Personally Identifiable Information

Where (not) to find it
COM-402: Information Security and Privacy

(slide credits: Linus Gasser)

Overview

- **What is Personally Identifiable Information?**
  - Sensitive and nonsensitive information
  - Value for third parties
- Confidentiality Impact Levels
  - Definition
  - Factors to identify
- Management concepts
  - Pre-collection
  - Operating phase
  - Incident response
- Legislation in CH, Europe and US

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

Personally Identifiable Information

NIST Special Publication 800-122 defines PII as

any information about an individual maintained by an agency, including
(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(1) is directly sensitive data
(2) combines data from same service or from different services

What is Sensitive Data?

- Data that you don't want to be known by others, because:
  - It's embarrassing
    - Data about your private life
  - You might get a disadvantage if it is known
    - Medical data that could influence your job, social life, financial situation
    - Financial data (credit-card numbers)
  - It can put you in danger
    - Famous people's location
    - Allergies
    - Drone attacks
    - Medical implants

Question #1

Which of the following information is sensitive?

A. Username and password
B. Medical data
C. Credit-card number
D. Postal code
E. Birthdate
F. Contacts on a dating website

Breach in Sensitive Data

Ashley Madison
The Observer

Life after the Ashley Madison affair

It's six months since hackers leaked the names of 30 million people who had used the infidelity website Ashley Madison. Resignations, divorces and suicides followed. Tom Lamont sifts through the wreckage

1705   851

Tom Lamont

Sunday 28 February 2016
00.05 GMT

ON OUR WEDDING DAY

End of the affairs: at the time of the leak, Ashley Madison claimed to have 37.6m members, all of them assured the site was totally discreet.

Ashley Madison Hack Stats

37 Million - Number of Ashley Madison member account files that were criminally hacked worldwide

30 Days - Number of days the Ashley Madison hackers gave Avid Life Media to shut down its site

10 Gigabytes - Number of approximate gigabytes of the Ashley Madison hackers first release of stolen information

20 Gigabytes - Number of approximate gigabytes of the Ashley Madison hackers second release of stolen information

300 Gigabytes - The number of gigabytes of stolen Ashley Madison information the hackers claim to have taken in total

47 Countries - The number of countries Ashley Madison operates in

$500 000 - The reward offered by Ashley Madison for information leading to the arrest of the criminal hackers

3.7 million - The number of estimated emails that have not been cracked from the Ashley Madison hack, thanks to strong user-created passwords

How Nonsensitive Info gets Sensitive

- By combining different sources:
  - colocation and position of the other party
  - Pseudonymous comments on discussion-forum and disclosure of full name on another site
  - Anonymised database of movie-preferences and comments on movie-site like tomato
- By re-defining what is sensitive
  - Your job-description just got under scrutiny from government

Co-Location and Position
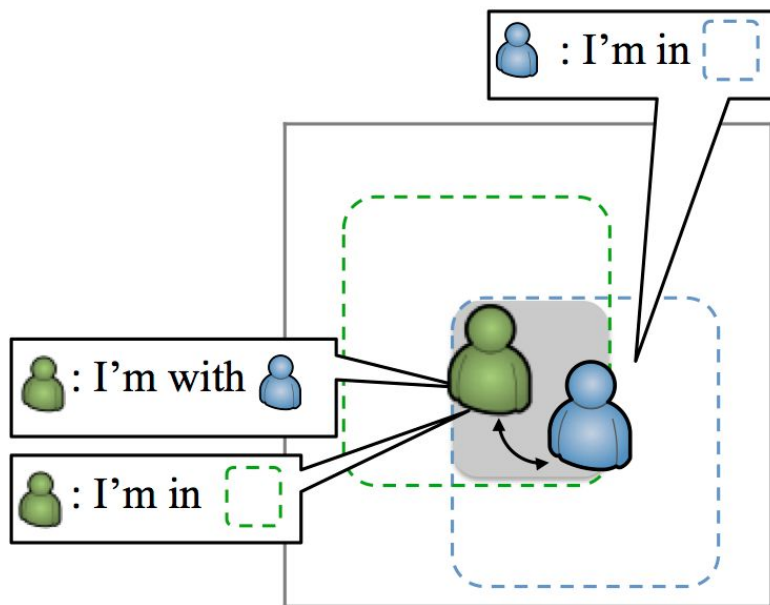
Reveals its position if position of
Is known

Co-location can be inferred from

- Face-recognition on pictures
- IP-addresses when connecting to a service
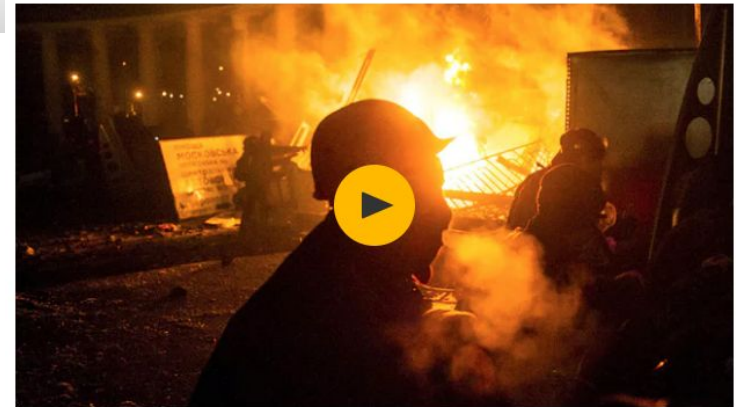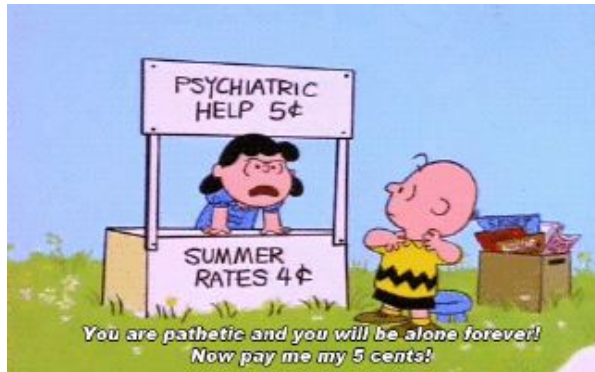- Available WLAN or GSM networks

So even if only [blue figure] has his GPS on, the

position of [green figure] can be inferred.

Why is Location so Privacy Sensitive?

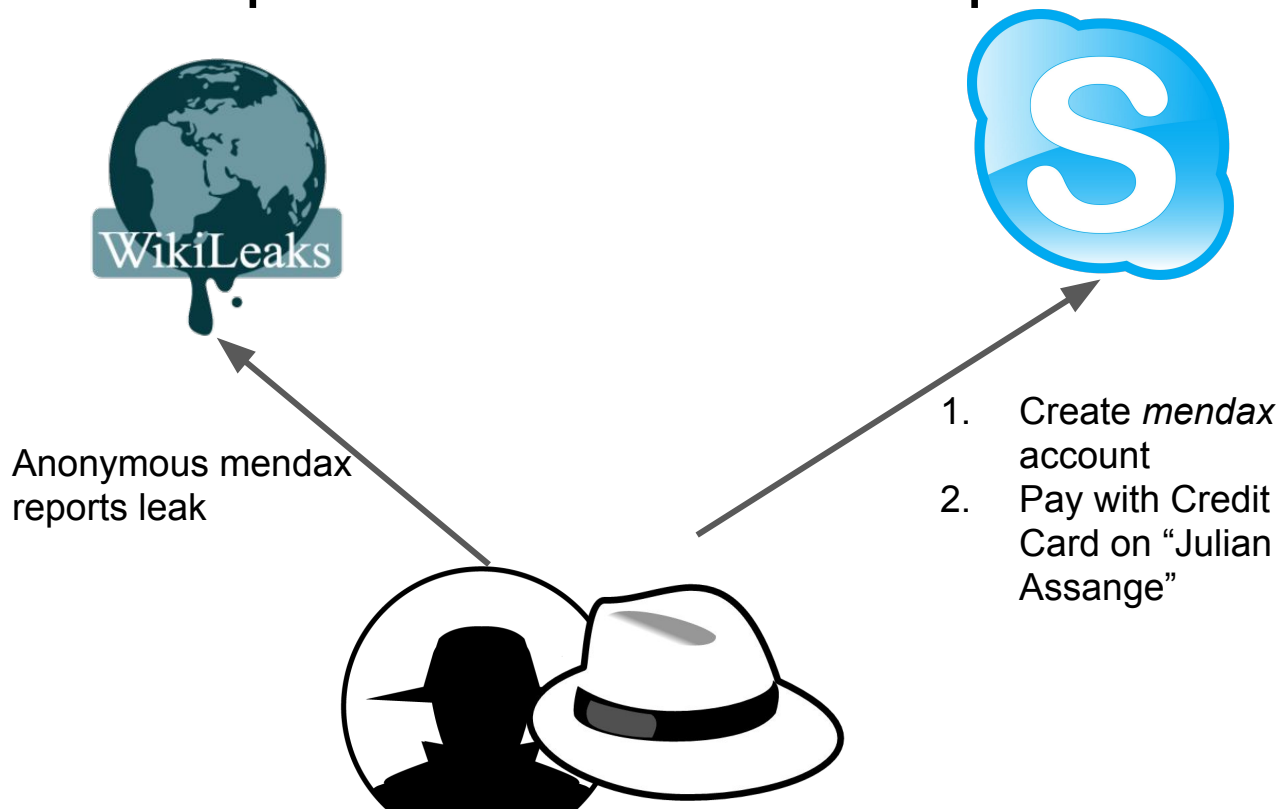Alcoholics Anonymous

Catch a CHEATER

Text messages warn Ukraine protesters they are 'participants in mass riot'

Mobile phone-users near scene of violent clashes in Kiev receive texts in apparent attempt by authorities to quell protests

"Dear subscriber, you are registered as a participant in a mass riot."

PSYCHIATRIC HELP 5¢

SUMMER RATES 4¢

You are pathetic and you will be alone forever! Now pay me my 5 cents!

10

Common Unique Data - Fake Example!

Anonymous mendax reports leak

1. Create *mendax* account
2. Pay with Credit Card on "Julian Assange"

Netflix De-Anonymization

WIRED   GEAR   SCIENCE   ENTERTAINMENT   BUSINESS   SECURITY   DESIGN   OPINION

Security Matters

Commentary by Bruce Schneier ✉ 🔊

POLITICS : SECURITY 🔊

Why 'Anonymous' Data Sometimes Isn't

By Bruce Schneier ✉   12.13.07

Last year, Netflix published 10 million movie rankings by 500,000 customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using. The data was anonymized by removing personal details and replacing names with random numbers, to protect the privacy of the recommenders.

Censored

Netflix Published Data - Anonymization

User	Movie	Date	Grade
Foo	The Wall	1/2/2003	5/5
Bar	Temps present	1/4/2004	4/5
Foo	Big Bang Theory	1/5/2004	4/5
Bar	Big Bang Theory	1/5/2004	5/5
Foo	Brazil	1/1/2002	4/5

→

User	Movie	Date	Grade
1234	554433	1/2/2003	5/5
4321	334455	1/4/2004	4/5
1234	16180	1/5/2004	4/5
4321	16180	1/5/2004	5/5
1234	773311	1/1/2002	4/5

Question #2

How do you think researchers de-anonymized the Netflix-data?

A. Breaking into the Netflix-database
B. Combining with other movie-related data
C. Machine-learning on the data
D. Breaking the hash used to anonymize the users

Netflix De-Anonymization

WIRED   GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION

Security Matters

Commentary by Bruce Schneier ✉ 🔊

POLITICS : SECURITY 🔊

Why 'Anonymous' Data Sometimes Isn't

By Bruce Schneier ✉   12.13.07

Last year, Netflix published 10 million movie rankings by 500,000 customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using. The data was anonymized by removing personal details and replacing names with random numbers, to protect the privacy of the recommenders.

Arvind Narayanan and Vitaly Shmatikov, researchers at the University of Texas at Austin, de-anonymized some of the Netflix data by comparing rankings and timestamps with public information in the Internet Movie Database, or IMDb.

De-Anonymization - 1/2

User	Movie	Date	Grade
1234	554433	1/2/2003	5/5
4321	334455	1/4/2004	4/5
1234	16180	1/5/2004	4/5
4321	16180	1/5/2004	5/5
1234	773311	1/1/2002	4/5

Netflix

+

User	Movie	Date	Grade
Foo	The Wall	1/2/2003	4/5
Foo	Big Bang Theory	1/5/2004	4/5
Foo	Brazil	1/1/2002	4/5

IMDb

→

De-Anonymization - 2/2

User	Movie	Date	Grade
Foo	The Wall	1/2/2003	5/5
Foo	Big Bang Theory	1/5/2004	4/5
Foo	Brazil	1/1/2002	4/5
Foo	Knightrider	1/6/2005	5/5

Attacker learns this new information

Re-defining what is sensitive

- Change of government and change of policy
  - Trump's government asking who visited clima-conferences
- If DNA is available and insurance companies find correlations between Genes and Illness
- https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

Value for Third Parties

Google: Serve better ads
Medical: Better treatments
Government: Better services

Ransom on divulging information
Identity-theft or selling the data
Killing in case of enemies of the state

Abusing PII to Hack

MAT HONAN   GEAR   08.06.12   8:01 PM
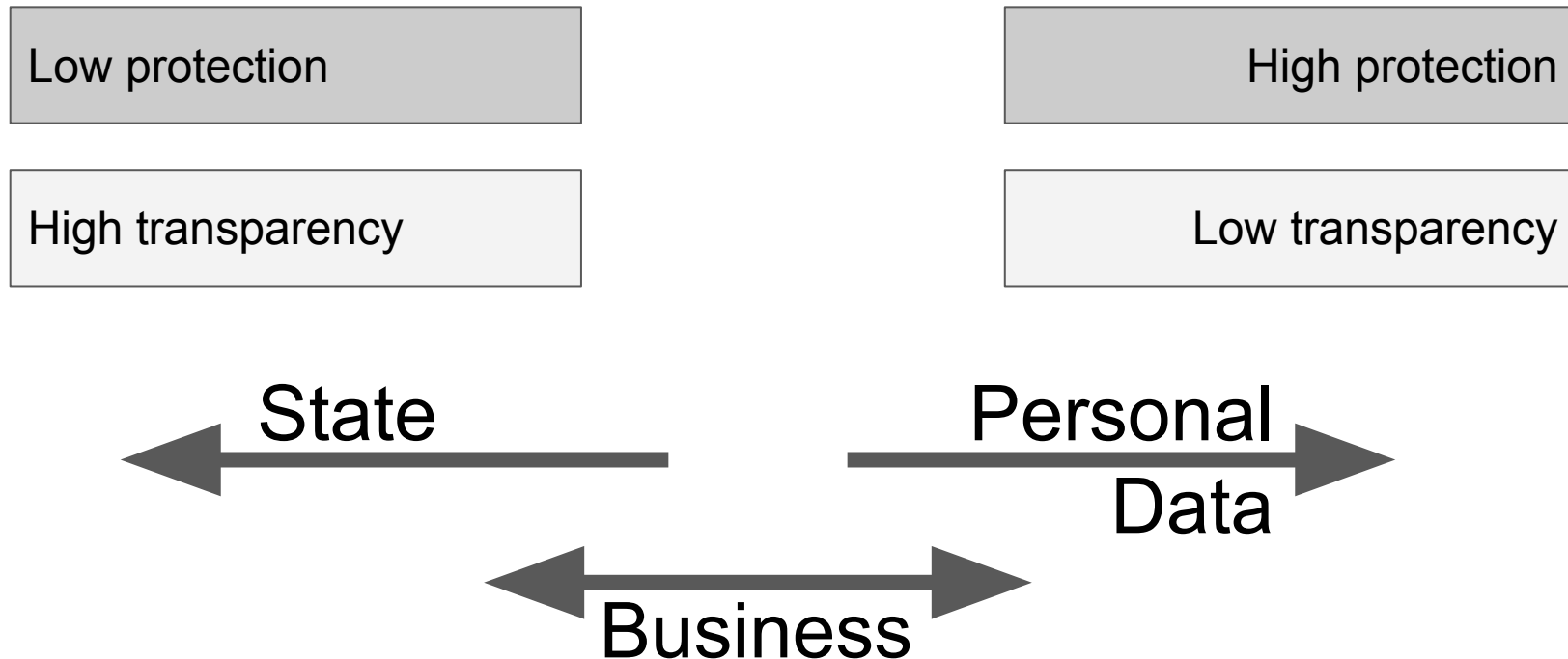
HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

SHARE

SHARE
838

TWEET

COMMENT
0

EMAIL

State Data, Business Data, and PII

Low protection	High protection
High transparency	Low transparency

State ←——————

Business ←——————→

Personal Data ——————→

Overview

- What is Personally Identifiable Information?
  - Sensitive and nonsensitive information
  - Value for third parties
- **Confidentiality Impact Levels**
  - Definition
  - Factors to identify
- Management concepts
  - Pre-collection
  - Operating phase
  - Incident response
- Legislation in CH, Europe and US

Confidentiality Impact Levels

From NIST: The PII confidentiality impact level - low, moderate, or high - indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

- Impact levels
  - Low - limited adverse effect
  - Moderate - serious adverse effect
  - High - severe or catastrophic adverse effect
- Factors to identify
  - Identifiability
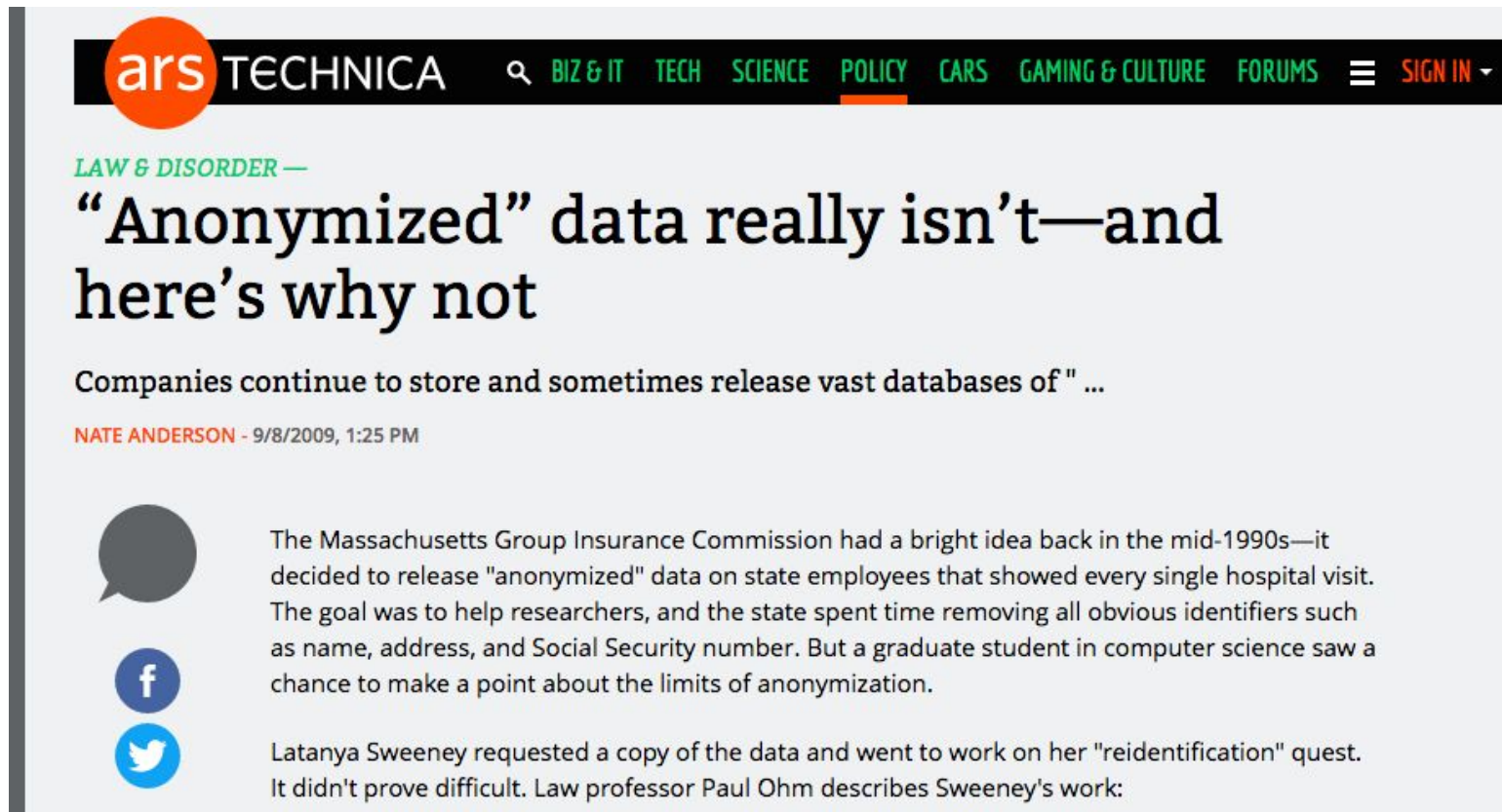 - Quantity of PII - 25 records or 25 million records?
  - Sensitivity

Impact Levels

Low	Moderate	High
limited adverse effect - cause a degradation in mission capability - result in minor damage to organizational assets - result in minor financial loss - result in minor harm to individuals.	**serious adverse effect** - cause a significant degradation in mission capability - result in significant damage to organizational assets - result in significant financial loss - result in significant harm to individuals that does not involve loss of life or serious life threatening injuries	**severe or catastrophic** - cause a severe degradation in or loss of mission capability - result in major damage to organizational assets - result in major financial loss - result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

Factors to Identify

- Identifiability
  - Direct identifiability like Social Security, AHV-numbers (Switzerland)
  - Also consider linked PII if the attached data has a high impact level
- Quantity of PII - 25 records or 25 million records?
  - Higher numbers give higher impact level
  - Don't neglect lower numbers
- Sensitivity
  - Consider data-fields in the context of other fields
    - Credit-card # alone has a low impact level, together with a name it's moderate
- Context of Use
  - What is the purpose of the collection?
  - Tel.-# and name - mailing-list: low - retirement benefits: moderate - undercover agents: high

Identifiability with Postal Codes

How to De-Anonymize

At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld **resided in Cambridge**, Massachusetts, a city of 54,000 residents and **seven ZIP codes**. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the **name**, **address**, **ZIP** code, **birth date**, and **sex** of every voter. By **combining** this data with the GIC records, Sweeney found Governor Weld with ease. Only **six people** in Cambridge shared his **birth date**, only **three of them men**, and of them, **only he lived in his ZIP code**. In a theatrical flourish, Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office.

NIST-Example: Intranet Activity Tracking

A company is logging the following information of **intra**web access:

A. The user's IP address
B. The URL and referring URL
C. The date and time the user accessed the web site
D. The web pages or topics accessed within the organization's web site (e.g., organization security policy)

Question #3 - What is Identifiable Information?

E. None of all

Linked PII

Knowing the company has a log of

- user IDs and corresponding IP addresses

Question #4

How do you evaluate the PII confidentiality impact level of this data now?
A.   Low
B.   Medium
C.   High
D.   I don't know

Question #5 - SpeakUp Discussion

Look at slide "Evaluation of a Chat-Application" and discuss what information has a moderate or high impact level and how it could be made less impacting.

Overview

- What is Personally Identifiable Information?
  - Sensitive and nonsensitive information
  - Value for third parties
- Confidentiality Impact Levels
  - Definition
  - Factors to identify
- **Management concepts**
  - Pre-collection
  - Operating phase
  - Incident response
- Legislation in CH, Europe and US

Management Concepts

- Pre-collection
  - What and why information is to be collected
- Operating phase
  - Put protective measures into place (encryption, separation)
  - De-identify or anonymize data (store age without reference for statistics)
  - Don't exchange unnecessary data (Facebook ad-services)
- Incident response
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activity

albert.io

© Can Stock Photo - csp12505550

axciom.com

Pre-Collection

- Before starting to collect the data
- Design-phase of project
- According to the service, define
  - What information is to be collected
  - Why the information is being collected
  - The intended use of the information
  - With whom the information will be shared
  - How the information will be secured
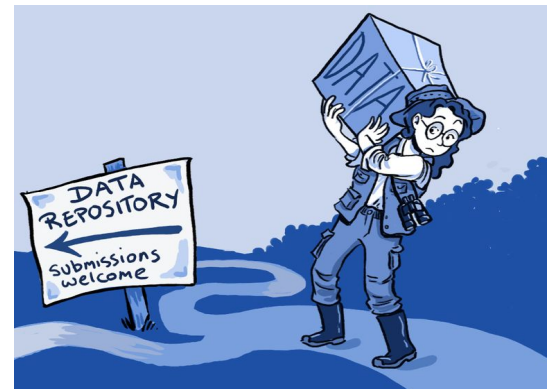
albert.io

Evaluation of a Chat-Application

What	Full name	Telephone-#	Birthday	Contacts	Credit Card
Why	Greeting, make contacts	Verify user	Verify offers	Write messages - get to know app	Additional offers
Intended use	Show	First-contact	Birthday greetings	Write to all contacts	Pay special offers
Shared with	Everybody	Friends	Everybody	Everybody	nobody
Securing with					Encrypted

Evaluation of a Chat-Application

What	Full name	Telephone-#	Birthday	Contacts	Credit Card
Why	Greeting, make contacts	Verify user	Verify offers	Write messages - get to know app	Additional offers
Intended use	Show	First-contact	Birthday greetings	Write to all contacts	Pay special offers
Shared with	Everybody	Friends	Everybody	Everybody	nobody
Securing with					

Evaluation of a Chat-Application

What	Full name	Telephone-#	Birthday	Contacts	Credit Card
Why	Greeting, make contacts	Verify user	Verify offers	Write messages - get to know app	Additional offers
Intended use	Show	First-contact	Birthday greetings	**Ask if** write to all contacts	Pay special offers
Shared with	Everybody	Friends	**Friends**	**Nobody**	nobody
Securing with		**Hashed**	**Only keep day/month**	**Delete on server**	Encrypted

Operating Phase - Protective Measures

- Encryption
  - At rest - storing data with a global encryption key
    - Where to store that key?
  - In transit - using TLS, VPN
    - Even inside data-centers
  - In Use - homomorphic crypto, mostly exotic
    - What DEDIS/LCA are working on

- Separation
  - Don't store all data in the same place
  - De-identify data and, if needed, re-identify

© Can Stock Photo - csp12505550

Operating Phase - De-Identify or Anonymize

© Can Stock Photo - csp12505550

- Generalizing the Data
  - Only store if age > 18 or not
- Suppressing the Data
  - Once the telephone-number is verified, delete it
- Introducing Noise into the Data
  - Add random noise to search results
- If only needed for statistics, you can
  - Swap the data of users
  - Only store the average

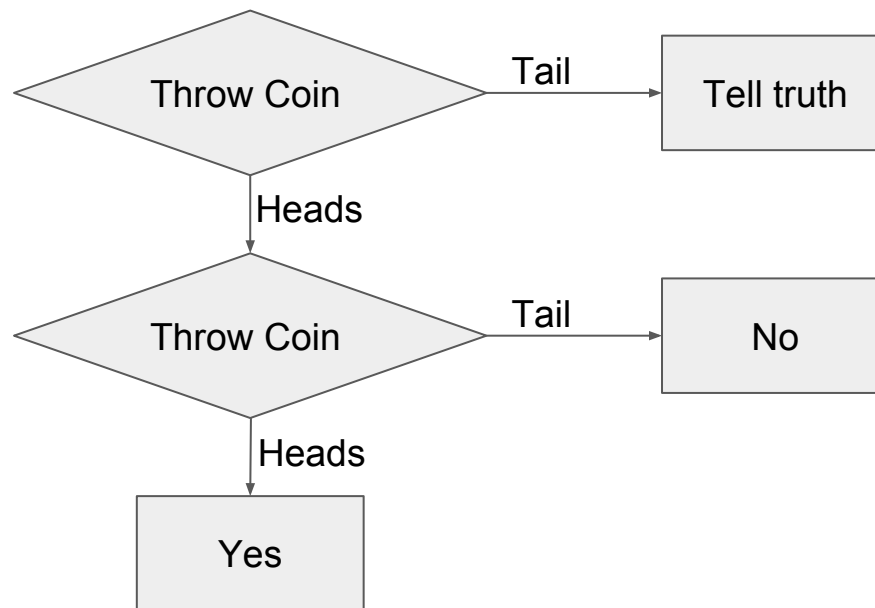# Introducing Noise in Data

ANDY GREENBERG SECURITY 06.13.16 7:02 PM

APPLE'S 'DIFFERENTIAL PRIVACY' IS ABOUT COLLECTING YOUR DATA—BUT NOT *YOUR* DATA

Senior vice president of software engineering Craig Federighi. JUSTIN KANEPS FOR WIRED

Did you ever break the law?

39

Operating Phase - Default: No Exchange

- With whom you want to exchange data
    - What data you want to exchange
    - Is it anonymized?
- Does the third party need access?
    - Google lets you define adwords, but never shows searches
    - Facebook at some time let you access user profiles
    - -> third party might only need confirmation: "sent x ads"

Leakage of data

ZDNet

CENTRAL EUROPE   MIDDLE EAST   SCANDINAVIA   AFRICA   UK   ITALY   SPAIN   MORE ▾   NEWSLETTERS   ALL WRITERS

EXCLUSIVE   MILLIONS OF RECORDS LEAKED FROM HUGE US CORPORATE DATABASE

Facebook apps have been accidentally leaking user data for years

Facebook has fixed a flaw affecting hundreds of thousands of its apps. You should still change your Facebook password though.

By Emil Protalinski for Friending Facebook | May 10, 2011 -- 15:15 GMT (16:15 BST) | Topic: Social Enterprise

http://www.zdnet.com/article/facebook-apps-have-been-accidentally-leaking-user-data-for-years/

Incident Response

- Preparation
  - How to report?
  - Who is in charge for leading? What resources are available?
  - What data can we collect to help detection? What backups are available?
- Detection and Analysis
  - Save all logs and state of servers
  - Investigate
- Containment, Eradication, and Recovery
  - Should fake data be provided?
  - Restore from backups
- Post-Incident Activity
  - What to improve for next time?

axciom.com

Preparation

axciom.com

- Regularly go through exercise
  - What are the most common attacks?
  - Who should be informed?
    - Internally - hierarchy, IT
    - Clients working with our data
    - Other customers
- For some kind of organizations, the state wants specific informations
- Have logs, lots of logs
- Make backups - **and verify them**

A Word on Backups
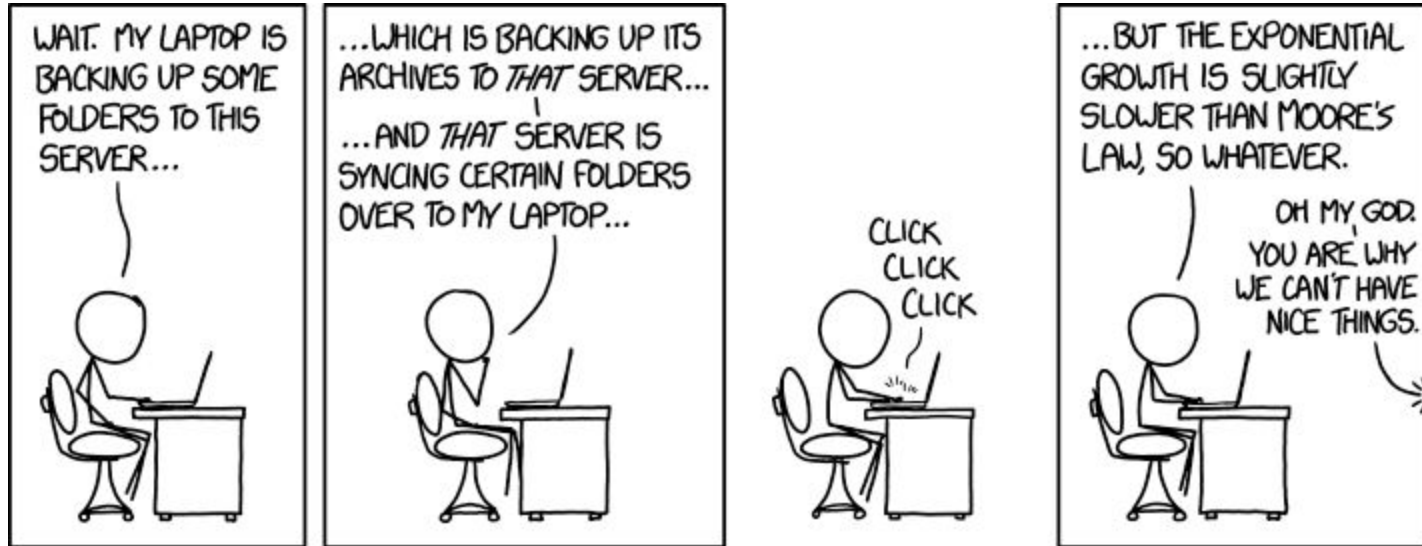
Maybe you should keep FEWER backups; it sounds like throwing away everything you've done and starting from scratch might not be the worst idea.

Detection and Analysis

- Follow prepared plan
- Make backups of all available logs and data
  - Only work on those copies
  - For virtual machines, take a snapshot
- If it's a high-value target
  - Don't show you know what's going on
  - Set up fake data
- Start investigation
  - Contact people defined in plan
  - Inform state agencies

Containment, Eradication, and Recovery

- Containment
  - If possible, remove sensible data from network
  - Should fake data be provided?
- Eradication
  - Re-install systems
  - Make sure they don't get infected again
  - Implement protection against threats discovered
- Recovery
  - Find out if those backups work
- Verification
  - No re-infection?

Post-Incident Activity

- What to improve for next time?
- Monitor better for new attack
    - Take new logs
    - Lessen attack surface
- Protect against discovered attacks
- Change data storage
    - Anonymize data
    - Don't store data

Example from RUAG incident

Timeline:

Sept. 2014
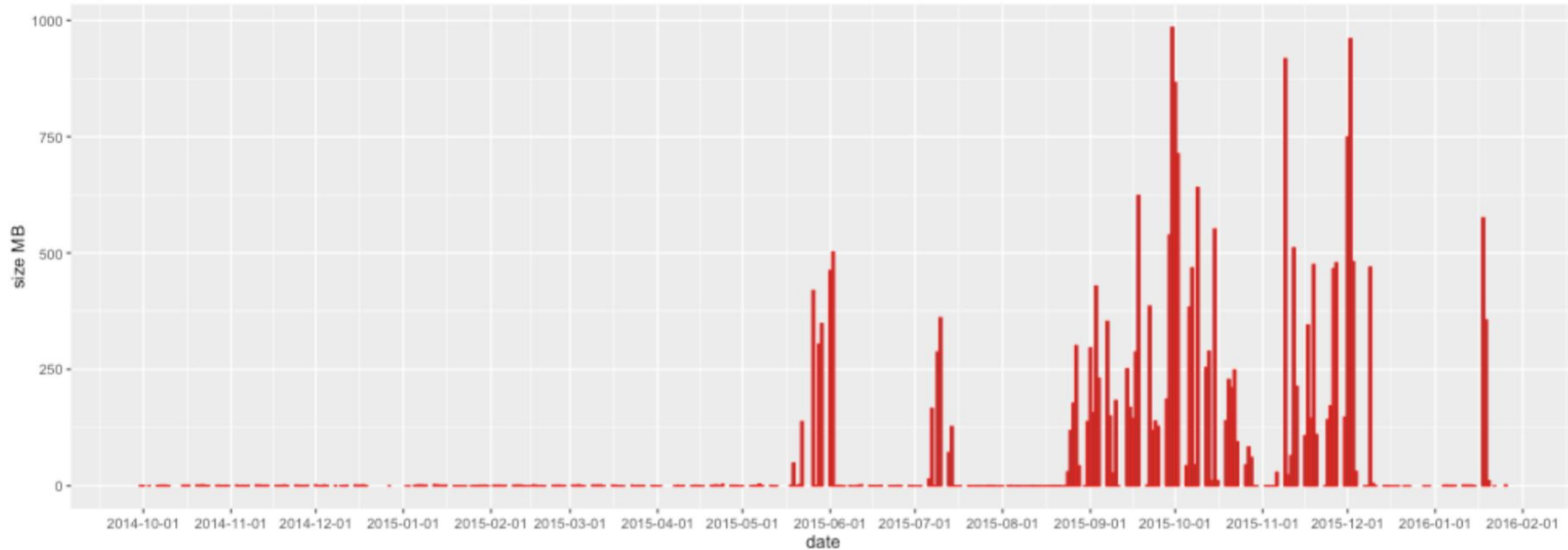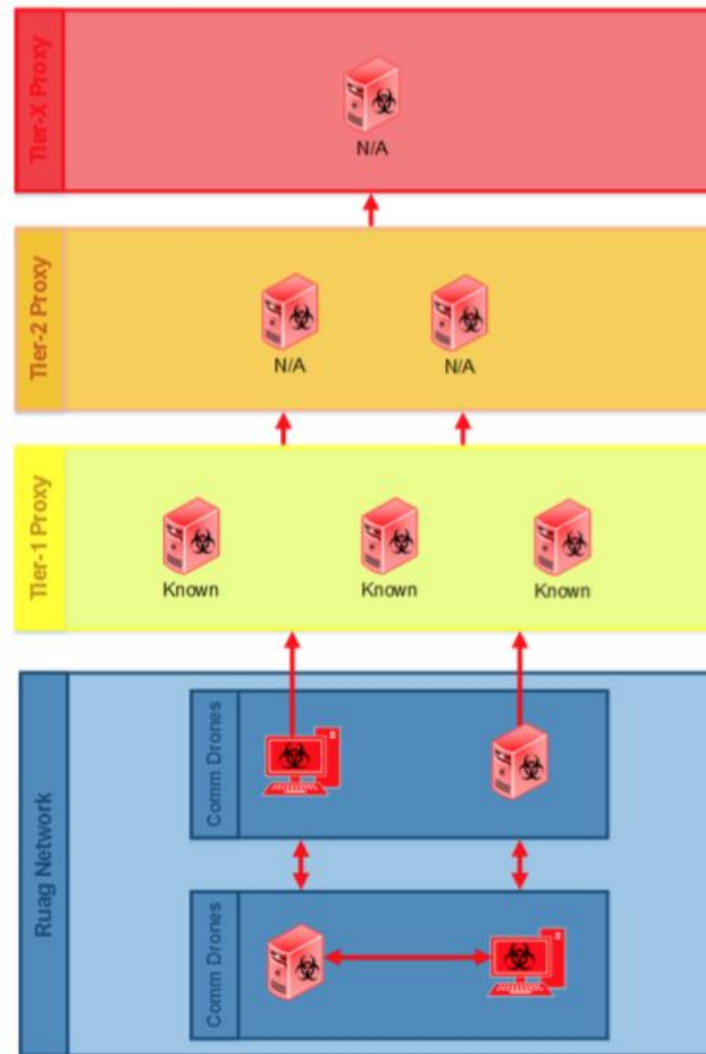IOC's already appear in Proxy-logs. Not yet detected though. No proxy logs available before this date. Initial vector still unknown

Dec. 2015
First hints (IP's) from external organisation. No in-depth search possible because proxy does not log internal client IP's

21.1.2016
- C&C servers and infected bots identified in proxy logs.
- Major incident opened by MELANI/GovCERT.ch and RUAG

22.1.-31.1.2016
- Attack goes back to Sept. 2014 were logs end, but we already see C&C traffic
- Turla/Tavdig Malware have been used.
- Hot phase of the incident response. Task-force established. Forensic analysis of logs, disks etc

1.2.-29.2.2016
- Several new C&C Servers found
- Exfiltration using HTTP over proxy in waves: June, July, Sept., Oct. and Dec. 2015
- Monitoring established

1.3-30.4.2016
Enhanced Monitoring established

3.5.2016
Several press reports about the incident. This leakage heavily damages the ongoing investigation, rendering the ongoing monitoring useless

Legend: Findings | Events, Tasks

Data Exfiltrated

Proxy Tier Topology

Question #6

What part of the preparation-phase should have been done better in RUAG?

A. Better backups
B. Listing of servers and workstations
C. Logging at the proxy
D. Traffic analysis

Overview

- What is Personally Identifiable Information?
    - Sensitive and nonsensitive information
    - Value for third parties
- Confidentiality Impact Levels
    - Definition
    - Factors to identify
- Management concepts
    - Pre-collection
    - Operating phase
    - Incident response
- **Legislation in CH, Europe and US**

IANAL/B

means

I am not a lawyer, but

by acronymsandslang.com

Legislation in CH, Europe and US

One for protection, one for openness of your and the government's data

- CH
  - The Federal Act on Data Protection, FADP
  - Freedom of Information Act, FoIA
- Europe
  - General Data Protection Regulation, GDPR
  - Data Protection Directive, DPD
- US
  - Health Insurance Portability and Accountability Act, HIPAA
  - Privacy Act of 1974 (Updated since then…)

Swiss Privacy Laws - FADP

- The Federal Act on Data Protection, FADP, applies to personal data, that is, all information relating to an identified or identifiable person, whether natural or legal
  - Bundesgesetz über den Datenschutz, DSG
  - Loi fédérale sur la protection des données, LPD
  - Legge federale sulla protezione dei dati, LPD

http://uk.practicallaw.com/9-502-5369?source=relatedcontent#
https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

Swiss Privacy Laws - FADP

- Regulated acts on data
  - Collection of data.
  - Storage of data.
  - Use of data.
  - Revision of data.
  - Disclosure of data.
  - Archiving of data.
  - Destruction of data.
- Jurisdictional scope
  - Data subject has its habitual residence in Switzerland
  - Data processor has its habitual residence or registered office in Switzerland.
  - Damage resulting from the data process is sustained in Switzerland

Swiss Privacy Laws - FoIA

- Freedom of Information Act, FoIA
  - Öffentlichkeitsgesetz, BGÖ
  - Loi sur la transparence, LTrans
  - Legge sulla trasparenza, LTras
- Governs the data the government has to publish
- Does not apply to private companies

EU Privacy

https://www.youtube.com/watch?v=5ByVaZ0rg8U&feature=youtu.be

EU General Data Protection Regulation

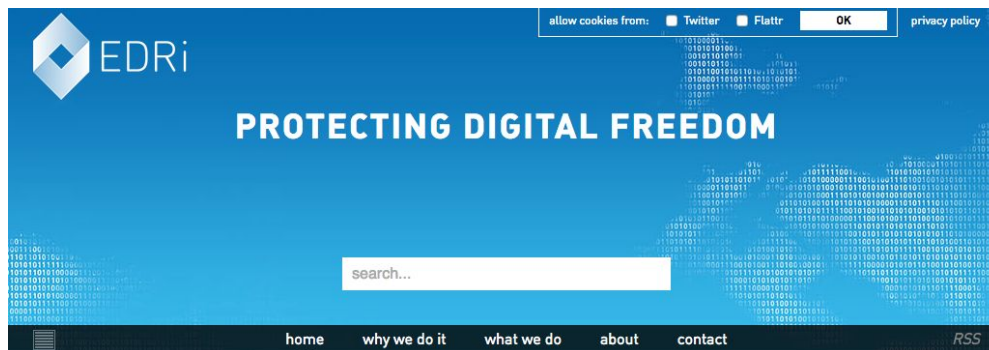https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

- Applies to you if the data controller or processor (organization) **or** the data subject (person) is based in the EU
- Responsibility and accountability
  - Algorithmic decision-making is punishable
  - Privacy by Design, setting must be "high" by default
- "Opt-in" instead of "Opt-out" for data usage
- Data breaches must be reported within 72 hours
- Right to be forgotten

EU - DPD

Data Protection Directive for the police and criminal justice sector that provides robust rules on personal data exchanges at national, European and international level

1. Notice - data subjects should be given notice when their data is being collected
2. Purpose - data should only be used for the purpose stated and not for any other purposes
3. Consent - data should not be disclosed without the data subject's consent
4. Security - collected data should be kept secure from any potential abuses
5. Disclosure - data subjects should be informed as to who is collecting their data
6. Access - data subjects should be allowed to access their data and make corrections to any inaccurate data
7. Accountability - data subjects should have a method available to them to hold data collectors accountable for not following the above principles

EU - Freedom Act?

US Privacy Laws

Not **1**, but **many** privacy laws

Finance	Health	Education	Communication
GLBA	HIPAA	FERPA	ECPA

https://www.teachprivacy.com/problems-sectoral-approach-privacy-law/
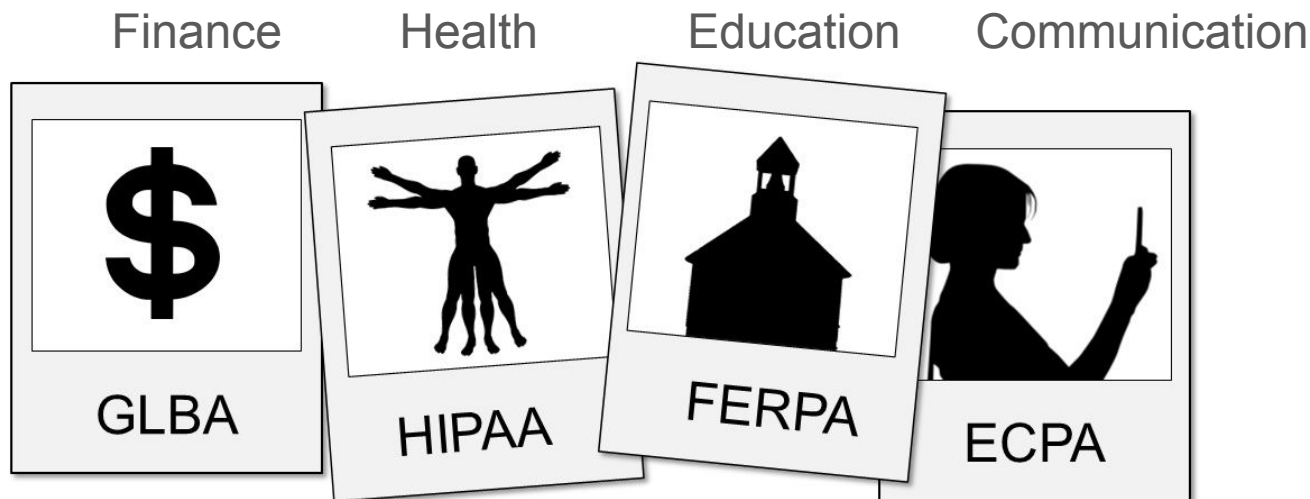
US - HIPAA

- Health Insurance Portability and Accountability Act - regulates medical information.
- Applies to
  - health care providers
  - data processors
  - pharmacies
  - other entities that come into contact with medical information.
- Governs collection and use of protected health information (PHI).
- HIPAA Security Rule provides standards for protecting medical data.
- HIPAA Transactions Rule applies to the electronic transmission of medical data.

US - Wall of Shame

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome   File a Breach | HHS | Office for Civil Rights | Contact

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

	Name of Covered Entity ⬍	State ⬍	Covered Entity Type ⬍	Individuals Affected ⬍	Breach Submission Date ⬍	Type of Breach	Location of Breached Information
⊙	Anthem, Inc. Affiliated Covered Entity	IN	Health Plan	78800000	03/13/2015	Hacking/IT Incident	Network Server
⊙	Premera Blue Cross	WA	Health Plan	11000000	03/17/2015	Hacking/IT Incident	Network Server
⊙	Excellus Health Plan, Inc.	NY	Health Plan	10000000	09/09/2015	Hacking/IT Incident	Network Server
⊙	University of California, Los Angeles Health	CA	Healthcare Provider	4500000	07/17/2015	Hacking/IT Incident	Network Server
⊙	Medical Informatics Engineering	IN	Business Associate	3900000	07/23/2015	Hacking/IT Incident	Electronic Medical Record, Network Server
⊙	Banner Health	AZ	Healthcare Provider	3620000	08/03/2016	Hacking/IT Incident	Network Server, Other
⊙	Newkirk Products, Inc.	NY	Business Associate	3466120	08/09/2016	Hacking/IT Incident	Network Server

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

64

US - Privacy Act of 1974

- [Wikipedia](#):
  - *It establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.*
  - Each agency that maintains a system of records shall
    - upon request by any individual ... permit him ... to review the record and have a copy made of all or any portion thereof in a form comprehensible to him …
    - permit the individual to request amendment of a record pertaining to him ...[2]

US - Freedom of Information Act

- Scope
  - The act explicitly applies only to executive branch government agencies.
- Nine exceptions
  - State secrets for national security
  - Trade secrets
  - Invasion of privacy
- Wikipedia:
  - The Center for Effective Government (now superseded by POGO) analyzed 15 federal agencies which receive the most FOIA requests in-depth. It concluded, that federal agencies are struggling to implement public disclosure rules.

Legislation in CH, Europe and US - Links

- CH
  - Federal Act on Data Protection
  - Freedom of Information Act
- Europe
  - http://ec.europa.eu/justice/data-protection/index_en.htm
  - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
  - https://www.access-info.org/
- US
  - https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
  - https://en.wikipedia.org/wiki/Privacy_Act_of_1974
  - https://en.wikipedia.org/wiki/Freedom_of_Information_Act_(United_States)
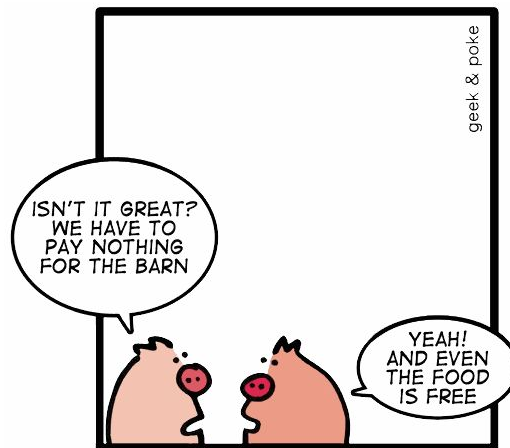 - http://pogo.org - Project on Government oversight

Conclusion

For Users

- Take care where you leave a trail
- PII is not where you think it is
- Remove data / only enter required data
- if you're not paying for the product, you are the product

For Organizations

- PII can pop up in unexpected places
- If you don't collect data, it cannot be stolen
- Prepare for failure - it will happen
- Be aware of PII-requirements in your country

geek & poke

ISN'T IT GREAT?
WE HAVE TO
PAY NOTHING
FOR THE BARN

YEAH!
AND EVEN
THE FOOD
IS FREE

A Summary of Your Online Privacy

YouTube	Facebook	Twitter	LinkedIn	Google+	Pinterest	MySpace
We know everything including that time in Cancun when you flashed the DJ. Niiiice!	We know everything & if you don't think we're gonna sell it you are a dumb fuck	We know everything but frankly most of it is worthless rambling crap	We know everything including the exagerrated background you came up with.	We know everything about all 14 of you.	We know everything but had no idea we'd become a desitnation for cat pictures	We used to know alot but then you left. Please come back. Pretty please.
Foursquare	Quora	Apple	CIA	WikiLeaks	Anonymous	Mom
We know everything but no one gives a shit where you are anymore	We know everything but surprisingly you never ask any questions about it.	We know everything but you are are so blinded by our awesomeness you don't care	It's none of you bee wax what we know. Just move along.	Don't worry about the CIA, we'll tell you.	We know everything but we are mainly here to fuck with Corporate America	I gave birth to you for crissakes & I'll tell the ladies at bridge everything if I want to. Call me.