DSci529: Security and Privacy In Informatics

Government Regulation

Prof. Clifford Neuman

Lecture 11
2 April 2021
Online

Course Outline

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

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation
13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare
14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

Upcoming Presentations – April 9th Free Expression - Disinformation

- Adriana Nana – Deep Fakes and Privacy
- Resherle Verna – Should Social Media company's have right of censorship

  – This group will have 20 minutes to present.

Upcoming Presentations Privacy and Finance – April 16th

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – History and Technologies for Cryptocurrencies
- Saurabh Jain – Privacy of Credit Card/Payment card information
- Yifeng Shi -Financial value of data gathered through free services

- 40 minutes

Secure Communication – Privacy Preserving Technologies – April 16th

- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

- 40 minutes

Upcoming Presentations
Other Security Topics – April 23rd

- Yo-Shuan Liu – User experience and Multi-Factor Authentication
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India

DSci529: Security and Privacy In Informatics

Government Regulation

Prof. Clifford Neuman

Lecture 11
2 April 2021
Online

INF529: Security and Privacy In Informatics

Apple v. FBI

Prof. Clifford Neuman

Lecture 10 B
2 April 2021
Online

Access to Data on Protected Devices

- For many years, law enforcement has been accessing data on devices seized in raids, or incident to arrest. There is a whole business around forensic analysis of such devices.
- With the widespread adoption of memory encryption in phones around 2014 this process was made more difficult.
- There had been proposed legislation to limit this kind of effective encryption, and we saw some of these bills earlier in this class. The events that follow effect the debate on the some of those bills.

Apple opposes order to help FBI unlock phone belonging to San Bernardino shooter

By James Queally and Brian Bennett · Contact Reporters

FEBRUARY 17, 2016, 8:32 AM

Apple Inc. CEO Tim Cook says his company will resist a federal judge's order to access encrypted data hidden on a cellphone that belonged to the terrorist couple who killed 14 people in San Bernardino last year.

In a statement released early Wednesday, Cook said that such a move would undermine encryption by creating a backdoor that could potentially be used on other future devices.

"In the wrong hands, this software -- which does not exist today -- would have the potential to unlock any iPhone in someone's physical possession," the statement said.

The judge's order is aimed at removing what had become a barrier in the investigation of the deadliest terrorist attack on U.S. soil since 9/11.

Authorities are trying to determine the couple's movements between the time of the attack at the Inland Regional Center the morning of Dec. 2 and their deaths in a wild firefight with police hours later. Last month, the FBI asked for the public's help in filling in an 18-minute gap in the narrative of the couple's whereabouts.

The FBI is also probing whether the couple received any help in plotting or carrying out the attacks.

U.S. Magistrate Judge Sheri Pym in Riverside directed Apple on Tuesday to help the FBI get around the phone's passcode protection and any auto-erase functions the device might employ.

Apple changed the way it manages phone encryption in September 2014, a move that makes it more difficult for law enforcement to access encrypted data on cellphones, according to Clifford Neuman, director of USC's Center for Computer System Security. Previously, forensic investigators could tap into a device's hardware port and gain access to a phone's data "independent of needing to try passcodes," he said.

"That path into the device is no longer possible," Neuman said.

The change in the encryption method means Apple may not be able to decrypt the data, according to Neuman. The company could, however, bypass the access code system that would cause the data to be erased, and then grant the FBI access to the encrypted data. Federal investigators would then have to decrypt the data themselves, Neuman said.

Full Coverage

Read more on the San Bernardino terror attack

The tech industry and the government have long been at odds over how much access law enforcement and national security agencies should be given to private phone data. Recently, Comey, Atty. Gen. Loretta Lynch and other national security leaders met with representatives from Google, Apple and Facebook in San Jose to try and find common ground that would help investigators gain crucial information about possible terror plots without compromising the privacy of the companies' customers.

The News Release

NEWS RELEASE

For Immediate Distribution

February 16, 2016

Eileen M. Decker
United States Attorney
Central District of California

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

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

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

The Motion and Order

The motion describes the reasons that the government is seeking an order to force Apple to assist them in getting access to the data on the device, and it describes the specific steps that they want Apple to perform.

Once issued (if issued) the order tells Apple what they must do, but Apple may appeal the order, or if "Apple believes that compliance with this order would be unreasonably burdensome," they may make an application to this court for relief within five business days.

Apple chose to appeal, and also to argue their case in "the court of public opinion". That option is not always possible since certain court orders prohibit disclosure of the request altogether. In any event, the issue became moot when the government was able to obtain the data on the phone through other sill undisclosed means. The debate is still important as it influences policy.

Ethical Issues

- Authority to search
  - Device owned by SB County
  - Court order based on showing of probably cause.
  - Genuine Probably Cause exists in this case
- Broader separate issue
  - Intentional vulnerabilities (back doors) in phone sold to other customers
  - Many problems with this

Legal Issues

- All Writs Act – a very board law used to provide the courts authority to order.
- At issue is the burden this imposes on Apple and whether that is appropriate. Apple further argued 1st amendment rights (no compelled speech).
- 4th Amendment Rights not at issue in this matter as cause has been established.
- 4th Amendment is an issue in the broader discussion regarding impact on privacy of other users.
- Would complying create a precedent.

Public Policy Issues

- Impact of Required Backdoors
- Requirements to provide access to cloud data

Technical Issues

- What data likely on phone: location, app data including communications.
- Which keys
  - Data key combined phone specific & passcode
  - Entropy of passcode
  - Different key (Apple's) used to sign new iOS.
  - Creating Backdoor vs using vulnerability
- Why not Google
  - Open nature of Android means different parties needed to sign the code.
  - Similar technical approaches exist.
- Newer hardware and iOS: capability for secure element (used for payment, but similar techniques can be applied.

International issues

- Level Playing Field
  - Other Countries will demand same access
- Access to cloud data across jurisdictions
  - International assistance

In the News FBI paid $1M for iPhone hack CBS News – April 21, 2016

- *http://www.cbsnews.com/news/fbi-paid-more-than-1-million-for-san-bernardino-iphone-hack-james-comey/*
- LONDON -- FBI Director James Comey alluded to the fact the bureau paid more than $1 million for the method used to disable the security feature of the San Bernardino shooter's iPhone.
- At an Aspen Institute discussion in London, Comey said the FBI paid more money than he would make in the time left as FBI director.

INF529: Security and Privacy In Informatics

Wikileaks v. CIA

Prof. Clifford Neuman

Lecture 10B
2 April 2021
Online

An Overview

- You saw a news clip last week
- Now let's analyze using the same framework

Ethical Issues

Apple v FBI

- Authority to search
  - Device owned by SB County
  - Court order based on showing of probably cause.
  - Genuine Probably Cause exists in this case
- Broader separate issue
  - Intentional vulnerabilities (back doors) in phone sold to other customers
  - Many problems with this

Wikileaks Disclosure

- Authority to “hack”
- Broader separate issue

Legal Issues

Apple v FBI

- All Writs Act
- Burden on 3rd parties
- Constitutionality
- Precedent.

Wikileaks Disclosures

Is the Hacking legal?

Broader Public Policy Issues

Apple v FBI

- Impact of Required Backdoors
- Requirements to provide access to existing data.

Wikileaks Disclosures

- Use of existing exploits
- Duty to protect?

Technical Issues

Apple v FBI
- Data on Phone
- Cryptography
- Security of Software
- Upgrades
- be applied.

Wikileak Disclosures
- IoT Security
- Sensors Everywhere

International issues

Apple v FBI

- Level Playing Field
- Access across jurisdictions

Wikileak Discosures

- Level Playing Field

Some Questions

- What's newsworthy?
  - None of what came out is really surprising in that we have known of these kinds of weakness for some time. We voluntarily surround ourselves with surveillance devices, i.e. cameras and microphones and location tracking, and it is only the strength of the security for the software on these devices that has protected us, and we know that thestate of software security is abysmal.

Some Questions

- How worried should the general public be about claims the government agencies can hack their electronic devices?
  - The public should be very concerned that their devices are hackable, not just by our own government agencies, but even more so by foreign intelligence services that also use these techniques, and by criminal enterprises that may have or might acquire such capabilities.

Some Questions

- Could you explain how you see the main vulnerabilities to users — is it mainly from apps or devices and operating systems?
  - The weakness are all in software, and that includes apps, operating systems, and software running on internet of things type devices like smart TVs. The impact occurs because the (vulnerable) software on these devices has access to the sensors that acquire sensitive information.

Some Questions

- What can tech companies do to protect users?
  - "control their software supply chains". By this I mean that they need to digitally sign updates to the software that runs on their devices, and protect the systems they use for development and distribution of such updates. They also need to ensure that thinks like "apps" that might run on their systems are appropriately examined before they are endorsed for use by their customers.

Some Questions

- Have the WikiLeaks releases provided enough detail for tech companies to recognize vulnerabilities and fix them?
  - It helps direct scrutiny to the areas that need examination and it will assist companies in identifying and fixing vulnerabilities, the current set of vulnerabilities will only be replaced by a new set of zero-days down the road, and one should never consider a software system to be completely secure.

Some Questions

- Wikileaks said in a statement it is "avoiding the distribution of 'armed' cyber weapons" — how damaging could these tools be if they fell into the hands of hackers and cyber criminals?
  - Many of these tools are already in the hands of cyber-criminals, and some might have been purchased from that community.

Some Questions

- How worried should we be that our smart TVs and wifi-enabled refrigerators and toasters could be spying on us?
  - They already are, the only question is one of what they do with the information they collect. We expect the information to be used for our benefit. More often than not, some of that information is used for commercial purposes (marketing), and as we saw from these leaks, the information may also be used for intelligence gathering. The only question is how much confidence we have in the software running on those devices, and the answer to that is "not much confidence at all".
  - Regularly when we install apps on our devices, we grant permission for the app to access sensitive information (camera, microphone, address book, location, etc). More often than not, if the app is commercial, that information is being sent to the provider of the app. Consider recent changes to the location information gathered by the uber app. The capability of apps to collect such information is not surprising.

Disclosure of Techniques in Legal Proceedings

- In FBI hacks, tech firms get left in the dark as feds resist call to divulge secrets - Los Angeles Times, March 31, 2016.
  - In US, when evidence is presented in court, defense has opportunity to refute, and due process may require disclosure of methods through which the evidence was collected.
  - In many cases, this limits the prosecutors ability to present certain pieces of evidence.

5th Amendement Rights?

Child porn suspect jailed indefinitely for refusing to decrypt hard drives – Ars Technia – April 27, 2016 – By David Kravets

A Philadelphia man suspected of possessing child pornography has been in jail for seven months and counting after being found in contempt of a court order demanding that he decrypt two password-protected hard drives.

The suspect, a former Philadelphia Police Department sergeant, has not been charged with any child porn crimes. Instead, he remains indefinitely imprisoned in Philadelphia's Federal Detention Center for refusing to unlock two drives encrypted with Apple's FileVault software in a case that once again highlights the extent to which the authorities are going to crack encrypted devices. The man is to remain jailed "until such time that he fully complies" with the decryption order.

Tracking TOR users
February 2016

- A judge has ordered the Federal Bureau of Investigation to turn over the complete code it used to infiltrate a child pornography site on the Dark Web, Motherboard reports. The FBI seized the Tor-based site known as "Playpen" in February 2015 and kept it running via its own servers for two weeks -- during this time, the bureau deployed a hacking tool that identified at least 1,300 IP addresses of visitors to the site worldwide.

- Playpen was "the largest remaining known child pornography hidden service in the world," according to the FBI. Roughly 137 people have been charged in the sting so far, Motherboard says. On Wednesday, a lawyer for one of the defendants won the right to view all of the code that the FBI used during the Playpen operation, apparently including the exploit that bypassed the Tor Browser's security features.

DSci529: Security and Privacy In Informatics

Government Regulation

Prof. Clifford Neuman

Lecture 11
2 April 2021
Online

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation

- Jia-Yu Lee - GDPR
- Kaifan Lu – China's Cybersecurity Law
- Yansong Wang - reCAPTCHA

13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare
14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

GDPR and companies established to comply with privacy regulations

JIA-YU LEE

Outline

What is GDPR

How GDPR apply to US

GDPR non-compliance cases

Startups that helps companies comply with GDPR

GDPR (General Data Protection Regulation)

- Personal data
- Data processing
- Data subject
- Data controller
- Data processor

GDPR (General Data Protection Regulation)

How GDPR apply to US

- The company offers good or services (even in the absence of commercial transactions) to EU/EEA residents.
- The company monitors the behavior of users inside the EU/EEA.

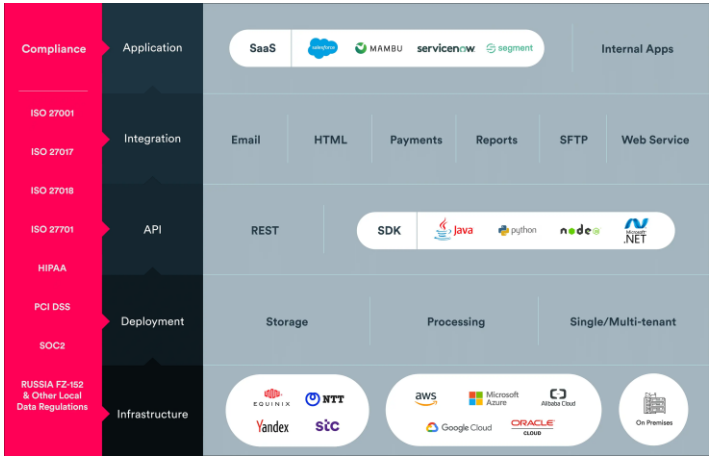
GDPR non-compliance cases

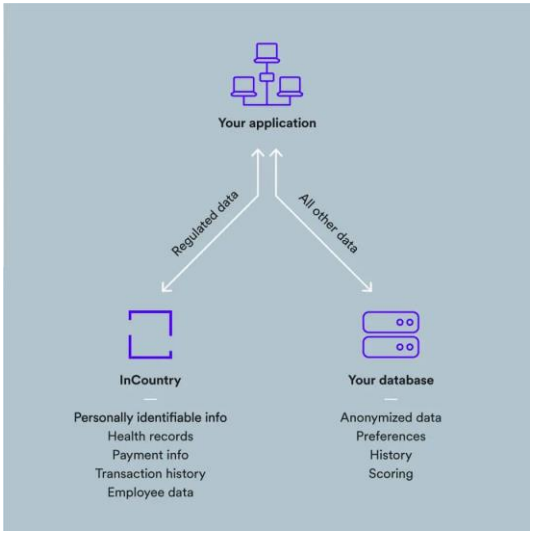
- Poland
  - Morele.net: data breach
- Sweden
  - A school in Skelleftea: facial recognition
- Romania
  - Unicredit Bank
- Finland
  - Taksi Helsinki (Taxi Operator): personal data processing

Startups that helps companies comply with GDPR

- InCountry

  A “data residency-as-a-service” platform that helps international companies store customer data locally.

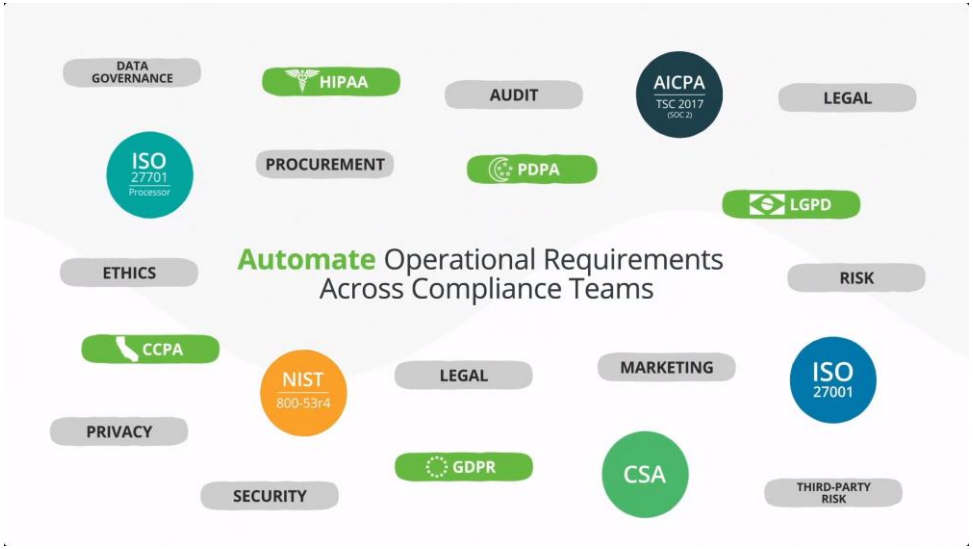




Startups that helps companies comply with GDPR

- OneTrust

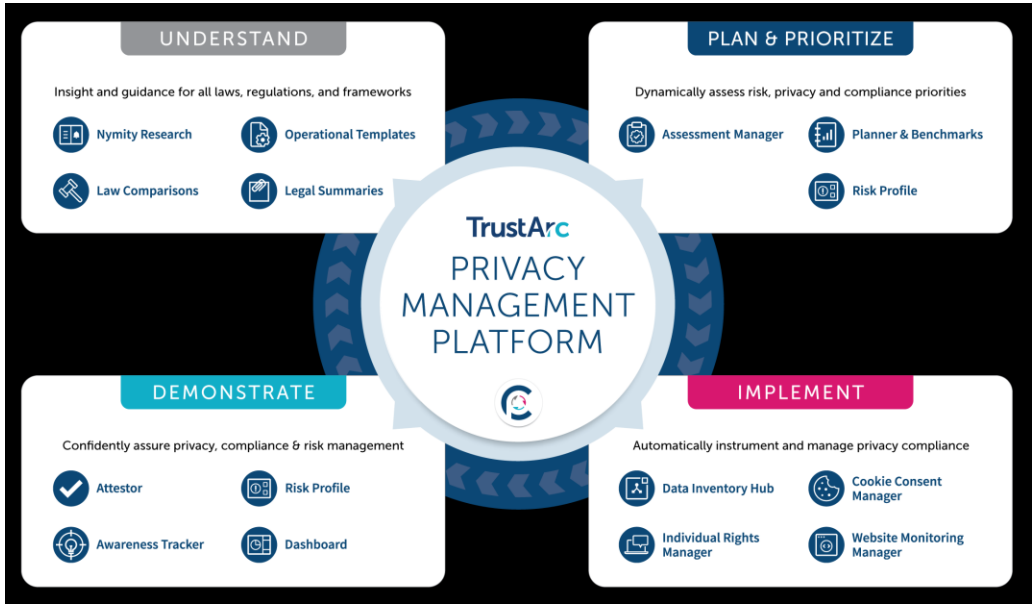
established to help businesses adhere to the growing array of regulations around the world, including GDPR and CCPA.



Startups that helps companies comply with GDPR

- TrustArc

develops data protection, certification, and compliance products for enterprises — its platform is about helping companies monitor risk around regulations and identify gaps across various regulatory frameworks.



Startups that helps companies comply with GDPR

- Privitar

  helps enterprises engineer privacy protection into their data projects, allowing them to leverage large, sensitive data sets while complying with regulations and ethical data principles.

Reference

https://gdpr.eu/what-is-gdpr/

https://www.cookiebot.com/en/gdpr-usa/

https://gdpr.eu/2019-small-business-survey/

https://www.nathantrust.com/gdpr-fines-penalties

https://securityboulevard.com/2019/09/polish-retailer-gets-e645000-fine-under-gdpr-for-insufficient-organizational-and-technical-safeguards/

https://www.telecompaper.com/news/swedish-school-board-fined-for-using-facial-recognition-to-take-class-register--1305319

https://business-review.eu/business/legal/first-fine-on-gdpr-202887

https://venturebeat.com/2019/07/23/5-data-privacy-startups-cashing-in-on-gdpr/

China’s Cybersecurity Law and Regulation

Kaifan Lu
DSCI 529 PRESENTATION

spring2021

Overview

1. Introduction
2. Legislative Background
3. Legislative Purpose
4. Legislative Framework
5. Major Principles
6. Discussion
7. Current Events
8. Citation

Introduction

- **In November 2016, China passed its first Cybersecurity Law,** aiming to strengthen cyberspace governance through a number of initiatives.
- **On June 1st, 2017 China's Cybersecurity Law ("CSL") took effect.**

Background

International background

More than **ninety countries** have enacted special laws to safeguard cybersecurity.

The major cybersecurity laws:

- The U.S. Cybersecurity Information Sharing Act (CISA) (2015)
- European Union Directive on Security of Network Information Systems (NIS Directive) (2016)
- The Cybersecurity Basic Act of Japan (2014)

Domestic background

- China built its first connection to the Internet in **1994** under Jiang Zemin's presidency.
- **Until 2010**, the government released its first white paper on the topic. The document entitled: "**The Internet in China**", established an early guideline on using of the internet.
- China has become one of the largest Internet markets in the world.
- China is one of the countries that suffered the most serious threats from the Internet.

Chinese Government

Chinese Government stated that the purposes of the law:

- To ensure cybersecurity
- To safeguard cyberspace sovereignty, national security, and social and public interests
- To protect the lawful rights and interests of citizens, legal persons, and other organizations
- To promote the healthy development of the informatization of the economy and society

46 International Organizations

- **United States, Europe, Asia, and Oceanic regions signed a letter opposing the draft law**
- **They insisted on revising the draft law in accordance with international trade regulations on the assumption that the law would raise trade barriers**
- **They think that the cybersecurity law is a tool to strengthen authoritarianism, especially in regard to information flows that could jeopardize government authority**

Framework

The general provisions

- Purpose and scope of the legislation
- National policy on cybersecurity protection
- Enforcement authorities
- Basic principles of the legislation
- Special protections for juvenile Internet users

The specific provisions

- Cybersecurity
- Network operations security
- Network information security
- Monitoring and emergency responses
- Legal liabilities
- Supplementary provisions

Major Principles

- **Cyberspace sovereignty**
- **Network operators' security obligation**
  - Hierarchical system for protecting cybersecurity
  - Security review of network products or services
  - Network real-name system
- **Protection of personal information**
  - The scope of personal information
  - Providing institutional space for the development of the big data industry
  - Right to correct and delete
- **Critical information infrastructure protection**
  - Legal obligations of critical information infrastructure operators
  - Local storage of data and data export security assessment

The cybersecurity law is a tool to create more control and represents another step on top of the content limitation measures set out by the Great Firewall?

Discussion

- **Article 10**: The construction and operation of networks, or the provision of services through networks, shall be done in accordance with the provisions of laws and administrative regulations, and in accordance with the **mandatory** requirements of State standards.
- **Article 22**: The network products and services shall comply with the relevant **mandatory** national standards.
- **Article 35**: The network operators or network products or services providers need to submit relevant contents to the **Chinese government** for **review purposes**, which might include software source code protected by intellectual property laws, encryption algorithms, design details, and trade secrets, etc.
- **Article 75**: For those who conduct attacks, intrusions, interference, destructions or other activities for the purpose of endangering the critical information infrastructure of the People’ s Republic of China, whether they are organizations or individuals, if they have caused serious consequences, the Chinese government shall take measures in accordance with the law to either freeze their assets or to take other necessary punitive measures.

Discussion --- *Regulations with Chinese characteristics*

✓ **PRIVACY:**

◆ **Data privacy**

- Personal data must be stored within China.
- There are also restrictions on transferring data across borders.
- Any cyber framework that conceals data or information from the Ministry of Public Security will be deemed illegally.

✓ **SECURITY:**

◆ **Privacy regulation for private companies**

- Organizations and network operators must accept government-conducted security checks.

◆ **Security requirement**

- The developers of systems and infrastructure should provide **adequate** security measure.

Current event - Steam's Chinese version

- While Steam has been accessible to gamers in China for years, it has existed in **a legal gray area.**
- Finally, Valve has partnered with a Chinese company to make a President Xi-approved version of Steam.
- Beginning in February 2021, gamers in China will have the option of using an official Chinese Beta version of Steam.

Why would they want to do that?

Does the Chinese version offer some compelling advantages for Chinese users???

Current event

✓ Search games:

◆ Regulation:

Chapter 3 Content Guidelines

Article 9: Online games must not contain the following content:

(1) Violating the basic principles established by the Constitution;

(2) Endangering national unity, sovereignty and territorial integrity;

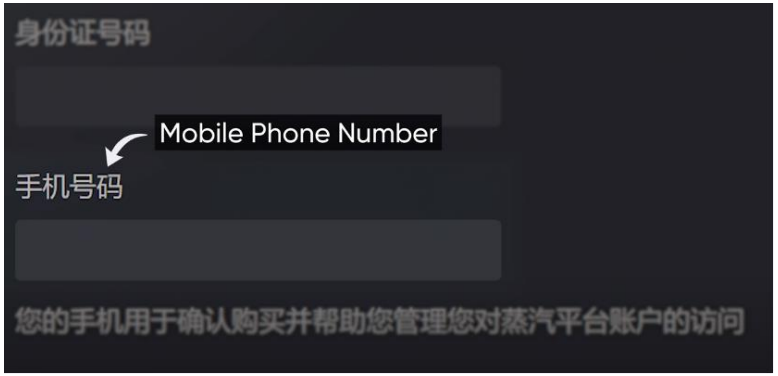
(3) Leaking state secrets, endangering national security or harming national honor and interests ; and

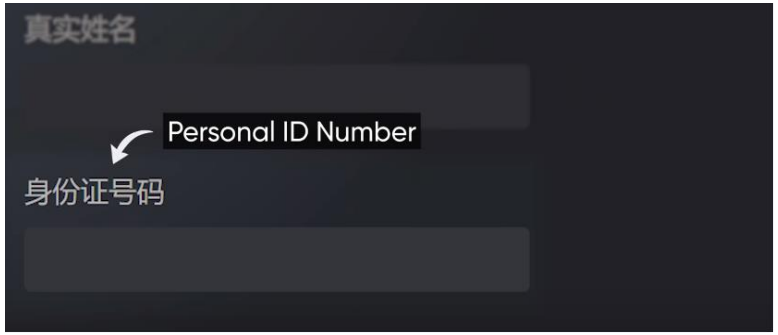
(iv) incitement to ethnic hatred, ethnic discrimination, undermining national unity, or infringes upon national customs and habits;

(e) propagating evil cults or superstition;

(6) spreading rumors, disturbs social order or undermines social stability;

✓ Create account:





Discussion

There are 2 kinds of laws:

- ***One to maintain social justice and morality***
- ***One to maintain social stability and order***

A Chinese tycoon just went on a very mysterious leave of absence

Citation

[1]. Qi, Aimin, Guosong Shao, and Wentong Zheng. "Assessing China's Cybersecurity Law." Computer Law & Security Review 34.6 (2018): 1342-1354

[2]. Wang, Di, et al. "Security Assessment of Blockchain in Chinese Classified Protection of Cybersecurity." IEEE Access 8 (2020): 203440-203456

[3]. Descamps, Maud. "China's Cybersecurity Legislation." (2020)

[4]. "China seeks Public Comments for Draft Regulations on Cybersecurity Multi-level Protection Scheme to Implement the Cybersecurity Law," Covington, July 05, 2018. Accessed November 15, 2019

[5]. "Overview of China's Cybersecurity Law," KPMG China, February, 2017. Accessed November 16, 2019

[6]. "China's Cybersecurity Legislation: A Paper Tiger or an Institutionalized Theft? " Maud Descamps, May, 2020

[7]. Pernot-Leplay, Emmanuel, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? (2020). Penn State Journal of Law & International Affairs, Vol. 8, No. 1, 2020

PDF Presentation
Yansong Wang - reCAPTCHA

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation
- Jia-Yu Lee - GDPR
- Kaifan Lu – China's Cybersecurity Law
- Yansong Wang - reCAPTCHA

13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare
14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

This Week – Privacy Regulations

- Europe's GDPR
  - https://eugdpr.org/
  - https://gdpr-info.eu/
  - https://gdpr.eu/
- California's CCPA
  - https://oag.ca.gov/privacy/ccpa
  - https://www.caprivacy.org/
  - https://www.mercurynews.com/2020/10/05/prop-24-big-tech-quiet-in-california-data-privacy-initiative-fight/
- China's Internet Privacy Law
  - http://www.cac.gov.cn/2019-08/23/c_1124913903.htm
  - (above is in Chinese only)
- Court Cases
  - From the Guardian
  - From US NPR on Google

Discussion

- What are the benefits of the regulations?
- What are the weakness (i.e. in what way might they be ineffective)?
- What is the impact for business?
  - Does it disrupt business models?
  - How are they mis-used to the detriment of society?

Europe's General Data Protection Regulations (GDPR)

GDPR – High level Goals

The GDPR sets out seven key principles:

Lawfulness, fairness and transparency

- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) GDPR

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

GDPR 6 Lawful Bases to Process

Article 6 of GDPR describe six lawful bases **for processing**, at least one of which must apply.

(a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes. ***(this may be revoked at any time)***

(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for **compliance with a legal obligation** to which the controller is subject.

(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.

(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Right to be Forgotten

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

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

https://www.npr.org/2019/09/24/763857307/right-to-be-forgotten-only-applies-inside-eu-european-court-says

Consider this in the context of US Law

Under FCRA, public record information regarding a bankruptcy can only remain on a credit report for 10 years.

- But are news archives, or search results limited by this, when they become "defector" credit reports.
- In practice, what becomes public can never be put back in the bottle.

CCPA – 5 Key Rights

Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

1. The right of Californians to know what personal information is being collected about them.
2. The right of Californians to know whether their personal information is sold or disclosed and to whom.
3. The right of Californians to say no to the sale of personal information.
4. The right of Californians to access their personal information.
5. The right of Californians to equal service and price, even if they exercise their privacy rights."

Source: CCPA Text

CCPA – Opt Out Provisions

1798.120 (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out. …

(c) A business that has received direction from a consumer not to sell the consumer's personal information … shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

1798.115 (d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to 1798.120.

CCPA – Non Discrimination for Opting Out

1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:
(A) Denying goods or services to the consumer.
(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.
(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.
(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.
(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.
(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

CCPA – Deletion of Data

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer….
(c) A business that receives a verifiable request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.
(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:
(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
(8) Comply with a legal obligation.
(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

CPReA – Changes to CCPA

- **Initiative on November 3rd California Ballot**
  - **Creates CA Privacy Protection Agency**
  - **Eliminates "safe harbor" period to correct discovered violations**
  - **Applicability:**

CCPA (2018)	Proposition 24 (2020)
• Businesses that earn $25 million in annual revenue. • Businesses that purchase, sell, or share the personal information of 50,000 or more consumers, households, or devices each year. • Businesses that earn 50 percent or more of their annual revenue from selling consumers' personal information.	• Businesses that earn $25 million in annual revenue. • Businesses that control the purchase, sell, or share the personal information of 100,000 or more consumers or households each year. • Businesses that earn 50 percent or more of their annual revenue from selling or sharing consumers' personal information.

  - **Difference in exemptions for Government use**

CPRA – For Consumers

- Proposition 24 would provide consumers with additional abilities regarding how businesses interact with their consumer data. Proposition 24 would require businesses to do the following:
- not share or sell a consumer's personal information to third parties upon the consumer's request;
- disclose whether the business collects *sensitive personal information*, the types of sensitive personal information collected, the purpose for which the sensitive personal information would be collected, and the length of time that the business intends to retain the sensitive personal information;
- provide consumers with an opt-out option for having their *sensitive personal information* used or disclosed for advertising or marketing;
- obtain permission before collecting data from consumers who are younger than 16;
- obtain permission from a parent or guardian before collecting data from consumers who are younger than 13; and
- correct a consumer's inaccurate personal information upon the consumer's request

The requirements listed above would be in addition to the requirements under the CCPA of 2018, which require businesses to:[1]

- disclose to the consumer the personal information that has been collected about the consumer and the commercial purpose of the information collected upon the consumer's request
- not sell a consumer's personal information to third parties upon the consumer's request.
- delete the consumer’s personal information upon the consumer's request; and

CPRA – Broader Exemptions

- vehicle information or vehicle ownership information retained or shared between vehicle dealers and manufacturers for the purpose of vehicle repairs;
- a consumer's credit standing, reputation, and worthiness for the purpose of consumer reports;
- personal information collected by a business for a job application and used within the context of the consumer's role as a job applicant, employee, or independent contractor;
- emergency contact information collected by a business and used within the context of having the information on file for emergency contact purposes;
- personal information collected by a business that is needed to administer employment benefits;
- personal information reflecting a written or verbal communication or a transaction between a business and an employee, owner, or independent contractor; and
- a student's grades, educational scores, or educational test results held on behalf of a local education agency.

CPRA – Penalties

- The CCPA of 2018 gave businesses 30 days to address and fix violations and data breaches before being fined. Proposition 24 would eliminate the notice period of 30 days for violations. Proposition 24 would adopt the following penalties for violations and data breaches:[1]
- up to $2,500 for each violation
- up to $7,500 for each violation involving the information of a person under the age of 16
- up to $750 per consumer per data breach incident or actual damages, whichever is greater
- Proceeds from fines and related settlements would be deposited into a Consumer Privacy Fund, which would be used to offset costs to courts, the attorney general, and the California Privacy Protection Agency that were associated with enforcing the consumer data law.[1]

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation
13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare

- Sharad Narayan Sharma
- Phuong Ngo
- Vartan Batmazyan

14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

Health & Healthcare

HIPAA

- A national standard that protects sensitive PHI from being disclosed without the patient's consent of knowledge.
- All covered entities must comply
- The sharing of specific information could be restricted upon request if it doesn't affect patient care
- A copy of PHI related to the patient may be requested at any time by the patient
- Applies to both physical health records as well as EHRs
- If a patient's data is incorrectly handled or falls victim to a breach, then the organization must notify the patient in a reasonable amount of time

HITECH Act

- Introduced by the Obama Administration in 2009
- Encourages the adoption of EHRs and improved privacy and security protections for healthcare data, introduces tougher penalties for HIPAA violations
- Deals with ePHI between doctors, hospitals and vendors that stores ePHI
  - Subtitle A - Promotion of health information technology
    - Improving healthcare quality, safety, and efficiency.
    - Application and use of health information technology standards and reports.
  - Subtitle B - Testing of health information technology. Subtitle C - Grants and loans funding
  - Subtitle D - Privacy and security of electronic health information.
    - Improving privacy and security of health IT and PHI
    - Relationship between the HITECH Act and other laws.

45 C.F.R. Part 160 and Part 164, Subparts A through E

Subpart A - General Provisions

Subpart B - [Reserved]

Subpart C - Security Standards for the Protection of Electronic Protected Health Information

Subpart D - Notification in the Case of Breach of Unsecured Protected Health Information

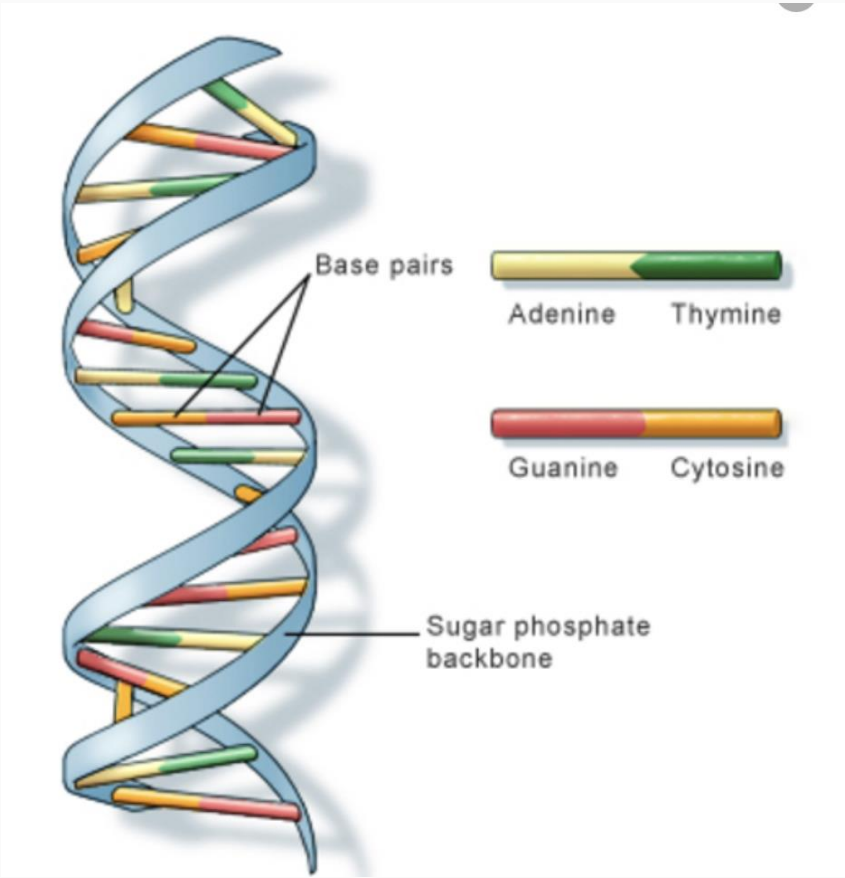
Subpart E - Privacy of Individually Identifiable Health Information

Universal DNA Database

Sharad Narayan Sharma

What exactly is DNA?

Deoxyribonucleic acid (**DNA**) is a nucleic acid that contains the genetic instructions for the development and function of living things.

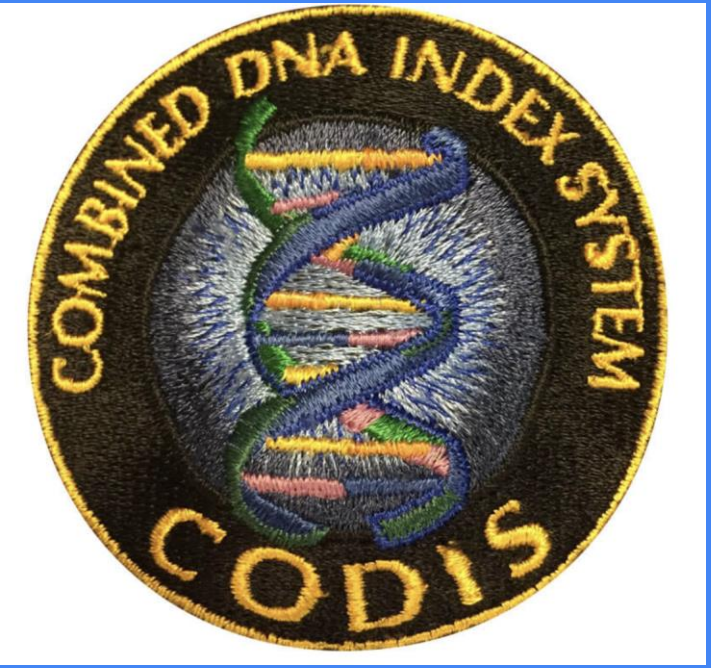


Why DNA?

- It is incredibly stable
- Storing it doesn’t require much energy

What is a DNA database?

- A DNA database or DNA databank is a database of DNA profiles which can be used in the analysis of genetic diseases, genetic fingerprinting for criminology, or genetic genealogy.
- DNA databases may be public or private, the largest ones being national DNA databases.



Types of DNA Databases

- **Forensic** : A forensic database is a centralized DNA database for storing DNA profiles of individuals that enables searching and comparing of DNA samples collected from a crime scene against stored profiles.
- **Genealogical** : GenBank is a public genetic genealogy database that stores genome sequences submitted by many genetic genealogists.
- **Medical** : A medical DNA database is a DNA database of medically relevant genetic variations. It collects an individual's DNA which can reflect their medical records and lifestyle details.

Are Universal DNA Databases any good?

- **It can provide another layer of evidence:** When a crime is committed without the presence of eyewitnesses, a person's DNA can serve as evidence of their presence at the scene.
- **There can be crime reduction rates :** DNA databases can help to reduce crime in communities that see criminal behaviors from repeat offenders.

  FACT CHECK : In a report published by Forbes and Quora, Jennifer Doleac, Assistant Professors of Public Policy and Economics at the University of Virginia, reports that DNA profiling makes violent offenders 17% less likely to reoffend.
- **The information can be used for genetic studies.**

Are Universal DNA Databases any good?

- **It facilitates information sharing between countries:** The sharing of data is becoming easier than ever before, with more information storage capacity available than ever before. That means international law enforcement agencies will be able to share more information with each other to pursue suspects that, in the past, may have slipped through the cracks.

  FACT CHECK : In 2015, there were already more than 60 different countries that were operating and maintaining at least one genetic database.

Privacy and Other Issues

- **Information can be stored infinitely :** Once DNA information is collected, the database can store that information for an infinite period of time. If the database is public and national, that information could be potentially exposed to individuals who want to use it for criminal intent.
- **Information can be hacked :** A DNA database does not need to be public to be vulnerable to the theft of the data it contains.
- **The data could be used against the individuals it represents**
- **DNA information is not 100% accurate.**
- **DNA sample contains information that can reveal people's ethnicity or how susceptible they are to disease. The risk of data abuse is therefore potentially high.**

Privacy and Other Issues

FACT CHECK : Terri Gossard submitted a DNA sample to two different databases and discovered a difference of 8 percentage points in her Irish and British descent.

- **DNA is susceptible to human error :** The DNA sample that is included in a database is susceptible to multiple layers of human error. The testing sample could be contaminated, for example, during the collection process.
- If a national database contains many samples, it might increase the chances of false positives.
- **Different nations may have different information storage procedures :** Some countries focus on the protection of freedoms. Others may not. If the information within a DNA database is shared, there is no guarantee that other countries will protect or destroy those records upon request. Different rules in holding data could create a patchwork of database laws that could put a person's genetic information at-risk globally.

Privacy and Other Issues

FACT CHECK : In 2010, the UK Government pledged to make changes to the length of time DNA samples are kept in the UK National DNA Database. These were included in the 2012 Protection of Freedoms Act. These changes ensure that the DNA (and fingerprints) of individuals arrested but not convicted of an offence is retained for a maximum of 5 years.In the U.K., more than 1.6 million fingerprint records were deleted in 2012. More than 1.7 million DNA profiles were deleted. An additional 7.7 million DNA samples, including 480,000 from children, were destroyed.

- Currently there are no comprehensive privacy regulations that would prevent governments from sharing DNA profiles with other groups, such as insurance companies.
- Searching the DNA database for partial matches raises concerns for the privacy of the relatives of people who are on the database.

CODIS AND NDIS - US Specific

- CODIS - Combined DNA Index System
- Used to describe the FBI's program of support for criminal justice DNA databases as well as the software used to run these databases
- NDIS - The National DNA Index System or NDIS is considered one part of CODIS
- CODIS was designed to compare a target DNA record against the DNA records contained in the database
- Laboratories that participate in the National DNA Index System are not required to track local or state conviction rates based on CODIS hits

CODIS AND NDIS - US Specific

- The DNA profile consists of one or two alleles at the 20 CODIS Core Loci
- No names or other personal identifiers of the offenders, arrestees, or detainees are stored using the CODIS software
- Pursuant to federal law (the DNA Identification Act of 1994), DNA data is confidential. Access is restricted to criminal justice agencies for law enforcement identification purposes. Defendants are also permitted access to the samples and analyses performed in connection with their cases.
- They do not mention anything related to data retention on the official website

References

1) CODIS and NDIS : https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet
2) Universal DNA databases: a way to improve privacy? :

https://academic.oup.com/jlb/article/4/3/637/4820756

1) UK National DNA Database:

https://www.yourgenome.org/facts/what-is-the-uk-national-dna-database

1) Ethics for DNA Database :

https://www.yourgenome.org/debates/is-it-ethical-to-have-a-national-dna-database

Health Devices: Data Privacy and Security

Phuong Ngo

Type of Health Devices

Wearables

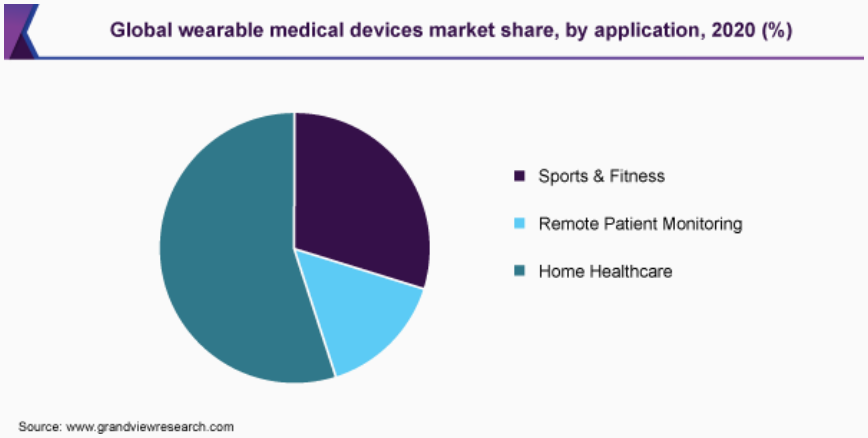
- Diagnostic
  - Fitness trackers
  - Smart watches
  - Wearable ECG monitors
  - Sleep tracker
  - Wearable blood pressure monitors
  - Other
- Therapeutic
  - Insulin Pumps
  - Sensing devices
  - Other

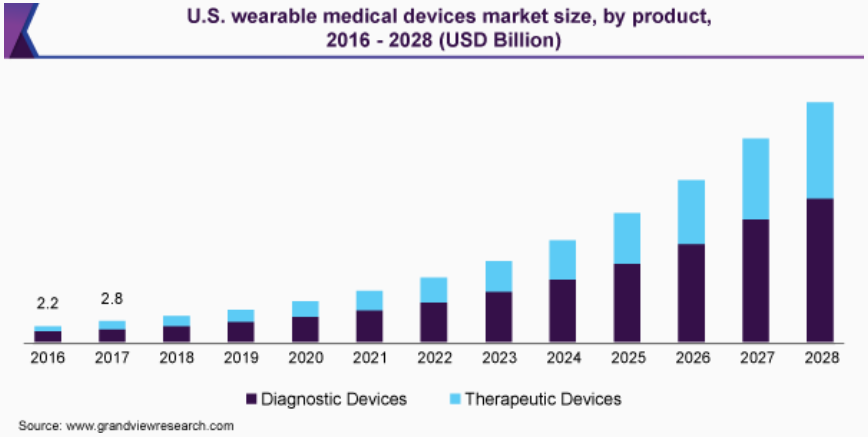
Implants

- Cardiac implantable electronic devices (CIEDS)
- Implantable Electrophysiology (EP)
- Pacemakers
- Other

Market & Stats

- Overall market size value in 2021: USD 21.3 billion, with North America dominating 38.1% of revenue share
- The diagnostic devices segment has the largest revenue share of 62.5% in 2020
- The strap/clip/bracelet segment dominated the wearable medical devices market with the largest revenue share of 51.2% in 2020





Data Collected & Storage

Type of Data

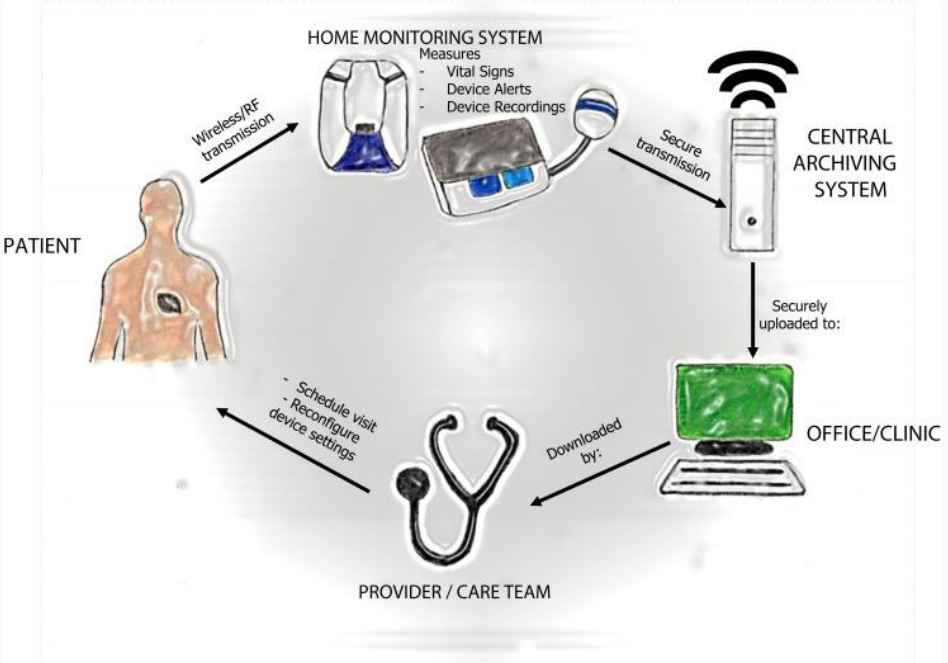
- Heart rate
- Steps Walked
- Blood Pressure
- Calories Burned
- Seizures
- Tones
- Measuring blood alcohol content
- Photos
- GPS location

Where data is stored

- On-premise
- Cloud
- Hybrid

How the data is being used

- Diagnostic and preventative measures by doctors and users
- Research and studies
- Marketing and advertising analytics by companies and third party analytics firms - users are sometimes not aware of this
- Poses privacy issues as privacy policy and how data is being use are often ambiguous, especially regarding consumer wearable health devices



HIPAA on Health Devices

Wearables:

- HIPAA Protection Does Not Extend to Wearables and Apps
- Private Companies Aren't Required to Be Protective and Transparent
- No Uniform Data Privacy Policy Exists for Apps and Wearables

Implants:

- Data collected is recognized and protected under HITECH and HIPAA
- FDA also issues safety communications on cybersecurity attacks on implantable devices and heavily criticizes companies that fail to address issues with such devices

Security Issues

- Same issues with IoT devices, since health devices are also considered as IoT (IoMT)
- Connected to some type of broadband and wireless network - Subjected to attack and hacking
- How providers choose to store the data also can introduce vulnerabilities (on-site vs. cloud)

Privacy Issues

- Many privacy issues met by IoT devices are also applicable to IoMT devices.
- Health data isn’t the only data being collected by these devices, especially for fitness trackers or any devices that are connected to apps
- HIPAA and HITECH only are applicable to implantable devices, ePHI and EHRs or health data, but not to consumer wearable devices and other data collected by them

Privacy Issues

- Big data mining by tech giants using personally identifiable health records without patient input also poses as a privacy concern as the data can be misused
- Steps taken, GPS tracking, tones and so on are among those data being collected without transparency on how they’re being used or stored
- Even when health data is being stripped off personal identifiers, it can be re-identified with low effort using machine learning techniques

References

1. IoT Big Data: Consumer Wearables, Data Privacy and Security, American Bar Association Website. https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/
2. Das, S., Siroky, G. P., Lee, S., Mehta, D., & Suri, R. (2021). Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. Heart rhythm, 18(3), 473–481. https://doi.org/10.1016/j.hrthm.2020.10.009
3. “Rethinking Patient Data Privacy In The Era Of Digital Health, " Health Affairs Blog, December 12, 2019. https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/
4. Wearable Medical Devices Market Size, Share & Trends Analysis Report By Type (Diagnostic, Therapeutic), By Site (Handheld, Headband, Strap, Shoe Sensors), By Application, By Region, And Segment Forecasts, 2021 - 2028. https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market
5. What is the HITECH Act. https://www.hipaajournal.com/what-is-the-hitech-act/

Privacy and Security Related to Medical Organizations and Research

Presented By: Vartan Batmazyan

Classifications of Data

- Anonymous Data:
  - Data that is not labeled with any personal identifying information (PII), nor with a code that the research team can link to PII
- Coded Data:
  - Data that is labeled with a code that the research team can link to PII when necessary
- Identifiable Data:
  - Data that is directly labeled with PII

Different Types of Research

- Quality of Life
  - No PHI, anonymous data
  - Remains within organization
- Clinical Research
  - Retrospective data collection
  - Active data collection

How Data is Collected

- Physical Forms or Audio/Video Recordings
- Online Data Collection
  - Qualtrics
  - RedCAP
- Retrospective Data Collection
  - Cerner
  - Kids
  - Epic

Where is Data Stored?

- Data collected by third parties are stored on their own servers
- Physically collected data is stored in locked compartments or transferred to a digital format manually and stored on the local device or approved storage solutions
- Digitally collected data is stored on either compliant devices or approved network storage solutions

BAA Required with 3rd Party Service Provider

- No use or disclosure of PHI by Business Associates shall be one that would violate HIPAA
- The Business Associate itself represents and warrants that it complies with each of the policies and procedures requirements and documentation requirements of HIPAA
- The Business Associate has a designated, agreed upon, period of time to report any compliance failures, breaches, or other breaches of data
- Upon termination of any agreement, the Business Associate will return or destroy any stored PHI

BAA Requirements for Network Storage

- Communication to and from the storage must be encrypted
- All PHI storage must be redundant and encrypted in its entirety
- Employees of the Business Associate are not allowed to interact with the data owner's storage unless explicitly given permission to do so
- Data mining or sale of PHI or other secure data is strictly prohibited
- Access to the online storage, as well as the storage itself, must be compliant with the data owner's security standards

Common Data Security Concerns

- The use of unencrypted flash drives to transfer study data
- Using personal email or personal network storage for storing study data
- Transferring data over the internet unencrypted
- Collecting identifiers when none are necessary
- Storing identified data in third party services as opposed to de-identified or anonymous
- Misunderstanding of what qualifies as PHI and how to properly deidentify data that is

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation
13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare
14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

HIPAA

Health Insurance Portability and Accountability Act

- The Health Insurance Portability and Accountability Act (HIPAA) sets requirements on the privacy and security of health information.
- The HIPAA Privacy Rule sets forth allowable uses and disclosures of protected health information and gives patients the right to obtain copies of their health data.
- The HIPAA Security Rule covers electronic protected health information, and the safeguards that must be implemented to keep the information secure.

The HIPAA Privacy Rules Cover:

Covered Entities and their Business Associates:

- Health plans
  - Health insurance companies,
  - Health maintenance organizations (HMOs)
- Health care clearinghouses
  - Billing services, Claims processing ,Consulting ,Data analysis
  - A business associate is a person or organization, other than a workforce member of a covered entity, that performs certain functions to covered entity that involve access to PHI.
- Health care providers that conduct certain health care transactions electronically
  - Clinics
  - Dentists
  - Doctors
- It is notable what is not covered

Non Covered Entities

Health information is now collected by apps and computer devices. The types of data collected are often exactly the same as the data collected by healthcare organizations, which are subject to the HIPAA regulations.

Some of the non covered entities are:
-Providers who do not have records in electronic form
- Social media(Facebook)
- Web search history
- Wearables(FitBit)
- Storage of data by the consumer/patient
- “Recreational” genetics(ancestry.com)

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Class Discussion Government Access – Apple - Wikileaks
12:30 – 13:00 Student Presentations – Government Regulation
13:00 – 13:35 Class Discussion – Privacy Regulation
13:35 – 13:45 Break
13:45 – 14:25 Student Presentations – Healthcare
14:25 – 15:00 Class Discussion - Healthcare
15:00 – 15:20 Current Event Discussion

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec11-ce.html