DSci529: Security and Privacy In Informatics

Government Access to Data Privacy in a Pandemic

Prof. Clifford Neuman

Lecture 10
26 March 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 – 12:45 Student Presentations – Privacy in the Pandemic
12:45 – 13:00 Class Discussion – Privacy in the Pandemic
13:00 – 14:10 Student Presentations – Government Access to Data
14:10 – 14:20 Break
14:20 – 15:00 Class Discussion Government Access
15:00 – 15:20 Current Event Discussion

Upcoming Presentations
Privacy&Security Regulation – April 2nd

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

- 30 minutes for this group to present

Upcoming Presentations Healthcare – April 2nd

- Vartan Batmazyan
- Phuong Ngo
- Sharad Sharma (DNA Databases)
- Ye Zheng - Fitness apps

- This group will have 40 minutes to present.

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 Access to Data Privacy in a Pandemic

Prof. Clifford Neuman

Lecture 10
26 March 2021
Online

Presentations: Privacy in the Pandemic

12:00 – 12:05 Introduction and Announcements
12:05 – 12:45 Student Presentations – Privacy in the Pandemic

- Jenny Gao
- Tanmay Ghai – Contact Tracing
- Yi Lin – Big Data in China related to the COVID Pandemic
- Gan Xin – Health QR Codes in China

12:45 – 13:00 Class Discussion – Privacy in the Pandemic
13:00 – 14:10 Student Presentations – Government Access to Data
14:10 – 14:20 Break
14:20 – 15:00 Class Discussion Government Access
15:00 – 15:20 Current Event Discussion

Pandemic and Privacy

DSCI 529| Spring 2021

Yueming Gao

Covid-19 Outbreak & Data Sharing

On 30 January 2020, the World Health Organization (WHO) declared the coronavirus disease 2019 outbreak a public-health emergency of international concern. Six weeks later, the outbreak was categorized as a pandemic.

The automated monitoring based on artificial intelligence technology is widely deployed, in particular, in a number of public places such as subways, railway stations, airports, shopping malls, grocery stores, social service centers, and so on in order to detect and control potential risks.

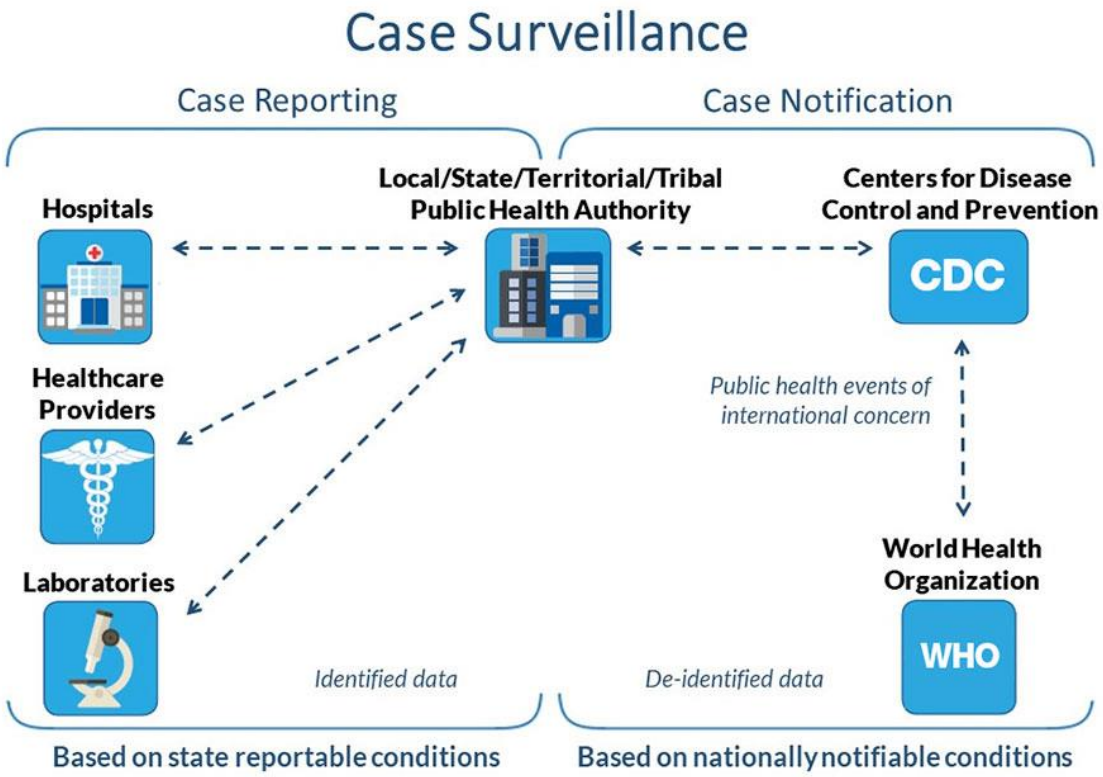
Personal information concerning identity, health, and a person's whereabouts is deemed an extremely important factor in making decisions on quarantine, isolation, or treatment.[3] In an age of big data, it seems both necessary and appropriate to use the big data technology to gather and process personal data that is helpful for the private/public decision-makers in this pandemic crisis.

Privacy Concerns

The first concern: Massive surveillance and the broad collecting and processing of the personal information

The second concern: The lack of regulations or specific policies to protect people's personal information in this global pandemic

How is COVID-19 Case Information Collected and Reported?



What data or IoT is revealed in this pandemic?

CDC has three COVID-19 case surveillance datasets:

COVID-19 Case Surveillance Public Use Data with Geography: Public use, patient-level dataset with clinical and symptom data, demographics, and state and county of residence. (19 data elements)

COVID-19 Case Surveillance Public Use Data: Public use, patient-level dataset with clinical and symptom data and demographics, with no geographic data. (12 data elements)

COVID-19 Case Surveillance Restricted Access Detailed Data: Restricted access, patient-level dataset with clinical and symptom data, demographics, and state and county of residence. Access requires a registration process and a data use agreement. (32 data elements)

Major applications of IoT for COVID-19 pandemic:

SNo	Applications	Description
1	Internet-connected hospital	The implementation of IoT to support pandemic like COVID-19 needs a complete integrated network within hospital premises
2	Inform the concerned medical staff during any emergency	This integrated network will allow the patients and the staffs to respond more quickly and effectively whenever needed
3	Transparent COVID-19 treatment	The patients can avail the benefits offered without any partiality and favours
4	Automated treatment process	The selection of treatment methods become productive and helps the appropriate handling of the cases
5	Telehealth consultation	This especially makes the treatment available for the needy ones in the remote locations via employing the well-connected teleservices
6	Wireless healthcare network to identify COVID-19 patient	Various authentic applications can be installed into smartphones, which can make the identification procedure smoother and more fruitful
7	Smart tracing of infected patients	The impactful tracing of patients ultimately strengthened the service providers to handle the cases more smartly
8	Real-time information during the spread of this infection	As the devices, locations, channels, etc. are well informed and connected, the on-time information sharing can be done, and cases can be handled accurately
9	Rapid COVID-19 screening	As the case arrived/found at first instance, the proper diagnosis will be attempted through smart connected treatment devices. This ultimately makes the overall screening process more superior
10	Identify innovative solution	The overall quality of supervision is the utmost goal. It can be achieved by making innovations successful to the ground level.
11	Connect all medical tools and devices through the internet	During COVID-19 treatment, IoT connected all medical tools and devices through internet which convey the real-time information during treatment
12	Accurate forecasting of virus	Based on the data report available, the use of some statistical method can also help to predict the situation in the coming times. It will also help to plan the government, doctors, academicians, etc. to plan for a better working environment.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7198990/table/tbl1/?report=objectonly

Lack of Privacy Protection Regulation

CDC's Privacy Protection:

CDC designed each dataset accounting for privacy and confidentiality and conducts ongoing privacy assessments using standard methods and systematically verifies the data prior to release. Strict privacy protections, including data suppression, were applied to all three datasets.

Conclusion:

The weak and unmanaged privacy protection causes greater concerns.

How European companies 's reaction to control the COVID-19 pandemic without undermining data privacy and security?

- Background Reading: France's privacy agency, the CNIL, stroke Google with a 100,000-euro fine in 2016, hoping to compel the company to "de-reference" disputed URLs on all its search engine domains worldwide, not only those in Europe.
- With the advent of the European General Data Protection Regulation (GDPR) in 2018 and the possible "ePrivacy Regulation," companies and institutions have increased their data awareness. These new regulations enforce stricter rules on privacy and data protection, setting new standards, in the words of the GDPR, for the "rights and freedoms of data subjects" around the globe.

State officials express privacy concerns over CDC's call for COVID-19 vaccine data registry

- 1. The CDC is instructing states to sign data use agreements that for the first time commit them to **sharing personal data, including names, birth dates, addresses and ethnicities**, with the federal government.
- 2. States including **New York** and **Minnesota** are pushing back against the initiative, with New York either refusing to sign the agreement or signing while refusing to share the information and Minnesota refusing to report identifying details to the CDC. Minnesota will submit only de-identified doses administered data.
- 3. New York Gov. Andrew Cuomo said that collecting personal data could dissuade undocumented people from getting vaccinated and called the CDC's initiative another example of the administration "trying to extort the State of New York to get information that they can use at **the Department of Homeland Security** and ICE that they'll use to **deport** people."
- 4. The CDC is not yet using a system **to encrypt personally identifiable data**, and department officials did not respond to the *Times*' requests for comment.
- 5. Collecting immunization data in the U.S. has been a state-by-state effort; two decades ago, there was a push to develop a federal registry that imploded after widespread backlash and concerns over **patient privacy and how the data would be used.**

COVID-19 Related Privacy Acts

COVID-19 Consumer Data Protection Act

On April 20, 2020, a group of Republican Senators, led by Mississippi Senator Roger Wicker, introduced the COVID-19 Consumer Data Protection Act ("CCDPA"). As written, the CCDPA would require companies under the jurisdiction of the Federal Trade Commission ("FTC") to obtain affirmative express consent from individuals prior to collecting, processing, or transferring their personal health, geolocation, or proximity information for the purposes of tracing the spread of COVID-19. Companies would also be responsible for disclosing at the point of collection how consumer data will be handled, transferred, and retained, while permitting individuals to opt out of the collecting, processing, or transfer process. Companies subject to the CCDPA would also be responsible for deleting or de-identifying all personally identifiable information once it is no longer being used for COVID-19 purposes.

Public Health Emergency Privacy Act

Following on the heels of the CCDPA, on May 14, 2020 Senate Democrats introduced the Public Health Emergency Privacy Act ("PHEPA"), which, among other things, would protect personal data collected in connection with COVID-19 from being used for non-public health purposes.

Other Privacy and Security Guidance

Financial Information Security

New York Department of Financial Services (NYDFS) issued Industry Letters detailing requests to regulated entities to prepare and submit plans of preparedness in response to COVID-19

The Financial Industry Regulatory Authority (FINRA) also issued an alert on March 26, 2020 providing guidance to firms on steps to "address increased vulnerability to cybersecurity attacks and to protect customer and firm data."

Education Information Privacy

On April 9, 2020, the Federal Trade Commission (FTC) issued guidance for companies operating in the education space during the COVID-19 pandemic, to ensure that organizations are aware of their compliance obligations with regard to the collection of personal information from children, as education moves online.

Department of Education (DOE) issued guidance designed to assist certain education agencies and institutions in preserving student privacy during the disclosure of personally identifiable information (PII) from student education records for COVID-19-related purposes.

To be conscious about your own Privacy and Security in COVID-19 Pandemic

- **1. How will the data be used?**
- Who collected/will collect this data?
- Is this the minimum amount of data necessary for decision making?
- Is this data representative?
- **2. Who will the data be shared with?**
- Who is it being shared with?
- What data is being shared?
- Can the data be transmitted/shared in a secured manner?
- Can the party receiving the data protect it?
- What was the individual's expectation when their data was collected?
- **3. How is the data being protected?**
- Does the project have the necessary resources and safeguards in place?
- Where will the data be stored?
- How is data being protected—now and in the future?
- Will vulnerable populations still be identifiable?
- What are the implications of the loss of privacy?
- What are the plans in the event of a data breach?
- What are the relevant laws?

Ways to protect your data security during Covid-19:

- Turn on automatic security updates, antivirus, and firewall.
- Don’t forget networking devices.
- Use Wi-Fi encryption options for access.
- Protect your digital identity.
- Keep your guard up in online chats and conferencing services like Zoom and WebEx.
- Use background blur or images to obscure your location.
- Use the right file-sharing service for the right task.
- Turn on device encryption.
- Phishing(jobs)

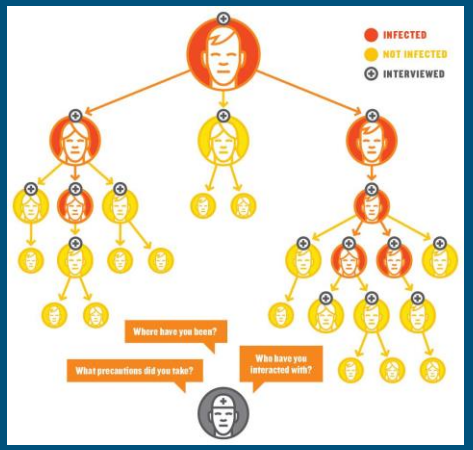
Privacy Implications of the Pandemic: Contact Tracing

Tanmay Ghai

Contact Tracing & Privacy

- **Contact Tracing**: “part of the process of supporting patients and warning contacts of exposure in order to stop chains of transmission” per CDC
  - Involves finding and tracing unreported infected people by locating back who could have possibly gotten infected from a confirmed infected entity
- **Privacy**: in class, we’ve discussed data collection, PII data, and system/public policies that relate to the broad concept of privacy
  - Involves (w.r.t contact tracing) tracing back individuals without collecting “unnecessary” information and revealing any personal data of any individuals in the tracing chain

- Rise of cases necessitated new infrastructure to discover new infections & slow the spread
  - Speed of development in places like China, Israel, Singapore vs. elsewhere **(was privacy considered?)**
  - **What types** and **how is data collected** to help with contact tracing? (GPS/location data, associations, partnerships with tech firms, etc)



Concerns w/ Contact Tracing

- As “tracing” and locating where people have been has become ubiquitous issue, many digital surveillance tools are being used for “social control”
  - Balance between **public safety and personal privacy,** on the global scale
  - Balance between **efficiency, policy & privacy, and efficacy**

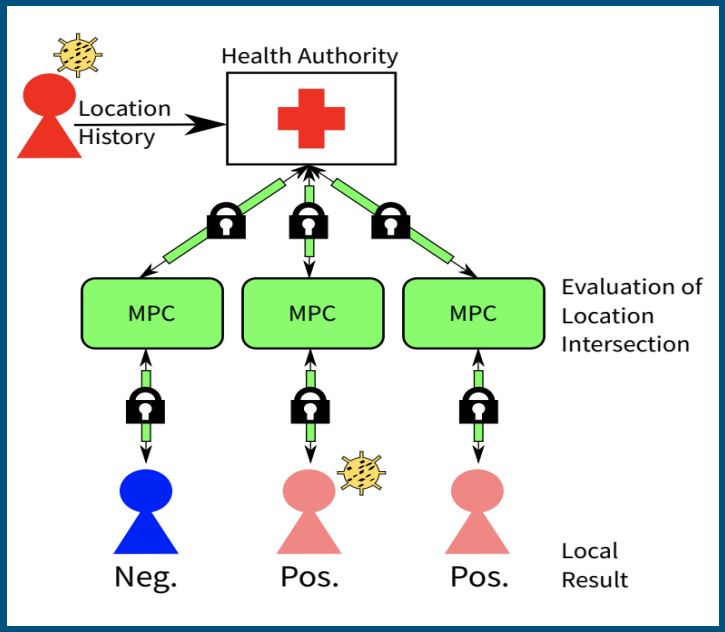
- Case studies:
  - **South Korea,** authorities have harnessed camera footage, smartphone location data, credit card purchase records to establish virus transmission
  - **Italy,** in Lombardy, authorities are analyzing location data transmitted by cellphones to determine following of government “lockdown order” and distance measurements to determine guidelines
  - **Israel,** the country’s internal security agency is using a cache of mobile location data (originally used for anti-terrorism efforts) to track down and pinpoint exposed individuals
  - **Singapore**, uses Bluetooth data on contact, requiring users to have their radio interface activated at all times for GPS data access

In-Depth w/ CT in South Korea

- South Korea's contact tracing touted as perhaps the **most aggressive, yet effective** "version"
  - Followed a **detect, contain, treat,** 3-step methodology
  - Over 600 screening/testing centers, over 150 diagnostic libraries, and thousands of health-care worker recruits
  - Deployed "intelligence" officers to investigate, with wide variety of available data sources (credit card transactions, television footage, etc)
  - **Efficacy** shown via case numbers (as one metric): only ~99k cases as of 3/2021 (U.S. in comparison at ~30M)
- **Privacy Implications:** study done Jung et al. (2020) showed the following:
  - 70% of cases disclosed significant PII data to public (gender, age, significant places (home/work) of individuals
    - Some cases even disclosed sensitive information such as **hobbies and religion**
    - In 48.7% of cases, patient's **social relationships** were disclosed

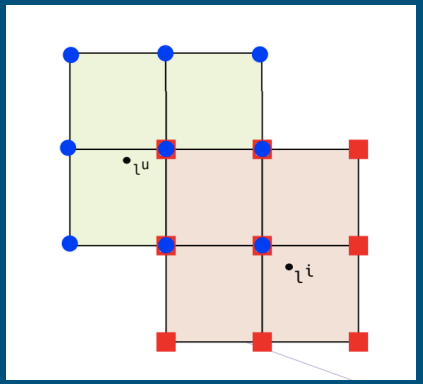
Privacy-Preserving Contact Tracing

- Framework proposed by Reichert, Brach, Scheuermann (one of many proposals!)
  - CT via GPS data, but centralized and **privacy-preserving**
  - **Secure multi-party computation:** protocols for joint computation on private, distributed data
  - **Idea**: HA's collect location histories of affected users; starts MPC sessions with individuals who want to trace; and creates circuit based on this network



System Design & Algorithm

- For each MPC session, computes **local intersection** to see if infected & non-infected people intersect
- **No information** about past locations of infected people or users is **revealed** to either side
- algorithm overview:
  - Input locations of the form **l = (x,y,t)** for geographical and temporal coordinates
    - Each user has **m** to-be-checked locations, and **n** location data points from infected individuals
    - **L** = set of locations from l where euclidean distance <= **t**
    - Both HA and user compute L for their data points; comparison done to see if region of user intersects with a region from an infected user (done via PSI & binary search)



Some Thoughts Moving Forward...

- **Privacy vs. Efficiency trade-off**: are users ok with private information being leaked if the methodology works?

- **Real-world efficacy of such a framework**: need real-world data to back-up the theoretical guarantees of this approach with actual results

- **Performance considerations** of such a framework vs. those implemented in various countries
  - **Practicality, cost, infrastructure** available for such computation?

References

- https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
- https://eprint.iacr.org/2020/375.pdf
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/#:~:text=Introduction%3A%20With%20the%20COVID%2D19,person%20infected%20with%20the%20coronavirus.
- https://ourworldindata.org/covid-exem
- https://blog.openmined.org/private-set-intersection/

Big data in China related to COVID-19

Yi Lin

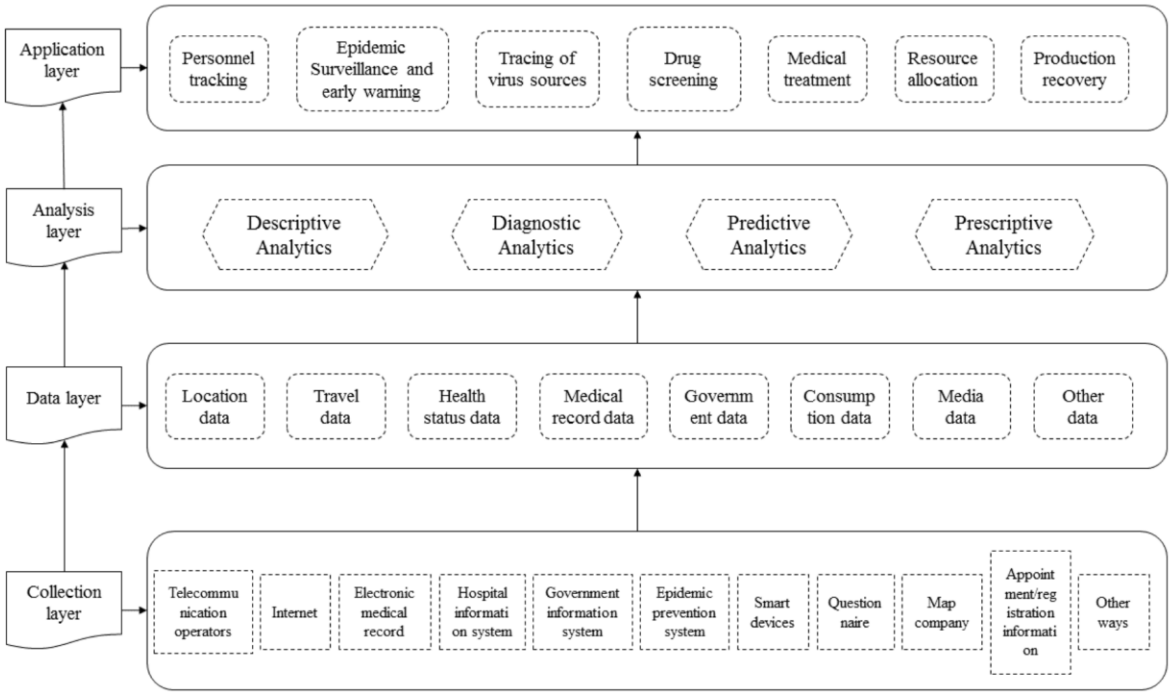
Content

- Data Use in China
  - Conceptual Structure
  - Data Concern (Privacy)
  - Data Legal Framework (Laws)
  - Data Retention and Location Tracking
- Electronic Measures to Fight COVID-19 Spread

  Health Code Apps (Application)

  Itinerary Card App (Application)
- Trade-off and Balancing

Conceptual Structure of COVID-19 with Big Data

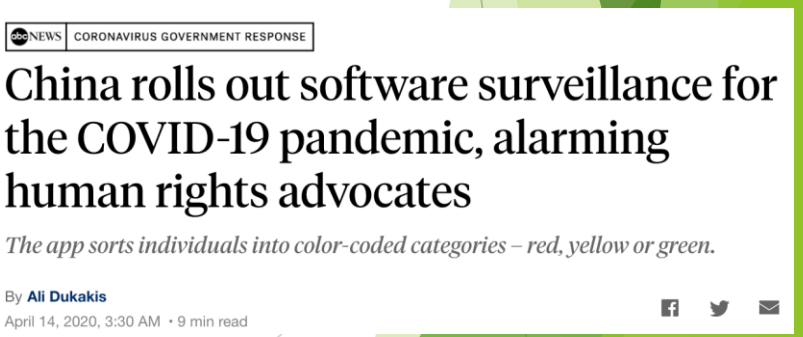


I. Data Use in China

- Location Data and Travel Data
  - Smartphone signaling data measures the density of people in specific areas and differentiate the display on the map through red, yellow, and green color differences to notify the public of areas to avoid/reduce the risk of infection.
- Medical and Health Data
  - Big data in health care can promote the timely detection and reporting of cases, and improve the efficiency of hospital management in a pressure environment.
  - Sharing data with emergency suppliers maintains unified prices to minimize unfair competition, ensure material quality.
  - Quick Response Codes (QR codes)
- New Media and Social Data
  - Inaccurate statements and misleading information
  - Using a series of lagging “social media search indexes” for various keywords including clinical symptoms of COVID-19 (such as dry cough, fever, chest pain, and pneumonia), the authors found that COVID-19 outbreaks could be found 6-9 days in advance.

II. Data Privacy Concern

- Leakage of personal data has become a widespread problem in China. In a survey done by a Chinese newspaper in 2020, 95% of respondents said their personal data had been stolen and almost 80% were concerned that their facial recognition data could be leaked from apps.
- Data sharing policies are often ambiguous
  - Share data with third parties without consent from user
- Expectation of Privacy
  - Surveillance tracking of its citizens through software during the pandemic
  - Fear that the government is merely using the ongoing public health crisis as a “convenient justification” to expand monitoring of its population[1].


abc NEWS | CORONAVIRUS GOVERNMENT RESPONSE

China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates

The app sorts individuals into color-coded categories – red, yellow or green.

By **Ali Dukakis**

April 14, 2020, 3:30 AM • 9 min read

III. Data Legal Frameworks (Laws)

1. Privacy and Data Protection
   - **Cybersecurity Law, National Guidelines**
     - The PRC Cybersecurity Law sets out general rules of data protection requirements for network operators. It contains an article prohibiting government authorities and their staff from leaking, selling, or otherwise illegally providing personal data.
     - Personal Data Protection Guidelines recently revised in March 2020, but such guidelines are recommended that lack of the force of law.
   - **Criminal Law**
     - Under the PRC Criminal Law, an individual may be sentenced to imprisonment for up to 7 years, if the circumstances are especially serious, for: (1) illegally selling or providing to others personal data; or (2) stealing or otherwise illegally obtaining personal data.

III. Data Legal Frameworks (Laws)

2. Data Retention and Location Tracking

- **Requirements under Cybersecurity Law and National Guidelines**
  - The Cybersecurity Law provides that network operators may only collect, store, process, disclose, and use personal data if individuals are notified of the purpose of such activities, and have consented to it.
  - However, the Cybersecurity Law does not distinguish between personal data and sensitive personal data.
- **Data Collection under Health Law**
  - On 02/09/2020, China issued a notice protecting personal information and regulating the use of big data to support joint prevention and control of diseases.
  - The Government only release information of public concern, such as “digitizing” individual patients. There are legal penalties for failing to follow the legal requirements on data handling.

III. Electronic Measures to Fight COVID-19 Spread

- Health Code Apps
  - The health code apps reportedly rely on a combination of self-reporting by the user, COVID-19 databases set up by government authorities, and data held by other sources including the public transportation, telecommunication, and banking sectors.
- Itinerary Card App
  - The itinerary card app does not require self-reporting by users, but asks for consent from users to access their travel history.
- Concern
  - Privacy experts have warned about the personal data breach and abuse associated with apps and have urged Chinese government to make sure the apps meet data privacy principles.
  - Responding to data privacy concerns, the apps claim that they do not collect the national ID numbers, home addresses, or any other personal data of users.

Trade-off and Balancing under the Pandemic

- How China flattened its curve
  - Big data technologies helped contain and control COVID-19.
  - China learned from SARS in 2002: the importance role of public health.
  - Chinese government limited the spread of the virus in real time under public health surveillance
    - Fast track to recovery
- What can US learn from China?
  - Need to centralized healthcare system
  - Big data tools: slow the spread of virus and moderate the social economic impact from the pandemic
  - Real-time monitoring capacity
- Data Privacy Concerns
  - Expectation of Privacy
  - Data Use, Data sharing, Data Retention

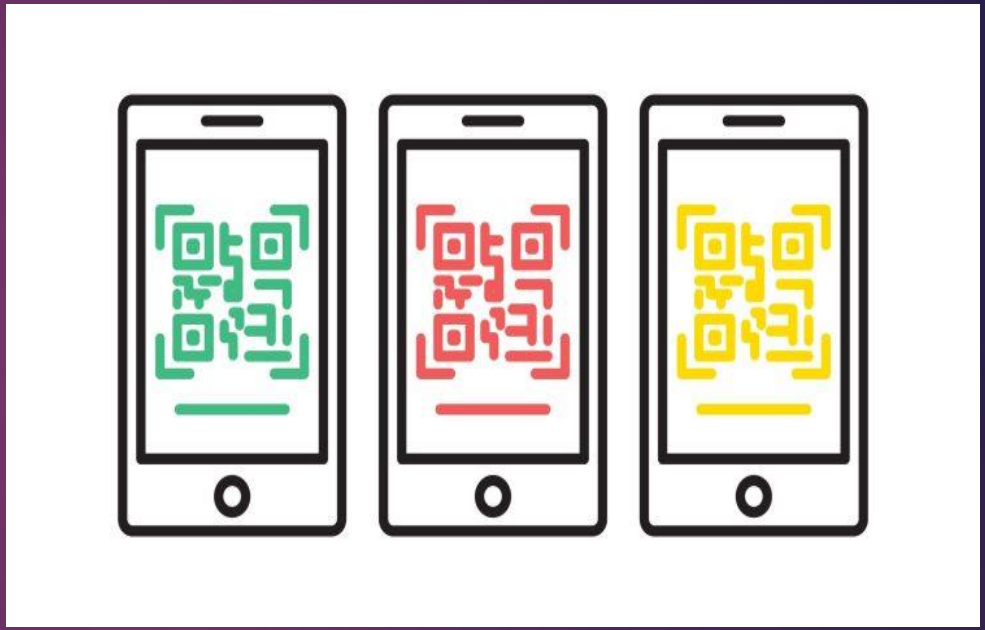
Work Cited

- https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355
- https://www.aicgs.org/2020/03/fighting-the-covid-19-pandemic-with-big-data-why-germany-should-learn-from-chinas-digital-experiments/
- https://www.usnews.com/news/best-countries/articles/2020-11-23/china-contains-the-coronavirus-with-science-and-strong-public-health-measures
- https://www.loc.gov/law/help/coronavirus-apps/china.php#_ftn21
- https://www.jmir.org/2020/10/e21980

Health QR code in China and its privacy issue

GAN XIN

DSDI 529 PRESENTATION, 2021 SPRING



Overview

1. Background
2. What is a health code and how does it work
3. Privacy issues

Background

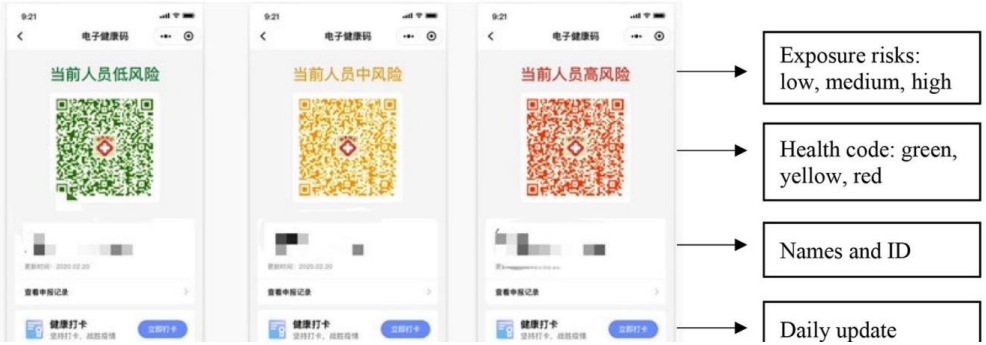
The outbreak of COVID-19 has resulted in a globally unprecedented response to health surveillance. At least 47 countries have implemented **contact-tracing apps** to contain the pandemic.

In China, two platforms Alipay and WeChat launched Health Code, a tracing app that aims to help governments identify people potentially exposed to COVID-19.

Not long after the Health Code in Hangzhou, other cities and provinces launched their own contact tracing apps.

The health QR code in China

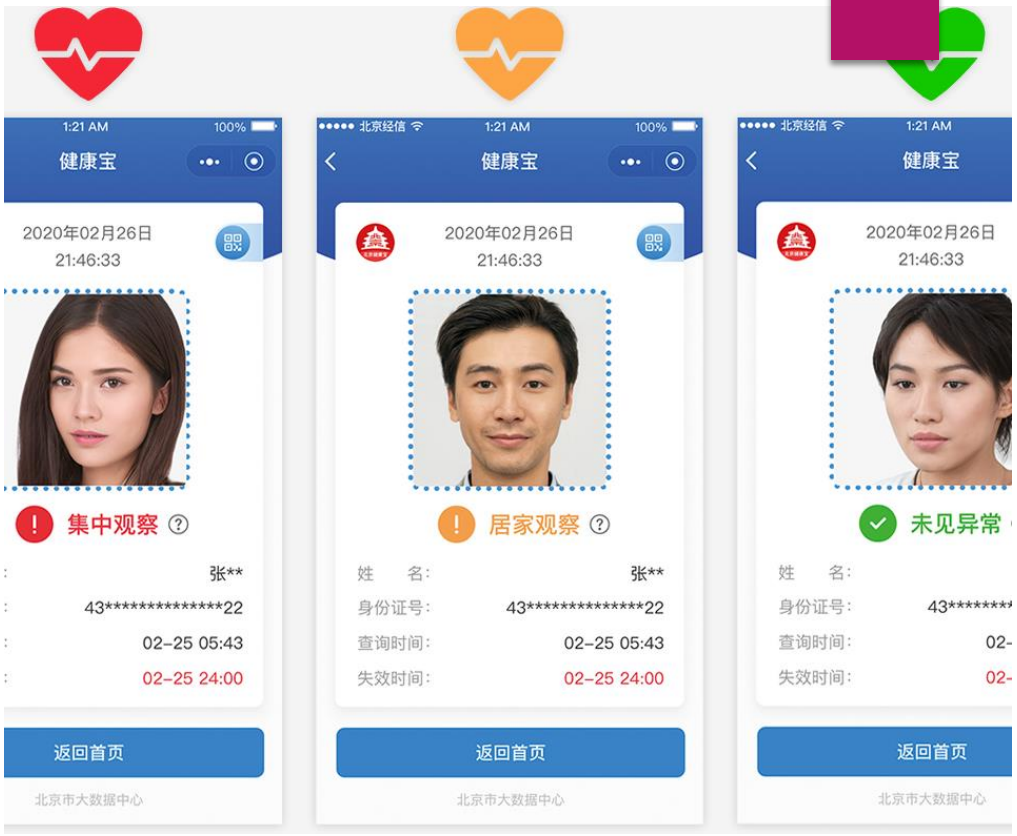
- Health Code can assess people's contagion risks based on factors like **travel history, duration of time spent in risky areas**, and **relationships to potential carriers**.
- Colors indicate the level of risk regarding Covid-19



The health QR code in China

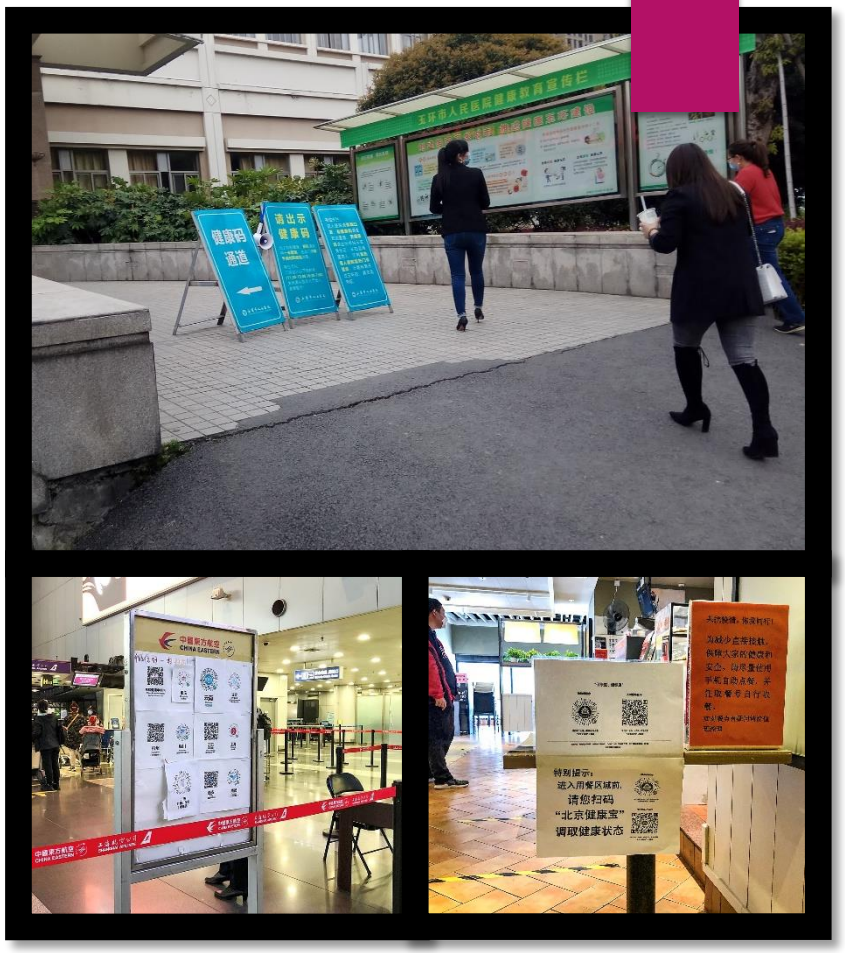
- Example:

Beijing Health Kit



The health QR code in China

- The color-based code has been assigned to 900 million users in over 300 cities, determining people's freedom of movement.



More than a QR code

There's various data involved in these Apps:

- **Personal info:**

Name, id, phone number, physical conditions, Covid-19 testing result, photos

- **Spatial-temporal data collected:**

by apps like WeChat and Alipay from daily usage

from cell phone GPS data,

from phone service providers

Some cases

Photo leakage from Beijing Health Kit

Some celebrities' photos were stolen from the Beijing Health Kit and sold online.

Personal information leakage of a Covid-19 carrier

Covid-19 carriers' personal information including name, photo, phone number and even ID number were made public by attackers.

Information mismatch

Many users in Shanghai noticed that their photos in the health code app are someone else's.
Users in Hubei found that photos and IDs are shown when login in their accounts.

Potential Privacy issues

- Data breach from the service providers
- Malicious scan of the code
- Health Discrimination
- Post Covid-19 usage of the data
- Controlled by the service providers

Post Covid-19 health code?

- **A controversial proposition was made that to add more features to the original health code.**

A health score for individuals.

Furthermore, scores for organizations using individual data.

Conclusion

- Many IoTs technologies used to fight against Covid-19 like all the contact tracing frameworks, big data applications are proved to be successful for controlling the spread of the virus.
- However, we should learn the lessons from the privacy issues occurred, for example we can implement more privacy preserving frameworks.

New Assigned Reading:

Privacy in the time of a pandemic

Chinmaya Pandit; Harshit Kothari; Clifford Neuman

2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges. Copenhagen, Denmark (online)

Chinmaya Pandit
Harshit Kothari
Clifford Neuman

Agenda

Introduction

Privacy Policy Changes

Data Dissemination

Changes to the Technology

Choice Vs. Compulsion

Conclusion

Introduction

- In December 2019, the world was struck by the unprecedented medical uncertainty that we now know as COVID-19

- In this paper, we explore the ways the ongoing pandemic has affected privacy ranging from the changes in privacy policy and regulation, through use of personal data for contact tracing and privacy in the technologies that have taken centre stage as we all work from home

Privacy Policy Changes

Many of the new measures are justified based on the extenuating circumstances of the pandemic, and the assumption is that they will only be used in such circumstances, but there is a danger that once the infrastructure is in place it will be used more broadly

Countries

1. Europe and UK
2. The United States of America
3. China

Data Dissemination

Even in the pre-pandemic era, there was a lot of information available to these third parties about us.

The aforementioned data collected is been put use in the following ways to combat the pandemic:

1. Contact Tracing
2. Mass Location Tracking
3. Surveillance Drones
4. AI and Big Data
5. Quarantine Enforcement
6. Biometrics and Symptom checking

Changes to Technology

1. Digital Banking
2. Online Education
3. Work from Home
4. Telehealth
5. Contactless delivery

Choice vs. Compulsion

Arguments regarding the Apple and Google technologies, or for that matter any other applications do not truly address the concern of choice vs. compulsion

Business, employers, or governments can impose requirements that citizen’s use the app in order to obtain services, or go to work, or perform other required activities, the choice whether to use a particular app might not be at the discretion of the end user.

Conclusion

The pandemic has not only created concerns for our health, but it has raised significant concerns regarding privacy

It is interesting to note that in the field of public health, monitoring the spread of disease and illness has always been referred to as epidemiological/disease surveillance, which highlights the intrusive nature of such monitoring

The pandemic could be a major event that puts privacy on the map, but it might also be an event that leads us to lose those protections we currently have.

Presentations: Privacy in the Pandemic

12:00 – 12:05 Introduction and Announcements
12:05 – 12:45 Student Presentations – Privacy in the Pandemic
12:45 – 13:00 Class Discussion – Privacy in the Pandemic
13:00 – 14:10 Student Presentations – Government Access to Data

- Xihao Zhou – Use of Data by Governments - Google in China
- Griffin Weinhold –Government encryption
- Yi Jin – How US and China collect and use personal data
- Congrui Li – Government use of camera surveillance
- Jinglun Chen – Use of location data
- Michelle Muldoon – Law Enforcement and Privacy w.r.t. Data Brokers
- Jiemin Tang – Security and Privacy regulation for food delivery services

14:10 – 14:20 Break
14:20 – 15:00 Class Discussion Government Access
15:00 – 15:20 Current Event Discussion

Why Google was Banned in Mainland China

- Xihao Zhou

The Main Difference

Between PISS (Personal Information Security Specification) and GDPR

Data Collection

	PISS	GDPR
Requirement of Data Collection	No one shall be deceived, tricked or coerced to provide data	Any data collection should have the “agreement” from individual users
The Definition of “Agreement”	Ask for agreement only required when: Collecting sensitive personal information, sharing or selling sensitive personal information	Data controllers need to prove that individual users have signed for agreement. The terms and policy should be easy to read and understand for any individual users.

Back to History

What happened in 2010?

Trigger

In January 2010, Google announced that, in response to a Chinese-originated hacking attack on them and other US tech companies, they were no longer willing to censor searches in China and would pull out of the country completely if necessary.

Then they shipped all service from Google.cn to Google.com.hk, anyone use the URL Google.cn will be relinked to the HK site.

What happened next

After Google moved everything to HK, people in Mainland China can only use VPN to access Google.

Baidu got over 65% Chinese search market shares, the number for Google was 2.57% in 2019.

Censorship

What is the censorship in China and why it is not acceptable to Google?

General Info

Internet censorship in the People's Republic of China (PRC) affects both publishing and viewing online material. Illegal content may be censored with the likes of pornographic content, content that promotes crime or violence and certain topics deemed to be controversial.

Self-Censorship Did by Google

Before Google give up China market, they accepted a self-censorship. After that self-censorship, people were not able to search sensitive key words on Google.cn like “Falun Gong” and “1989 Tiananmen Square protests”.

Public Safety vs. Freedom of Speech

- Google against “Freedom of Speech”?
- People are required to provide their IDs to speak on some Chinese social media
- Hate speech in EU: https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/

Similar Cases

What about TikTok in the US?

Why It Should be Banned

Trump cited national security concerns as the reason for enacting the executive order to ban TikTok after, according to Forbes (2020), “inquiry into the app uncovered several threats to the private data of US citizens.” In late 2019, almost nine months before the executive order, the US Navy instructed members to refrain from downloading the app on any government-issued phones and tablets, and to delete it if they had already installed the software; the app was then banned by the US Army as well (Tali, 2020).

Data they Collect

- User profile and phone number
- Device id
- Linked social media data
- User Generated Content(UGC), including photos, videos and comments
- Information to verify account like an email address
- Messages sent or received through TikTok chat function
- Cookies

Difference between TikTok and Google

TikTok did:

- Promised to provide more job opportunities
- Store sensitive data within US

Other facts about Google:

- Only have 32% Chinese search market shares and the rate keeps going down
- Employee salary is too high while the profit did not meet expectations

US Government Access to Encrypted Data

By Griffin Weinhold

The Paradigm

By the beginning of 2019, roughly 87% of web traffic was encrypted.

Section 230, which absolves tech companies of what their users post, supports tech's efforts in implementing end-to-end encryption.

While web data becomes more and more encrypted, governments across the globe wish to decrypt this data whenever needed.

In Motion in the US

In the United States, a bill titled the *Lawful Access to Encrypted Data Act (LAED),* which requires companies to grant access to encrypted data when requested via the proper legal channels, was put forth this past summer.

It is a “crystal-clear ban on providers from offering end-to-end encryption in online services”, says an Associate Director of of Cybersecurity at Stanford.

Precedence

In 2019, Australia passed a similar law that requires companies to hand over encrypted data at the request of government agencies. If companies lack tools to monitor and retain this data, they are forced to implement them.

Other Western nations have become increasingly focused on limiting encryption, and in 2016 France’s movement for a “backdoor mandate” fell short by only one single vote.

The United States’ EARN IT act, a “sneak ban” on encryption, which requires tech companies to surveil users more intensely to limit child exploitation was first introduced in March of 2020.

Privacy Concerns

The US Government is pushing for access to encrypted private data through the LAED act.

There are two methods by which the US can achieve access to our encrypted data

- Key Escrow
  - A copy of private encryption keys are saved on a third party server and are readily accessible, given a subpoena, to decrypt a person's data.
- Encryption Backdoors
  - These involve keeping track of the seeds used in Pseudo Random Number Generators so that government agencies can decrypt previously encrypted data.

Big Tech’s Stance

After the tragic San Bernardino shooting of 2016, Apple refused a judge’s order to hack the culprit’s iPhone.

This was deemed a threat to customer security by Apple, and would involved creating a “backdoor” that is too dangerous to create”.

Nevertheless the US Government paid a third party service to hack the device.

Positives

Governments must protect citizens at all costs.

Access to citizens' private data is inevitable.

With transparency, can be implemented fairly.

Will save more lives than it will harm.

Drawbacks

Backdoors are not secure, other nations and malicious individuals could find their way in.

The 4th amendment protects digital property from unlawful search.

The definition of ‘serious’ crime is ambiguous.

As we move to a more remote world, secure encryption is not a luxury but a necessity.

Conclusion

Encryption is imperative to every citizen’s security online, and to allow our government backdoor access is an infringement on our rights, security and privacy.

The ubiquity of encrypted data on the web today and its role in our justice system cannot be solved with an archaic approach and laws that compromise privacy without precedents set.

Overall - Government access to encrypted data at this moment cannot be allowed.

References

https://www.globalsign.com/en/blog/why-lawful-access-encrypted-data-act-threat-your-rights-and-privacy

https://duo.com/decipher/encryption-privacy-in-the-internet-trends-report

https://www.forbes.com/sites/forbestechcouncil/2018/10/26/should-world-governments-get-access-to-encrypted-data-11-tech-experts-weigh-in/?sh=3c2d41a436f7

https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html

https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-france/

https://www.businessinsider.com/what-is-section-230-internet-law-communications-decency-act-explained-2020-5

https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

https://www.brookings.edu/techstream/the-earn-it-act-is-a-disaster-amid-the-covid-19-crisis/

Big data in China related to COVID-19

Yi Lin

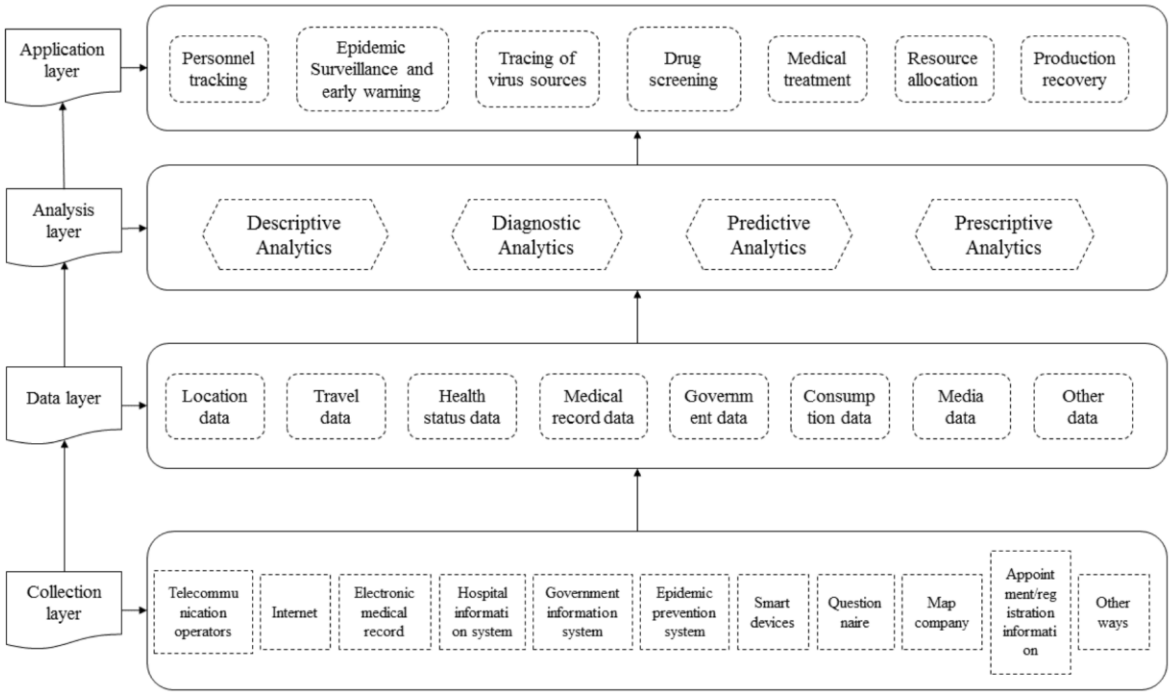
Content

- Data Use in China
  - Conceptual Structure
  - Data Concern (Privacy)
  - Data Legal Framework (Laws)
  - Data Retention and Location Tracking
- Electronic Measures to Fight COVID-19 Spread

  Health Code Apps (Application)

  Itinerary Card App (Application)
- Trade-off and Balancing

Conceptual Structure of COVID-19 with Big Data

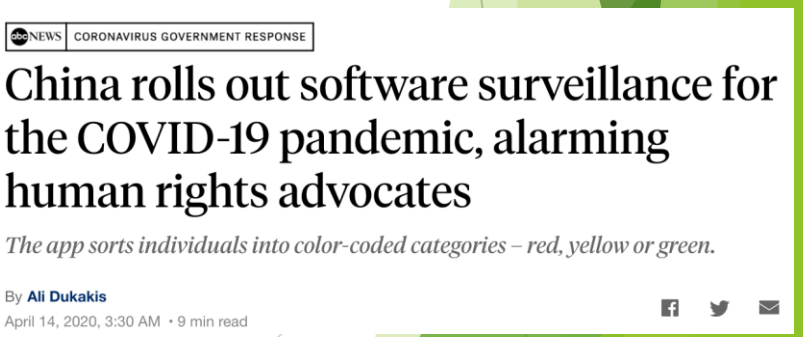


I. Data Use in China

- Location Data and Travel Data
  - Smartphone signaling data measures the density of people in specific areas and differentiate the display on the map through red, yellow, and green color differences to notify the public of areas to avoid/reduce the risk of infection.
- Medical and Health Data
  - Big data in health care can promote the timely detection and reporting of cases, and improve the efficiency of hospital management in a pressure environment.
  - Sharing data with emergency suppliers maintains unified prices to minimize unfair competition, ensure material quality.
  - Quick Response Codes (QR codes)
- New Media and Social Data
  - Inaccurate statements and misleading information
  - Using a series of lagging “social media search indexes” for various keywords including clinical symptoms of COVID-19 (such as dry cough, fever, chest pain, and pneumonia), the authors found that COVID-19 outbreaks could be found 6-9 days in advance.

II. Data Privacy Concern

- Leakage of personal data has become a widespread problem in China. In a survey done by a Chinese newspaper in 2020, 95% of respondents said their personal data had been stolen and almost 80% were concerned that their facial recognition data could be leaked from apps.
- Data sharing policies are often ambiguous
  - Share data with third parties without consent from user
- Expectation of Privacy
  - Surveillance tracking of its citizens through software during the pandemic
  - Fear that the government is merely using the ongoing public health crisis as a “convenient justification” to expand monitoring of its population[1].


abc NEWS | CORONAVIRUS GOVERNMENT RESPONSE

China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates

The app sorts individuals into color-coded categories – red, yellow or green.

By **Ali Dukakis**

April 14, 2020, 3:30 AM • 9 min read

III. Data Legal Frameworks (Laws)

1. Privacy and Data Protection
   - **Cybersecurity Law, National Guidelines**
     - The PRC Cybersecurity Law sets out general rules of data protection requirements for network operators. It contains an article prohibiting government authorities and their staff from leaking, selling, or otherwise illegally providing personal data.
     - Personal Data Protection Guidelines recently revised in March 2020, but such guidelines are recommended that lack of the force of law.
   - **Criminal Law**
     - Under the PRC Criminal Law, an individual may be sentenced to imprisonment for up to 7 years, if the circumstances are especially serious, for: (1) illegally selling or providing to others personal data; or (2) stealing or otherwise illegally obtaining personal data.

III. Data Legal Frameworks (Laws)

2. Data Retention and Location Tracking

- **Requirements under Cybersecurity Law and National Guidelines**
  - The Cybersecurity Law provides that network operators may only collect, store, process, disclose, and use personal data if individuals are notified of the purpose of such activities, and have consented to it.
  - However, the Cybersecurity Law does not distinguish between personal data and sensitive personal data.
- **Data Collection under Health Law**
  - On 02/09/2020, China issued a notice protecting personal information and regulating the use of big data to support joint prevention and control of diseases.
  - The Government only release information of public concern, such as “digitizing” individual patients. There are legal penalties for failing to follow the legal requirements on data handling.

III. Electronic Measures to Fight COVID-19 Spread

- Health Code Apps
  - The health code apps reportedly rely on a combination of self-reporting by the user, COVID-19 databases set up by government authorities, and data held by other sources including the public transportation, telecommunication, and banking sectors.
- Itinerary Card App
  - The itinerary card app does not require self-reporting by users, but asks for consent from users to access their travel history.
- Concern
  - Privacy experts have warned about the personal data breach and abuse associated with apps and have urged Chinese government to make sure the apps meet data privacy principles.
  - Responding to data privacy concerns, the apps claim that they do not collect the national ID numbers, home addresses, or any other personal data of users.

Trade-off and Balancing under the Pandemic

- How China flattened its curve
  - Big data technologies helped contain and control COVID-19.
  - China learned from SARS in 2002: the importance role of public health.
  - Chinese government limited the spread of the virus in real time under public health surveillance
    - Fast track to recovery
- What can US learn from China?
  - Need to centralized healthcare system
  - Big data tools: slow the spread of virus and moderate the social economic impact from the pandemic
  - Real-time monitoring capacity
- Data Privacy Concerns
  - Expectation of Privacy
  - Data Use, Data sharing, Data Retention

Work Cited

- https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355
- https://www.aicgs.org/2020/03/fighting-the-covid-19-pandemic-with-big-data-why-germany-should-learn-from-chinas-digital-experiments/
- https://www.usnews.com/news/best-countries/articles/2020-11-23/china-contains-the-coronavirus-with-science-and-strong-public-health-measures
- https://www.loc.gov/law/help/coronavirus-apps/china.php#_ftn21
- https://www.jmir.org/2020/10/e21980

Government Use of Camera Surveillance

Present by: Congrui Li

Introduction

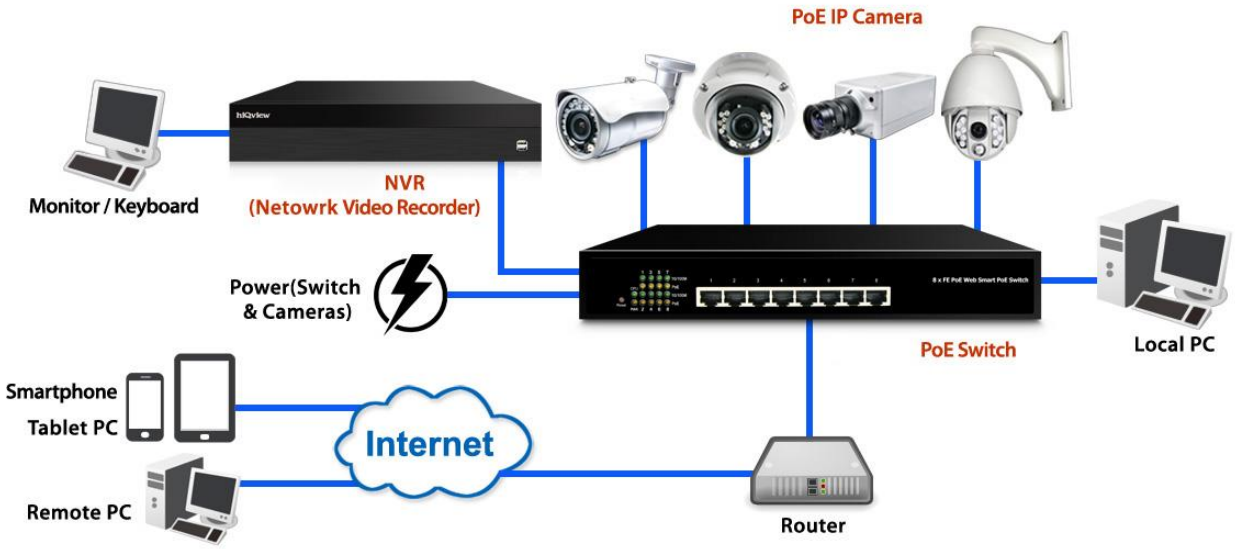
- Person of Interest
- "The Machine"
  - Citizen Identifiable Information and Profile
  - Government Camera Surveillance System
  - Phone and email records
  - Hack into most security system: phone, computer, company's system…
- Designed to prevent large-scale terrorist activities like 911
- But realized that she can also uncovered the plots against ordinary people
- Admin(Finch) use backdoors to help people

Development – Technical View

- Closed-circuit television (CCTV): analog cameras, Video Cassette Recorder (VCR)
- Digital Video Surveillance: Digital Video Recorder(DVR), Server, and Control
- Network Video Surveillance: real-time record and Internet transit
- Smart Video Surveillance: artificial intelligence, deep learning, and cloud computing

Development – Technical View

- Architecture – where is our data?



Development – Government View

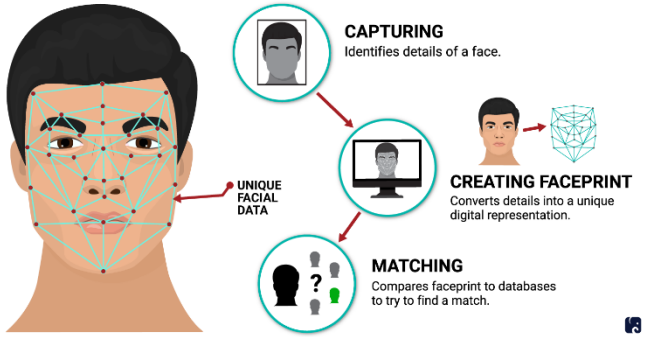
- Germany Uses CCTV Technology to Monitor Weapons During World War II in 1942
- By 1949, a U.S. contractor called Vericon started selling this technology for use in the commercial space.
- In 1961, in U.K., London Transport started installing CCTV cameras throughout the train station to bolster public safety.
- In Newcastle, with the introduction of a CCTV system in 1992, the crime rate in 1994 was 11% lower in street violence, 44% lower in burglary, and 44% lower in criminal offenses, compared to 1991
- Common in U.S. since 1990s, massive growth after 2001
- Common in China since 2005 with the Skynet mass surveillance system
- More and more countries and cities are using them.

How many cameras are there?

- 65% in Aisa, China has 170 million in 2018
- U.S. has 30 million in 2011
- UK has ~4 million

Country	# of CCTV Cameras	# of People	# of CCTV Cameras per 100 People
United States	50 000 000	327,167,430	15.28
China	200 000 000	1,392,730,000	14.36
United Kingdom	5 000 000	66,488,990	7.5
Germany	5 200 000	82,927,920	6.27
Netherlands	1 000 000	17,231,020	5.80
Australia	1 000 000	24,992,370	4
Japan	5 000 000	126,529,100	3.95
Vietnam	2 600 000	95,540,400	2.72
France	1 650 000	66,987,240	2.46
South Korea	1 030 000	51,635,260	1.99

New Threat to Privacy



- Facial Recognition and Smart Analysis
  - Face detection: open-source algorithm within seconds
  - Behavior recognition: fight detection, emotion recognition, fall detection, loitering, dog walking…
  - Anomalous or unusual behavior detection: recording a fixed area for a period of time and determining “normal” behavior for that scene.
- More reliable than operator but more ability to focus on everyone
- Facial detection technology developed quickly in the 2000s, and a forensic database became available to law enforcement in 2009.

- When data are connected, we have the most powerful tools to watch people, but also make everyone exposed.

Image Dataset Issues

- We can easily access to many online image datasets for research, on Kaggle, Github,…, that inlcuding photos, videos of real people
- No federal laws address commercial uses of facial recognition, but some states have privacy protections in place for consumers.
- The General Data Protection Regulation (“GDPR”) classifies biometric data as a special category of personal data because it makes it possible to uniquely identify a person. Biometric data is particularly significant in connection with the protection of individual privacy because (1) it is impossible to erase or change the data and (2) it is strongly identifying.
- Is the data only access by Government?

Cases in China

- SkyNet also works with top A.I. Companies, like Hikvision, SenseTime, Alibaba, Dahua …
- The system matches crime scene offenders to criminal databases in seconds to remove threats off streets
- Thus far, the tool has identified 2,000 suspects and solved 100 cases
- The system is also working on software that will parse data from thousands of live camera feeds and be used by police to track everything from vice and accidents to suspects on blacklists.
- Face Recognition widely used in public transportation, retail, etc

Cases in US

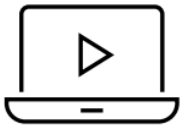
- Surveillance drones deployed in large public gatherings, including major protests
- Wide Area Persistent Surveillance (WAMI) is a form of airborne surveillance system that collects pattern-of-life data by recording motion images of an area larger than a city – in sub-meter resolution.
- Many American cities have been aggressive in putting in surveillance infrastructure, including Detroit, which recently installed cameras to monitor public housing residents, and Baltimore, whose police department conducted secret aerial surveillance of residents for several years.

Discussion

- A 3-tier model from Western Digital and Accenture

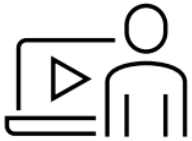
TIER 1

Current Public Safety Ecosystem: CCTVs are used retroactively to understand "what happened." Data is housed in siloes.



TIER 2

2025 Public Safety Ecosystem: Video data is crowdsourced from the private sector, augmenting CCTVs with AI capabilities and real-time analytics to identify anomalies.



TIER 3

2035 Public Safety Ecosystem: Video data is crowdsourced from residents, and data is supplied from disparate sources, to predict crime in real time.

Discussion

The Machine

Good?

Samaritan

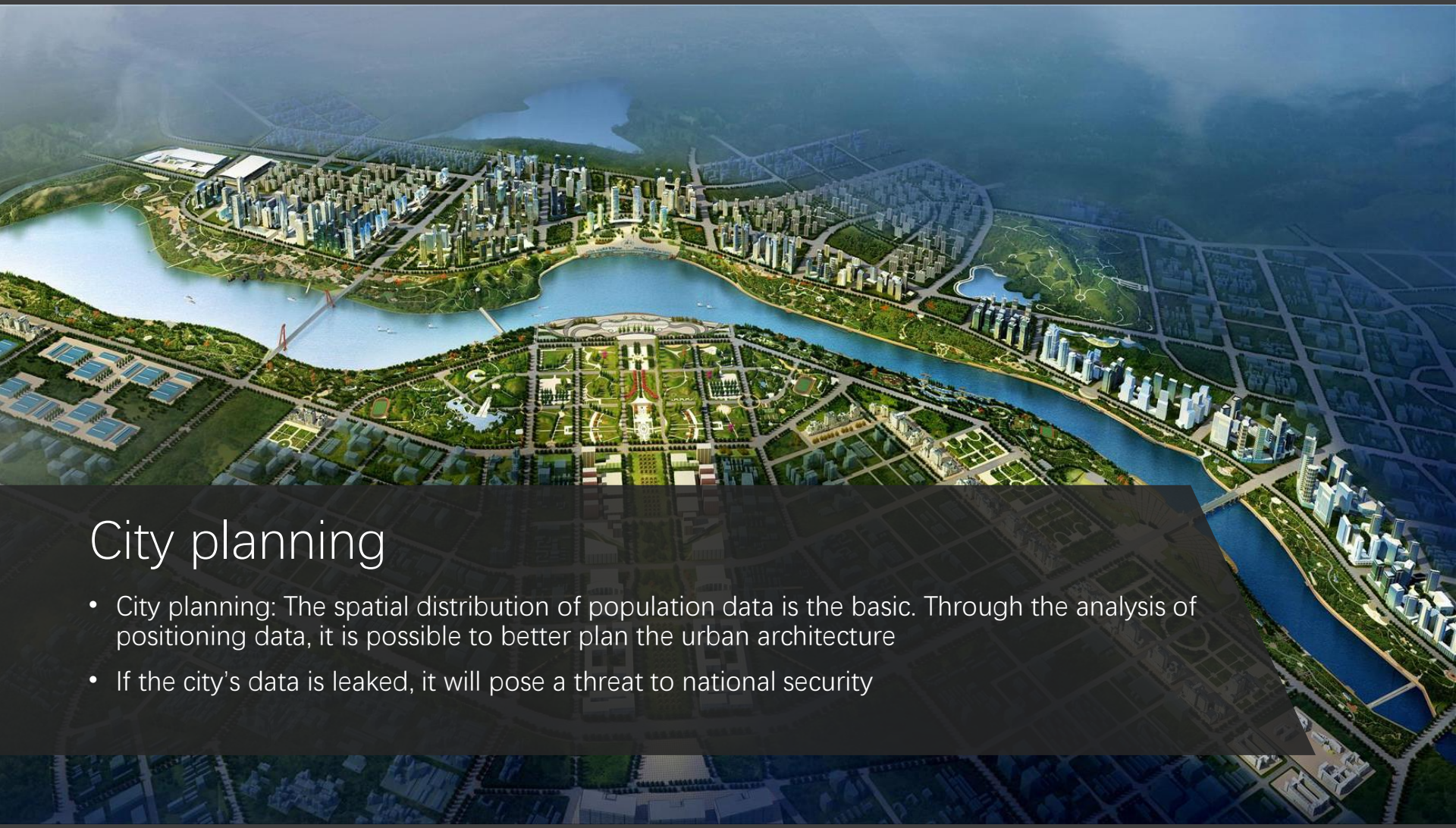
Bad?

Jinglun Chen

Use of location data

LBS

- LBS（Location Based Service) Use various types of positioning technologies to obtain the current device location. Then provide information and basic services through the mobile Internet.
- Positioning technology: GPS, WIFI positioning, IP address positioning,
- Geographic information system platform



City planning

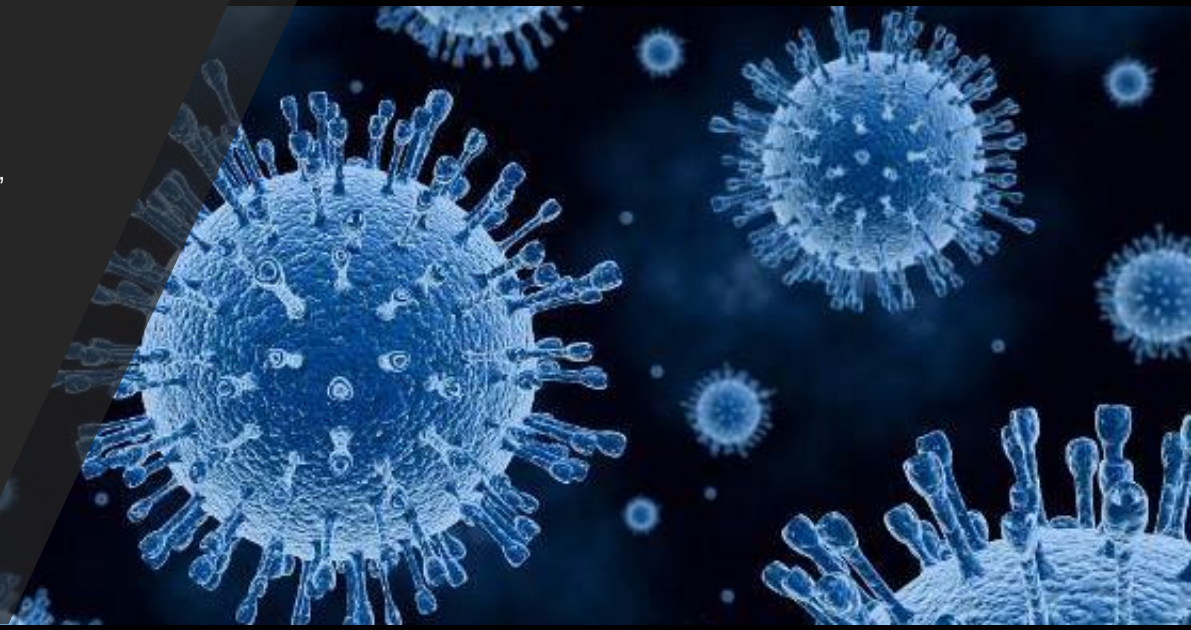
- City planning: The spatial distribution of population data is the basic. Through the analysis of positioning data, it is possible to better plan the urban architecture
- If the city's data is leaked, it will pose a threat to national security

app

- App can reflect the congestion of the surrounding environment through the flow of people's location, so as to achieve the purpose of safe travel. Such as navigation software. The government can send more traffic police to congested streets to maintain order
- But if this information is overused, people’s daily travel data will also be known, and the government will control housing prices based on this information.

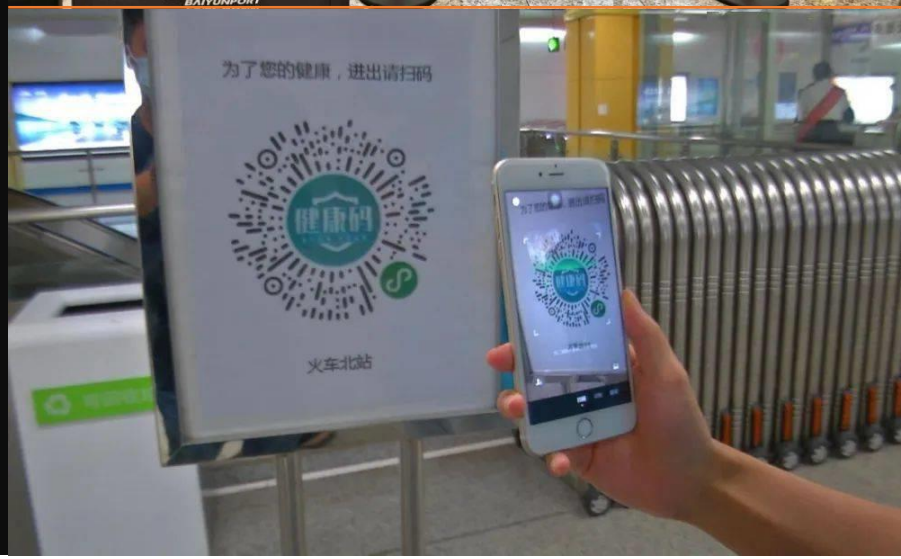
Passport during the epidemic

- COVID-19 has changed everyone travel mode. In China, for example, every citizen has his own health QR code. The QR code serves as an electronic certificate to go to the public place.
- There are three types of "health QR codes" green can be entered directly, red are quarantined for 14 days, and yellow quarantined within 7 days.
- Personal QR code can be obtained through WeChat applet



Passport during the epidemic

- All public places such as subways, train stations, airports, shopping malls, companies, etc. need people to scan the QR code to generate a personal health pass code before they can enter. This means that wherever you have been, the government has a record.



Passport during the epidemic

- Advantages: By using local data, the government effectively prevented the spread of the epidemic
- Disadvantages: All citizens' travel information is controlled by the government, which violates personal privacy. If personal itinerary information is leaked and used by others, it will threaten personal safety.
- With the birth of vaccines, countries may implement international vaccine passport

Conclude

- Most of the location data used by the government is to provide convenience to citizens, but some of the data is misused, which not only violates personal privacy, but also brings security threats.
- Need to find a better balance between them. Strengthen self-safety and privacy awareness. For example turn off the location function of many apps in the mobile phone, and minimize the connection to public WiFi

Reference

- https://baike.baidu.com/item/LBS/1742?fr=aladdin
- https://blog.csdn.net/yimenglin/article/details/91417124
- https://www.thepaper.cn/newsDetail_forward_11884559
- https://www.cebnet.com.cn/20170209/102363289.html


Thanks

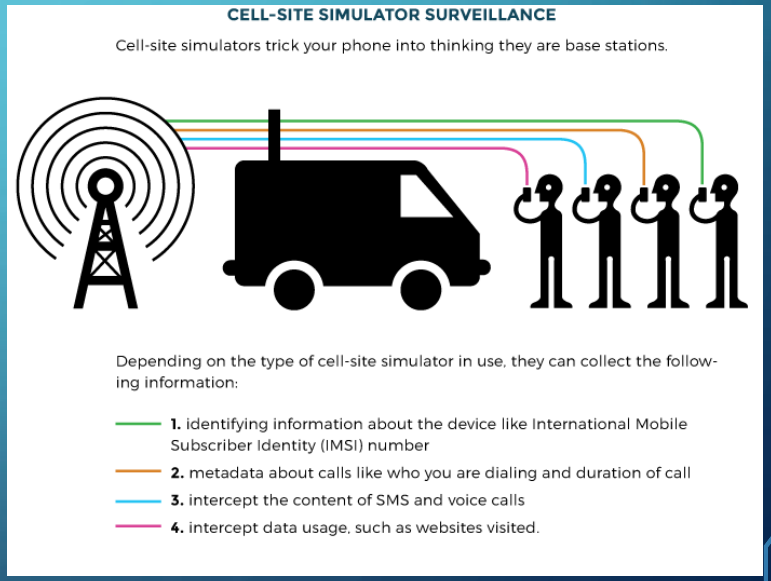
LAW ENFORCEMENT AND DATA BROKERS

-MICHELLE MULDOON

ARE THEY ACTUALLY WATCHING YOU?

LAW ENFORCEMENT DATA COLLECTION

- **Stingray/IMSI Catchers** –acts as a cellphone tower forcing all nearby cellphones to connect
- Can collect data usage, text, calls
- Up to 10,000 phones at a time
- CA requires warrant, but not all states do



LAW ENFORCEMENT DATA COLLECTION

- **Automatic License Plate Readers-** fixed in location or mobile on police vehicles

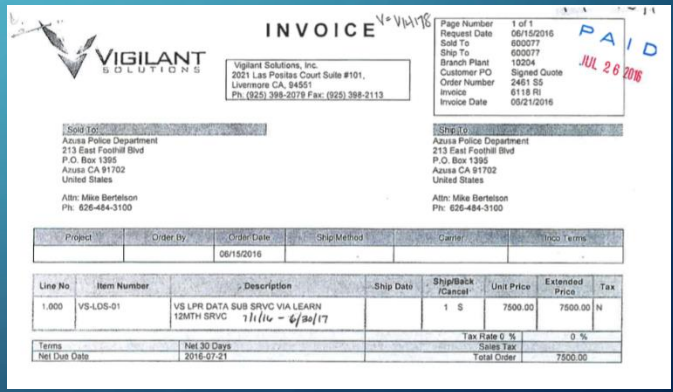
-collect location, time, date, make, model

-reads thousands of plates per minute

-data stored in databases for up to 5 years and maintained by third party

-data often sold to companies/insurers

-when combined with algorithm, can predict driving patterns and future locations



VIGILANT SOLUTIONS

INVOICE V-VIH178

Vigilant Solutions, Inc.
2021 Las Positas Court Suite #101,
Livermore CA, 94551
Ph. (925) 398-2079 Fax: (925) 398-2113

Page Number 1 of 1
Request Date 06/15/2016
Sold To 600077
Ship To 600077
Branch Plant 10204
Customer PO Signed Quote
Order Number 2461 S5
Invoice 6118 RI
Invoice Date 06/21/2016

PAID JUL 26 2016

Sold To:
Azusa Police Department
213 East Foothill Blvd
P.O. Box 1395
Azusa CA 91702
United States
Attn: Mike Bertelson
Ph: 626-484-3100

Ship To:
Azusa Police Department
213 East Foothill Blvd
P.O. Box 1395
Azusa CA 91702
United States
Attn: Mike Bertelson
Ph: 626-484-3100

Project	Order By	Order Date	Ship Method	Carrier	Inco Terms
		06/15/2016			

Line No	Item Number	Description	Ship Date	Ship/Back /Cancel	Unit Price	Extended Price	Tax
1.000	VS-LOS-01	VS LPR DATA SUB SRVC VIA LEARN 12MTH SRVC 7/1/16 - 6/30/17		1 S	7500.00	7500.00	N

		Tax Rate 0 %	0 %
Terms	Net 30 Days	Sales Tax	
Net Due Date	2016-07-21	Total Order	7500.00

LAW ENFORCEMENT DATA COLLECTION

- **Body Cameras-** collect audio, video, and location

-uploaded to databases run by police or third party

-faces can be used for facial recognition

-some videos can be edited/deleted

-many cases where footage went missing or corrupted file

LAW ENFORCEMENT DATA COLLECTION

- **Drones**- can have HD, thermal infrared cameras, high sensor, radar, cell phone interception, facial recognition

-can determine changes in landscape, foot prints, tire marks

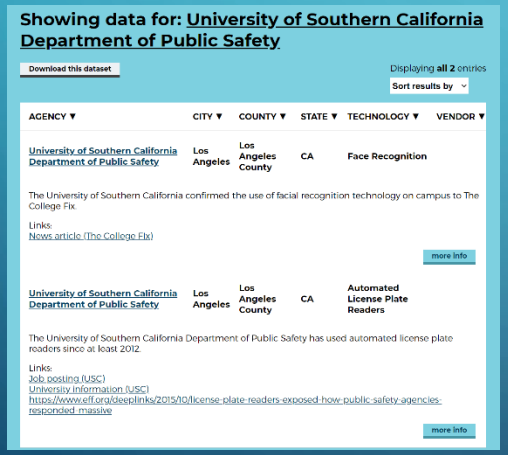
-large amount of data collected

-lots of states don't require warrant

LAW ENFORCEMENT DATA COLLECTION

- **Face Recognition-** collected from social media, CCTV, traffic cameras, ALPR, airports

-often misidentifies people especially ethnic groups



Showing data for: University of Southern California Department of Public Safety

Download this dataset

Displaying **all 2** entries

Sort results by

AGENCY	CITY	COUNTY	STATE	TECHNOLOGY	VENDOR
University of Southern California Department of Public Safety	Los Angeles	Los Angeles County	CA	Face Recognition	

The University of Southern California confirmed the use of facial recognition technology on campus to The College Fix.

Links:
News article (The College Fix)

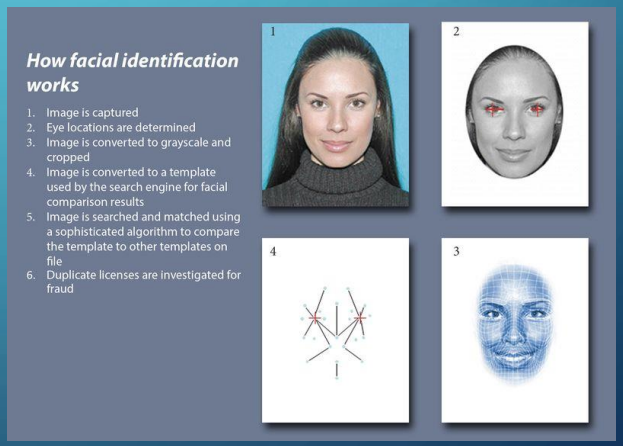
more info

AGENCY	CITY	COUNTY	STATE	TECHNOLOGY	VENDOR
University of Southern California Department of Public Safety	Los Angeles	Los Angeles County	CA	Automated License Plate Readers	

The University of Southern California Department of Public Safety has used automated license plate readers since at least 2012.

Links:
Job posting (USC)
University information (USC)
https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive

more info



LAW ENFORCEMENT DATA COLLECTION

-Iris/Tattoo Recognition

-Gunshot Detection- can hear voices

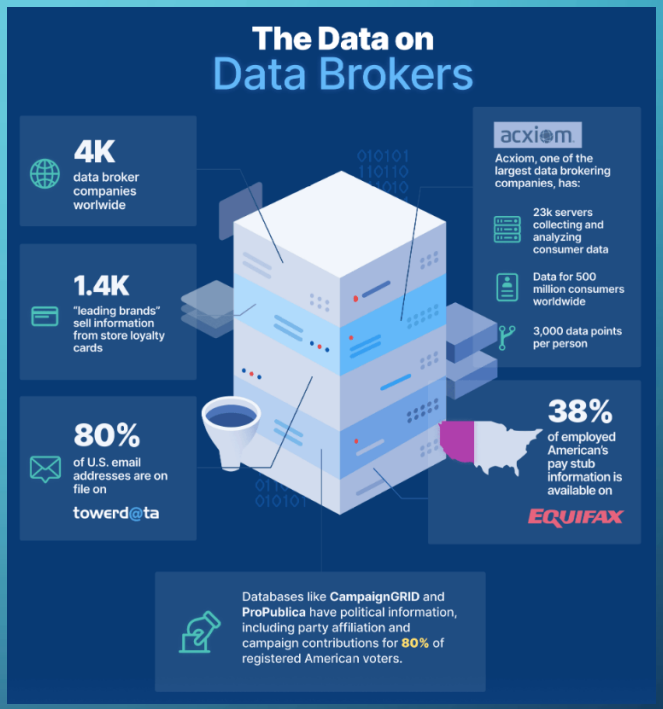
-Electronic Monitoring-ankle

-Surveillance Cameras

WHERE DOES THIS DATA GO?

DATA BROKERS

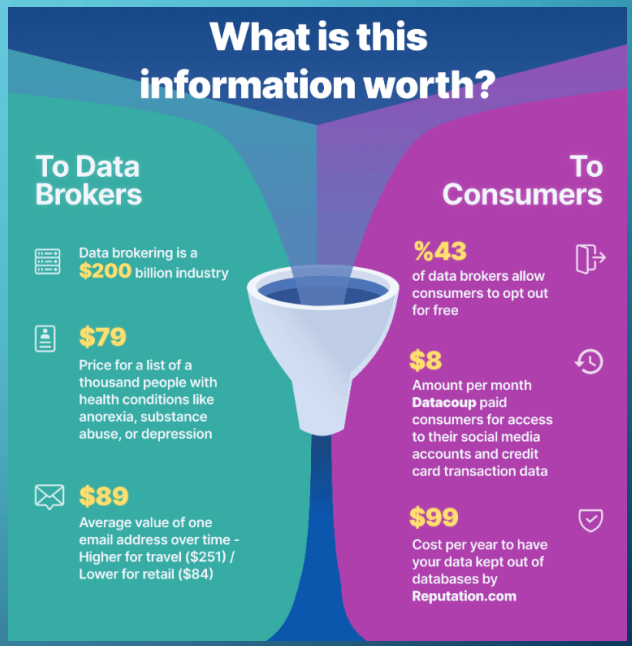
- Collect data from public websites (DMV, voter registration, paystub, store data)
- Combine/analyze with other data and sell it



GOOGLE YOURSELF

-Unless you've paid websites to remove you or you've done so manually…

-Data brokers list your name, age, address, phone number, email, family's information, assets



WHY IS THIS A PROBLEM?

-No consent

-Hackers can gain access to data

-Mistaken identity

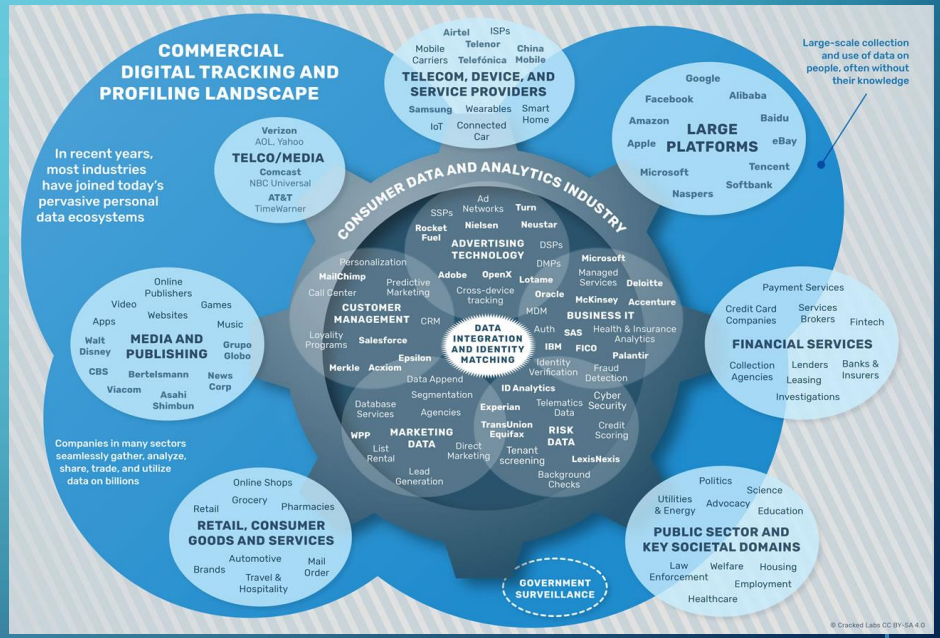
-Mass collection of sensitive data

-Groups of people targeted

-Have to pay to escape data brokers

-Victims of abuse/stalking have information put online by data brokers

-Connect data broker with data gathered from police and more… you have no privacy



REFERENCES

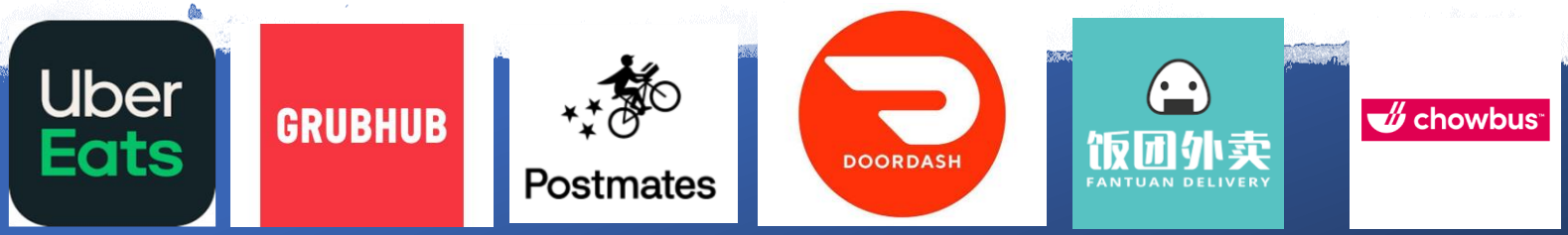
- Washington March Protests NSA Spying. (2013). [Photograph]. http://www.solidarity-us.org/files/NSAbanner.jpg
- WebFX Team. "What Are Data Brokers - And What Is Your Data Worth? [Infographic]." *WebFX* Blog, 21 Aug. 2020, www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/.
- Christl, Wolfie. "Corporate Surveillance In Everyday Life." *Cracked Labs*, Cracked Labs, 8 June 2017, crackedlabs.org/en/corporate-surveillance.
- University of Southern California Department of Public Safety - *Atlas of Surveillance*, atlasofsurveillance.org/search?utf8=✓&location=University of Southern California Department of Public Safety.
- Maass, Dave, and Nathan Sheard. "Street-Level Surveillance." *Electronic Frontier Foundation*, www.eff.org/issues/street-level-surveillance.

Security and Privacy in Food Delivery Services

Jiemin Tang

Growth of the Food Delivery Services

Major Food Delivery Services:



- Online food delivery has grown over 20% over the last five years
- Expected to grow to more than $220 billion by 2025, which accounts to approximately 40% of the total restaurant sales
- During the COVID pandemic, the four major food delivery services, DoorDash, UberEats, Grubhub, and Postmates, raked in roughly $5.5 billion in combined revenue from April to September 2020, more than doubled the revenue they had during the same period in 2019

Security and Privacy that Came with the Growth in Food Delivery Services

- With the flourishing of the food delivery services, many privacy and security concerns arise
- There has ben increased cyber attacks on the food delivery platform targeting the stored credit card and personal information of the users

- Some Incidents:
  - On May 4th, 2019, 4.9 million user records from DoorDash were accessed by an unauthorized third party
  - In March 2020, Cheney Brothers. Inc., the 10th largest food distributor in the US, disclosed that one of its websites had been hacked, allowing attackers to steal credit card and login information
  - Also in March 2020, the German food delivery company 'Takeaway.com N.V.' witnessed a distributed denial-of-service attack on its website
  - On October 5th, 2020, Chowbus suffered from an information leak, more than 800,000 records of the users and merchants were sent out to customers via email

Incidents of Food Delivery Service Information Leak - Chowbus

What was leaked:

- Two excel files of restaurant and user information were sent out to Chowbus users in the email
- None of the financial information or passwords are exposed, but the stolen data contained name, mailing address, email address, phone number of the users. Some famous Chinese celebrities were even on the list.
- Commission rates of the merchants (the amount they pay to the delivery platform)

How did it happen:

- Actual cause was not identified, and the motive for the breach is unclear.
- Allegedly disclosed by an inside man who was dissatisfied with the company

Incidents of Food Delivery Service Information Leak - DoorDash

What was leaked:

- Profile information including names, email addresses, delivery addresses, order history, phone numbers, as well as hashed and salted passwords
  - Hashed: represent data with a series of symbols
  - Salted: Take a random variable to the input before hashing.
- For some consumers, last 4 digit of credit cards
- For some Dashers and merchants, the last 4 digit of bank account number
- For approximately 100,000 Dashers, driver license number were accessed

How did it happen:

- DoorDash relied on a unnamed third-party service provider to manage parts of its website, mobile app, networks and systems
- Since no further information of the provider was given, it is hard to conclude how the breach happened

Privacy and Security Issue that Affects the Merchants - Fake Domains Registered by Grubhub

- Grubhub registered tens of thousands of fake domains to resemble a landing page for the official business
- The pages have complete online ordering forms, but are completely unassociated with the restaurants themselves
- Led users to believe that they are ordering directly from the restaurants to help restaurants avoid paying fees to Grubhub
- Grubhub typically charges a 3 to 15 percent commission fee; however, if the ordered is placed from the fake websites that Grubhub set up, Grubhub can bill for an additional 20 percent commission on a single order

Effect on the User

1. Spam email/text message/phone call because of information sold to third-party companies
2. Fraudulent phone call or emails
    - For example, calls about insurance expiration and request for payment
3. Stolen credit card number
    - Users could be billed for foods and drinks that they did not order because of stolen account information has stored credit card number
    - Stolen credit card numbers could be used on other websites
4. Identity theft
    - In the case of Dashers, their driver license might be used as proof of ID when opening accounts
5. Users' schedules and daily routines could be analyzed from the order history
6. Dietary preferences and allergies can be accessed
7. Stolen data can be used to predict the number of residents in the given household

Effect on the Restaurants

1. Small local restaurants feel forced into the online delivery platforms and pay high commission rates, otherwise they may be driven out of the market

2. Food delivery system that registered fake domain of the restaurants may have outdated menu and thereby affect the operation and reputation of the businesses, especially during peak hours

3. In the case of Grubhub registering fake domains for the restaurants, the extra commission rates charged would lead to decrease in revenue for the restaurants, which could largely affect small local businesses

4. Cutthroat competition among delivery platforms and between businesses

Actions Government has Taken

Targeting Food Delivery Services and restaurants:

CCPA requires the restaurants to update privacy policy to include, at a minimum:

- What kind of information is collected and processed from guests
- The reason to collect such information
- How the information is collected and processed
- How guests can request access to, change, move, or delete their personal information
- How you verify the identity of the person who submits one of the requests above
- How, why, and to who personal data is sold
- How a guest can opt-out of having their information sold

Targeting Food Delivery Services to protect the rights of restaurants

Assembly Bill No. 2149

- Prohibits a food delivery platform from arranging for the delivery of an order from a facility without first obtaining an arrangement with the food facility expressly authorizing the food delivery platform to take orders and deliver meals prepared by the food facility

Some Precautions We as Users Can Take

- Choose not to enter real name, use alias instead
- Do not store credit card information on the application, enter manually each time
- If live in apartment, avoid entering the complete unit number
- Be wary of unsecured Wi-Fi networks in the public
- Set up strong and unique password for each app we use


Thank you!

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:45 Student Presentations – Privacy in the Pandemic
12:45 – 13:00 Class Discussion – Privacy in the Pandemic
13:00 – 14:10 Student Presentations – Government Access to Data
14:10 – 14:20 Break
14:20 – 15:00 Class Discussion Government Access
15:00 – 15:20 Current Event Discussion

INF529: Security and Privacy In Informatics

Apple v. FBI

Prof. Clifford Neuman

Lecture 10
26 March 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 10
26 March 2021
Online

An Overview

- A couple of news stories

- 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.

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec10-ce.html