to privacy tend to disclaim expectations of privacy, so no damages to demonstrate, and other damages usually limited by the terms of the agreements.
- Litigation can be initiated by injured parties, class actions, or by government agencies in some cases (e.g. FTC).
- Terms of such agreements can’t allow either party to “break the law” or violate other regulations, but they can change how certain breaches are to be treated (e.g. opt-in)
- Deceptive trade practices…(can provide alternative remedy)
Discovery

When bringing suit (litigating) civil matters, all parties have the right to compel disclosure of facts that may benefit their case.

- The process of forcing disclosure of such information is called Discovery.
- If you are a party to the suit then you may be required to produce “discoverable” information.
  - A good reason not to keep some things to begin with.
  - A good reason to have a data retention/destruction policy
    - It is illegal to destroy the data after you have reason to believe that it will become subject to discovery.
  - Third party doctrine applies
    - Data about you may be obtained from third parties
    - You may have an opportunity to object to such disclosure, but not always.
Privacy Implications of Discovery

• Examples:
Laws protecting privacy of consumers
  - HIPAA
  - FERPA (Buckley Amendment)
  - Fair Credit Reporting Act
  - Others
  - Regulations by FTC (and at one point FCC)
  - Data Breach Notification Laws
Health Insurance Portability and Accountability Act


Provides a framework for:
- Nationwide protection of patient confidentiality
- Security of electronic systems
- Standards for electronic transmission of health information.
HIPAA Privacy Rule

- The **HIPAA Privacy Rule** establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.
  - Defines Protected Health Information (PHI)
  - Provides outline for protecting PHI
The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

– Relationship to NIST Framework
Protected Health Information (PHI) is individually identifiable health information that is:

- Created or received by health care provider, health plan, employer, or clearinghouse that:
  - Relates to the past, present, or future physical or mental health or condition of an individual;
  - Relates to the provision of health care to an individual
  - Or payment for provision of health care

Includes information in health record such as:

- Encounter/visit documentation
- Lab results
- Appointment dates/times
- Invoices
- Radiology films and reports
- History and physicals (H&Ps)
- Patient Identifiers
Patient Identifiers (examples)

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code
Minimum Necessary Disclosure

– To use or disclose/release only the minimum necessary to accomplish intended purposes of the use, disclosure, or request.

– Requests from employees at Organization:
  • Identify each workforce member who needs to access PHI.
  • Limit the PHI provided on a “need-to-know” basis.

– Requests from individuals not employed at Organization:
  • Limit the PHI provided to what is needed to accomplish the purpose for which the request was made.
HHS announces first HIPAA breach settlement involving less than 500 patients

- **Hospice of North Idaho settles HIPAA security case for $50,000** - The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services’ (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

- The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance.
FERPA

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The law gives parents or "eligible students" (those who are over 18 years old) certain rights with respect to a student's educational records.
FERPA

• The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that Schools, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your education records.
FERPA – Directory Information

• **Directory information** is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. **FERPA** requires each institution to define its **directory** items, and such information may be quite broad. Students can request non-disclosure of such directory information.

• [USC’s FERPA Notices](#)
Universities have lots of Data

- Personally Identifiable Information (PII)
  - SSN, Drivers License, Credit/Debit Card, Passport Number, Banking Records, DOB, Parents Information
- Protected Health Information (PHI)
  - Medical Record, Health status, provision and payment of health care
- FERPA controlled information
- Financial Information
What does USC follow?

• **Education records**: Under the Family Educational Rights and Privacy Act of 1974, or “FERPA,” USC may not disclose records relating to a student without the student’s written permission. “Directory” information is an exception.

• **Health information**: Under the Health Insurance Portability and Accountability Act of 1996, or “HIPAA,” USC may not use or release identifiable health information without the patient’s written authorization. USC must notify patients and the federal government if there is a breach of patient information.

• **Personal information**: Under California law, USC must protect personal information including name and any of the following data: – Social Security number – Drivers license number – Credit card and pin number – Medical information

• **Customer information**: Under a federal law known as the Gramm-Leach Bliley Act, USC must protect personally identifiable financial information that it collects about an individual in connection with providing a financial product or service such as financial aid or faculty housing loans.

• **Research records**: These records may be protected by copyright, trademark, trade secret, patent, or other intellectual property laws.
Security Measures

• Password & Log-in Monitoring
  • Use a combination of upper case, lower case, numbers, and special characters
  • Use misspelled words
  • Numeric substitutions
  • Configuring your system to log off automatically is a relatively simple task
  • DUO, Two Factor Authentication

• Malicious software and security reminders
  • Viruses, Worms, Spyware, Trojan Horse, Social Engineering, Phishing

• Physical security
  • Door Locks, paper shredder, Safes. Laptop security, Mobile security
  • Encryption (laptop, USB, external hard drive)
The **Fair Credit Reporting Act**, 15 U.S.C. § 1681 ("FCRA") is U.S. Federal Government legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. The FCRA regulates the collection, dissemination, and use of consumer information, including consumer credit information.
Fair Credit Reporting Act

- Defines purposes for which such reports may be requested.
- Imposes requirements on the reporting agencies, users of reports, and furnishers of information.
  - Including Notice requirements.
  - Permissible purposes.
  - Ability to correct information.
Federal Trade Commission

- The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Act. Since then, rapid changes in technology have raised new privacy challenges, but the FTC’s overall approach has been consistent: The agency uses law enforcement, policy initiatives, and consumer and business education to protect consumers’ personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace.
  - FTC's Privacy Report: Balancing Privacy and Innovation
  - The Do Not Track Option: Giving Consumers a Choice
  - Making Sure Companies Keep Their Privacy Promises to Consumers
  - Protecting Consumers’ Financial Privacy
  - The Children’s Online Privacy Protection Act (COPPA)
FCC Broadband Privacy (rescinded)

- In 2016 the FCC released rules to protect consumer broadband privacy. As discussed, congress rescinded these rules, leaving the issue to be covered by state law, privacy policies and contract provisions, and the FTC.
Data Breach Notification Laws

- “Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.” (according to national conference of state legislatures)

- Security breach laws typically apply to particular classes of business and define personally identifiable information such as name combined with SSN, drivers license or state ID, account numbers. They also define what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice; and exemptions based on whether the information was encrypted, if disclosure would impede law enforcement investigations, etc.

- Federal law is by sector (e.g. FERPA, HIPAA, etc). See comparison of various laws.
Google Quietly Adds Search Engine Privacy Option To Chrome - Here's How To Enable It - Forbes

Google Chrome has added DuckDuckGo as a default browser. It’s released in 60 countries and blocks advertising trackers, keeps your search history private, and allows you to take control of your personal data by not storing it. It does not provide the search results that Google does but still protects your privacy by not selling your information to third party advertisers. -Chloe Choe

Google quietly adds search engine privacy option to Chrome : Forbes 03/14/2019
The latest Google Chrome update has added DuckDuckGo to the list of default search engines in 60 countries which includes the US and UK. The advantage of this is increased privacy and the disadvantage is that users will not get personalized search since DuckDuckGo doesn't store any of the users' personal data. However, everyday search results for DuckDuckGo compare relatively well with Google, so it is more of an advantage to have DuckDuckGo under the hood. –Anupama

Google fined $1.7 billion by EU : NPR 03/20/2019
EU fined Google 1.5 billion euros for antitrust violations in the online advertising market. Google allegedly abused its market dominance by limiting its rivals from working with companies that had deals with Google. The search boxes that appear on websites, blogs etc and display ads by Google gave Google a wide range of controls through Adsense contracts. Conditions in contracts allowed Google to control how its rivals' ads would appear in the ad boxes. Google stopped using the exclusivity clauses in 2016 when EU objected to them. --Anupama
Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years – Krebs on Security
Krebs on Security revealed that Facebook has been storing hundreds of millions of user passwords in plain text in its internal system. Facebook spokesman explains that the passwords have never been exposed to outside. -- Fumiko Uehara

Keeping Passwords Secure Facebook 3/21/2019
Facebook announced on Thursday that the passwords of "hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users" were stored in a readable format. Even though Facebook claims that these passwords were never exposed to anyone outside Facebook, this is still making Facebook negligent when it comes to privacy. Facebook has proven to the world that the company is taking an ant-privacy approach in their business line because there is no other excuse Facebook has for all of these privacy flaws
- Faris Almathami

Facebook Did Not Securely Store Passwords. Here’s What You Need to Know – The New York Times 3/21/19
Millions of user account passwords have been stored insecurely, allowing Facebook employees to access user accounts without their knowledge on Thursday. Do not use the same password on multiple sites and set up security features such as two-step verification. Set up your Facebook account to receive alerts when unrecognized devices or unfamiliar locations log in to your account and click the remove button to boot it. – Sophia Choi

FACEBOOK STORED MILLIONS OF PASSWORDS IN PLAINTEXT—CHANGE YOURS NOW - Wired 03/21/2019
It was found 3 months ago that passwords for Facebook platforms were stored as plaintext or in a readable format on Facebook internal storage systems. Users of these platforms, namely Facebook, Facebook Light and Instagram, were informed through email about this incident but were not forced to reset their passwords. It took Facebook almost two months to fix the issue as the passwords weren't all stored in one system and didn't result from a single bug in the password management system. - Abdulla Alshabanah
This week, it was reported that Facebook has been storing user passwords in plaintext - in fact, it has been doing this for years. To make matters worse, all of these passwords were searchable by Facebook employees. The company is coming under fire yet again for this, especially since the problem was discovered in January and not addressed until March. -- Ann Bailleul

Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years — Krebbs on Security
Hundreds of millions of Facebook users had their account passwords stored in plain text and it was searchable by thousands of Facebook employees dating back to 2012, according to KrebsOnSecurity. The investigation indicates that between 200 - 600 million passwords were stored in plain text. Facebook claims no passwords reset are required at this moment. -- Louis Uuh

 Millions of Facebook Passwords Exposed Internally - BBC 3/21/2019
Back in January, Facebook discovered a security flaw that allowed developers to create applications that logged and stored passwords without encrypting them. They mentioned that most of the people impacted were users of Facebook Lite and that they would notify hundreds of millions of Facebook Lite users, tens of millions of Facebook users, and tens of thousands of Instagram users. Facebook stated that it would only enforce a password reset if they found proof of abuse due to the login credential issue. -- Yulie Felice
Current Events - Facebook

Facebook employees had access to millions of user passwords - CNBC 3/21/19
The article discusses about how Facebook apparently stored up to 600 million users passwords in unencrypted form on its servers, allowing employees to easily view them in plain text. Facebook said that it would start notifying users that had been affected and that this had been going on as far back as 2012. Facebook claims that no misuse of the data has been found, however under GDPR passwords are supposed to be stored securely so a thorough review will be done on this issue. -Ahmed Qureshi

Facebook sues over 'data-grabbing' quizzes - BBC 3/11/2019
Facebook is suing Andrey Gorbachov and Gleb Sluchevsky that work for Web Sun Group for developing quiz apps which are able to gather personal information of users through its browser extension. The app states that it would only retrieve limited amount of public data from user profiles but they are found to obtain names, profile pictures and private list of friends through Facebook login system. The app has been installed 63,000 times and has caused over $75,000 damages for Facebook. -Yulie Felice

Facebook's Data Deals Are Under Criminal Investigation 03/12/2019 Nytimes
Federal prosecutors in the Eastern District of New York were conducting a criminal investigation into deals Facebook had made with other companies that gave them access to data, allegedly without the consent of users. Mr. Zuckerberg unveiled a plan that would begin to pivot Facebook away from being a platform for public sharing and put more emphasis on private communications. – Deepti

Facebook says no one flagged New Zealand mosque shooting livestream. AP 3/19/19

Facebook says none of the 200 or so people who watched live video of the New Zealand mosque shooting flagged it to moderators, underlining the challenge tech companies face in policing violent or disturbing content in real time. The video's rapid spread online puts renewed pressure on Facebook and other social media sites such as YouTube and Twitter over their content moderation efforts. Facebook uses artificial intelligence and machine learning to detect objectionable material, while at the same time relying on the public to flag up content that violates its standards. To report live video, a user must know to click on a small set of three gray dots on the right side of the post. -- Gene Zakrzewski
Current Events

Apple ad focuses on iPhone's most marketable feature - privacy - Techcrunch
Summary: Apple has released a buzz-worthy new ad for the iPhone that centers around the idea of privacy being the iPhone's central feature. The ad features funny situations of where one would need privacy- and suggests that if privacy matters to people in their life, it should also matter to the phone that is so closely tied to peoples' lives today. The ad is yet another reinforcement of Apple’s recently emphasized message that they stand behind good privacy practices; unlike other tech companies such as Google or Facebook, Apple relies less on ads and 3rd party data selling and more on their own hardware/services sales, allowing them to take a stronger stance and commitment to privacy. -- Kate Glazko

Apple sells data privacy, yet again US News and World Report
Extract: Apple launched an advertising campaign promoting its stance on data privacy, seeking to differentiate itself from tech industry rivals such as Google and Facebook which are often a target of privacy breach issues. The ad played during the march madness which had theme that if privacy matters to people when they close the blinds and doors of the house, it should matter to the phone which we use as well as we do pretty much everything in our phone these days. 'Privacy. Thats iPhone'. Apple does collect user data but since they are encrypted, even apple cant look into it and hence a tighter privacy. --Kavya Sethuraman

Constitution Corner: Right to be secure in our persons, houses, papers, effects -- West Hawaii Today - 3/21/2019
We now know that the FISA warrant which was responsible for kickstarting the Trump/Russia collusion investigation grossly ignored America’s 4th Amendment protections. In the nearly 40 years of the court’s existence, it has only rejected about 0.03 percent of total requests, giving credence to the idea that it’s a rubber-stamp operation to suit the government’s need and sometimes at the peril of innocent Americans. On a more local level the hairs on the back of my neck pricked when I first heard that the Department of Motor Vehicles in conjunction with issuing safety checks would soon include photographing our cars. SmartGridNews, a website supported by the high-tech meter industry, acknowledged that smart meters are gathering private information on homeowners. Utility companies have the ability to analyze the data collected from smart meters to build a profile for every utility customer. -- Gene Zakrzewski
Big data and healthcare: Life saving benefits and future challenges | Datacenter Dynamics | March 14, 2019
Data driven machine learning algorithms can offer critical secondary feedback and aid in early detection and risk assessment through use of image and non-image based data. Example - “As just one example, when evaluated by ophthalmologists, a deep learning algorithm had over 90 percent specificity and sensitivity for diabetic retinopathy when fed thousands of retinal photographs. In dermatology, when fed 130,000 patient images, an algorithm was comparably accurate to dermatologists in identifying skin cancer. “ Some challenges such as data integrity especially pulling together large sets of healthcare data; data leaks are also notorious amongst EHR based data. Much of this may result in misdiagnosis, false positives, or mismanagement of treatment as a result of poor integrity of data. This may result in a bigger stress / invasion of privacy. - Arjun G. Raman

Slack hands over control of encryption keys to regulated customers | TechCrunch | March 18, 2019
Slack announced launch of Enterprise Key Management (EKM) for Slack, a new tool that enables customers to control their encryption keys in the enterprise version of the communications app. Slack currently encrypts data in transit and at rest, but the new tool augments this by giving customers greater control over the encryption keys that Slack uses to encrypt messages and files being shared inside the app. This is important because Slack is placing control of access points (via key) back to the organization that is leveraging slack. It's an important first step to in the future having key management (and potentially generation) at the edge. For now, this step pushes key management via AWS Key Management Tool - placing the security efforts back to the originating organization and in-turn encourages better security practices. Enterprise customers can gain greater visibility into activity inside of Slack via the Audit Logs API as well. - Arjun Raman
Utah Just Became A Leader in Digital Privacy Wired

Summary: The abundance of data available about people and the ability of law enforcement to easily access such data had provided a platform for the ACLA of Utah and Libertas Institute to push the Utah legislature to pass a new privacy law. The law would restrict the ability of the government to access of 3rd parties’- such as Facebook and Google- private data. Law enforcement would instead now have to obtain a warrant before accessing such data. -- Kate Glazko

Dutch Data Protection Authority chips away at ‘cookie walls,’ declaring they violate GDPR - SC Media 03/11/2019

Dutch Data Protection Authority (DDPA) has issued a statement explaining that cookie walls which is the practice of websites making visitors agree to accept cookies to view the content – violate the European Union's General Data Protection Regulation (GDPR). They said that if users cannot access a site without agreeing to be tracked, they are being forced to share their data. The privacy issue is not with cookies per se but with third party cookies. One needs to know the source and use of the cookies in order to be able to give informed consent. - Sevanti Nag

National Security Agency halts surveillance program - cnn.com - Mar 5, 2019

The program has been plagued by challenges including a technical problem which reportedly lead the system to collect calls on US citizens without authorization. -- Dewaine Reddish

Why WA's data-privacy bill might not go far enough - Crosscut

This article discusses recently proposed data privacy legislation, that legislators compare to international policies. However, many privacy advocates believe the proposal is weaker than GDPR and California data privacy policies. A major concern being that the legislation is not clear on requiring companies to delete user data upon request. -- Joseph Mehlretter
Facial Recognition can Speed You Through Airport Security - 3/21/2019
At 17 airports in the US, the departure gate is using a face-matching system called Biometric Exit. The US Customs and Border Protection plans on having the system scan 97% of all outbound international travelers by 2021. The system scans your face and sends your image to a remote system that matches it to a stored copy of your passport photo. You then have your photo taken again at the security line and then again at the gate. If all of these images match, you’d be allowed on board. This poses an issue as the algorithm used has error rates depending on the persons race and gender. This could lead to certain groups of people having to face extra screening. -Andrew Carmer

Facial Recognition Usage in Law Enforcement - Cnet 3/19/2019
Police have been using Amazon's Rekognition facial recognition software in multiple theft cases since 2017. However, the ACLU has challenged this use, stating that errors in the system may cause the wrong people to be targeted/arrested, and that misuse of this technology can lead to a mass surveillance system. The police state that this system saves time and is not used in the way that the ACLU claims, and that no mass surveillance is planned or in use. How can we make sure that this is the case, and that this will not change in the future? - Lance Aaron See

Questions of suspect privacy arise as DNA genealogy sites progress criminal cold cases - WHNT 3/20/19
Websites like Ancestry.com and 23andMe are helping law enforcement agencies make progress on previously stagnant cold cases. Backlash has been received by the American Civil Liberties Union claiming the violation of privacy rights. Law enforcement officials have doubled down stating that using these genealogy databases is legal and that innocent people have also been exonerated using this information. -- Aaron Howland
Researchers Create Fake Profiles on 24 Health Apps and Learn Most Are Sharing Your Data – Gizmodo - March 21, 2019
Researchers in Canada, the U.S., and Australia teamed up for the study, where they tested 24 popular health-related apps used by patients and doctors. Among the more popular apps, some of them reminded users when to take their prescriptions, while others provided information on drugs or symptoms of illness. From the study, they found 79 percent of apps shared at least some user data outside of the app itself. They even found that many third parties marketed themselves bundle the data and share it to credit reporting agencies - companies that are far from the health industry. This study was published in a medial journal. -- Minyi (Mindy) Huang

ICE taps huge license-plate database, ACLU says, raising privacy concerns – Washington Post 3/14/19
According to the ACLU (American Civil Liberties Union), ICE agents have tapped into a database of license plates to track down people. The database was taken from police cars and scanners above major roads. The scanner records license plate data in every passing car, making innocent people an inappropriate target of government surveillance. – Sophia Choi

ICE is tapping into a huge license-plate database, ACLU says, raising new privacy concerns about surveillance - The Washington Post 03/13
U.S. Immigration and Customs Enforcement agents believed to be accessing databases of license plate numbers to track individuals believed to be in the country illegally. The databases contain records from verity of scanners such as red lights and toll road cameras, which rapture not only violators but any passing car or truck. ICE spokesman said that the agency allows employees to access the data only for “mission-related purposes.” Abdullah Altokhais

What Does Brexit Mean for Data Protection?
This article discusses what happens with data protection foe the UK on 29 of March when the Brexit transition begins. During this transition UK will have to follow EU rules; therefore, GDPR. During this transition the UK must develop data practices that are deemed "adequate" by the EU; otherwise, issues may arise regarding the flow of data between the two. -- Joseph Mehltretter
Current Events

Should Nation-States be allowed to hack back? – infosecurity 3/20/19
This article speaks about a survey that was passed around during the RSA conference. In it, responders were asked if they thought that Nation-States should be allowed to hack back. The survey result was 72% of responders saying that hacking back should be allowed. One of the views with this argument is that countries should be entitled to defend their assets and retaliate against those that overstep that boundary. Other argue that it can become increasingly difficult to draw the line as to how much hacking back is allowed and when does it cross a line. -Jairo Hernandez

Uber 'surfcam' spyware ThreatPost 3/20/19
Uber was accused of deploying a spyware program called "Surfcam" to try and poach drivers from local Australian competition, GoCatch. Strangely, Uber did not know about the existence of this software until it was used in Singapore for supposedly a similar effort to undermine Grab, Uber's Singaporean rival. The software is said to scrape public websites for data on cars online at the time and get info on drivers. - Charlene Chen

The Paranoid Person's Guide to Online Privacy-03/21/19 Fast Company
From ditching Google to using a burner phone for 2FA, this article highlights the eight primary ways that privacy-savvy consumers can expand their privacy in the online world. Consumers are developing a heightened awareness of online surveillance by tech giants, ISPs, social media and marketing firms, and this guide seeks to teach readers how to provide zero to minimal personal information to third parties. Among the solutions include using a VPN, Tor routing, secure messaging, anonymous and private social media accounts, never using Smart devices, Android devices, nor Facebook. -Jacqueline Dobbas