Cyber Security and Privacy
MS6880

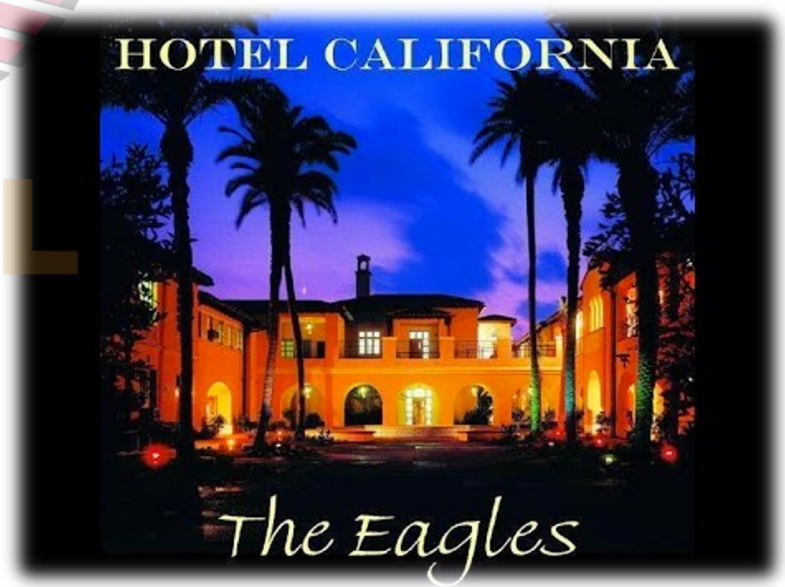
Regulation for Privacy

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

The Web (https://www.youtube.com/watch?v=UehilhnMt5Y)

- Welcome to the Hotel California
  Such a lovely place (Such a lovely place)
  Such a lovely face
  They livin' it up at the Hotel California
  What a nice surprise (what a nice surprise)
  Bring your alibis

  Last thing I remember, I was
  Running for the door
  I had to find the passage back
  To the place I was before
  "Relax, " said the night man,
  "We are programmed to receive.
  You can check-out any time you like,
  But you can never leave! "



"I like the privacy, but it does make it hard to see."

"Shaadi"

- "With respect to Content you submit or make available for inclusion on publicly accessible areas of the Site including but not limited to your contact details, you hereby unconditionally and irrevocably grant to Shaadi.com the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such Content on the Site and to Shaadi.com Centre members from time to time."

- By posting Content to any public area of Shaadi.com, you automatically grant, and you represent and warrant that you have the right to grant, to Shaadi.com, and other Shaadi.com Members, an irrevocable, perpetual, non-exclusive, fully-paid, worldwide license to use, copy, perform, display, and distribute such information and content and to prepare derivative works of, or incorporate into other works, such information and content, and to grant and authorize sublicenses of the foregoing.

Policy fine print

- It takes 76 working days to read and understand a typical privacy policy (Luca & Bazerman, 2021)
- Field experiments generally do not require consent as it leads to demand effect
  - If you are in social media, you are an uninformed participant in several behavioral experiments

But,

- Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves (Posner, 1978)

- However, despite the complaints, it appears that consumers freely provide personal data. … the "privacy paradox" or the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors (Norberg et al., 2007)

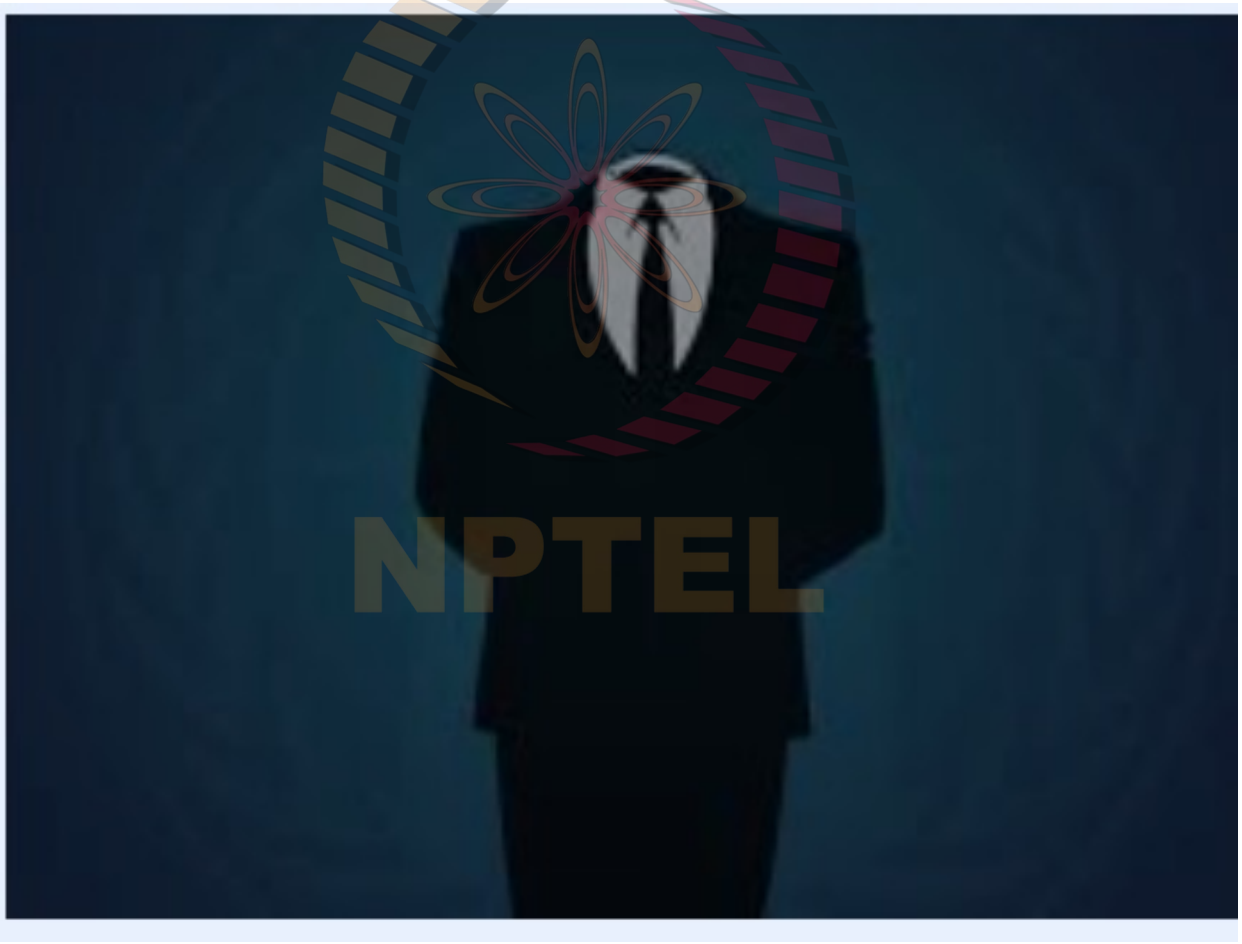
Personal experience and privacy

- Co-creation of value: the imperatives
  - Personalization
  - Personally identifiable data
- Give identity, get privileges
- Orwell's surveillance society vs small town life

"Yes we have a right to privacy. But in this society we can't have a right to anonymity"

-Derek Smith, CEO, ChoicePoint

Right to anonymity?



Personal data

- Personal data is any information that relates to an *identified or identifiable living individual*.
- Personal data that has been de-identified, encrypted or *pseudonymised* but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Examples of personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;

Related words

- *Anonymity*: Anonymity is the ability to conceal a person's identity. individuals can choose to be totally anonymous, pseudonymous, or identifiable.
- *Secrecy*: Secrecy has been defined as intentional concealment of information. Privacy need not hide; and secrecy hides far more than what is private
- *Confidentiality*: Concerns the externalization of restricted but accurate information to a specific entity. British law embraces privacy as confidentiality
- *Security*: protection of personal information with three specific goals-integrity, authentication and confidentiality.

Amount of Personal Information Externalized

High

Low

1

ANONYMITY

Sharing of personal information while concealing a consumer's real identity.

4

TRANSPARENCY

Disclose large amount of personal information

Reveal an accurate representation of the self

2

SECRECY

Sharing of little and potentially inaccurate information

Avoid digital representations of the real self

3

CONFIDENTIALITY

Externalization of restricted but highly accurate information

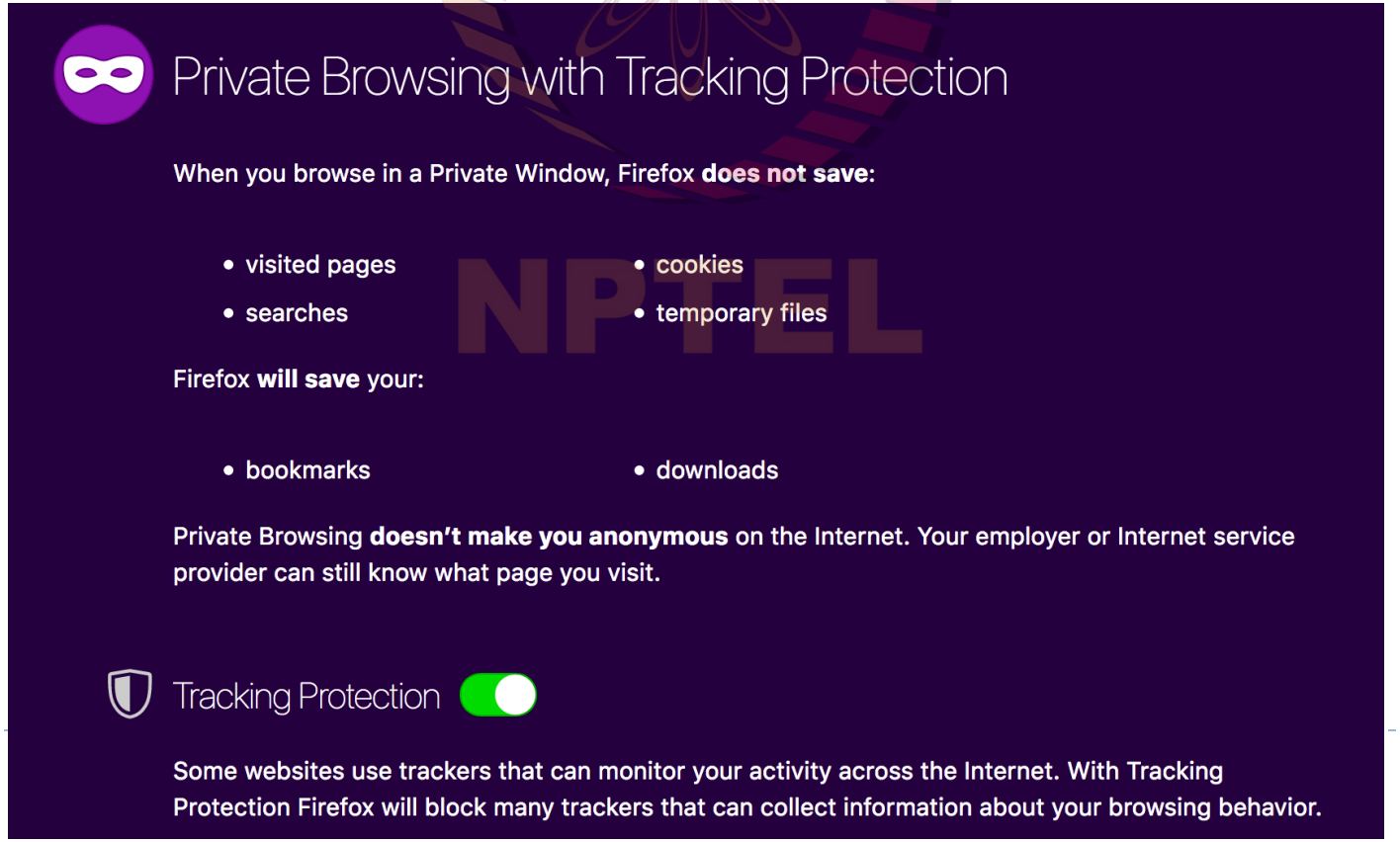
Low

Accuracy of Personal Information

High

Anonymity

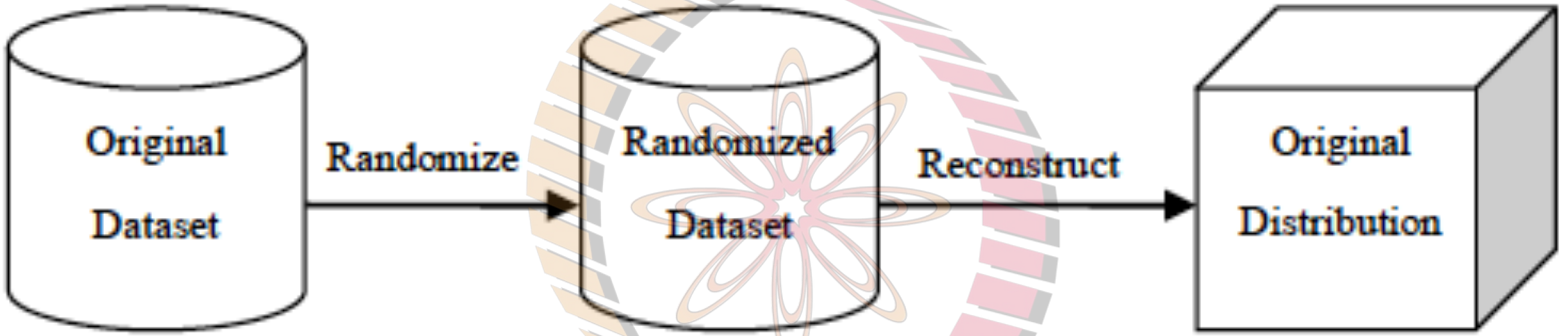
- Anonymity is the ability to conceal a person's identity
- Central for the information collected for statistical purposes, and use of IT



Privacy preserving data mining

- Anonymity exists when someone is acting in a way that limits the availability of identifiers to others
  - totally anonymous, pseudonymous*, or identifiable
- The goal of privacy preserving data mining is to develop data mining methods without increasing the risk of misuse of the data
  - Randomization
  - Anonymization
  - Encryption

Randomization



- Data providers randomize their data and transmit the randomized data to the data receiver
- The data receiver estimates the original distribution of the data by employing a distribution reconstruction algorithm
- If x_i is the value of a sensitive attribute, $x_i + e_i$, rather than x_i , will appear in the database, where e_i is a random noise drawn from some distribution

Anonymization

- k-anonymity model widely used (Sweeney, 2002)

Definition 2.2 (k-anonymity requirement) *Each release of data must be such that every combination of values of quasi-identifiers can be indistinctly matched to at least k individuals.*

- Uses suppression and generalization

Suppressed

Generalized

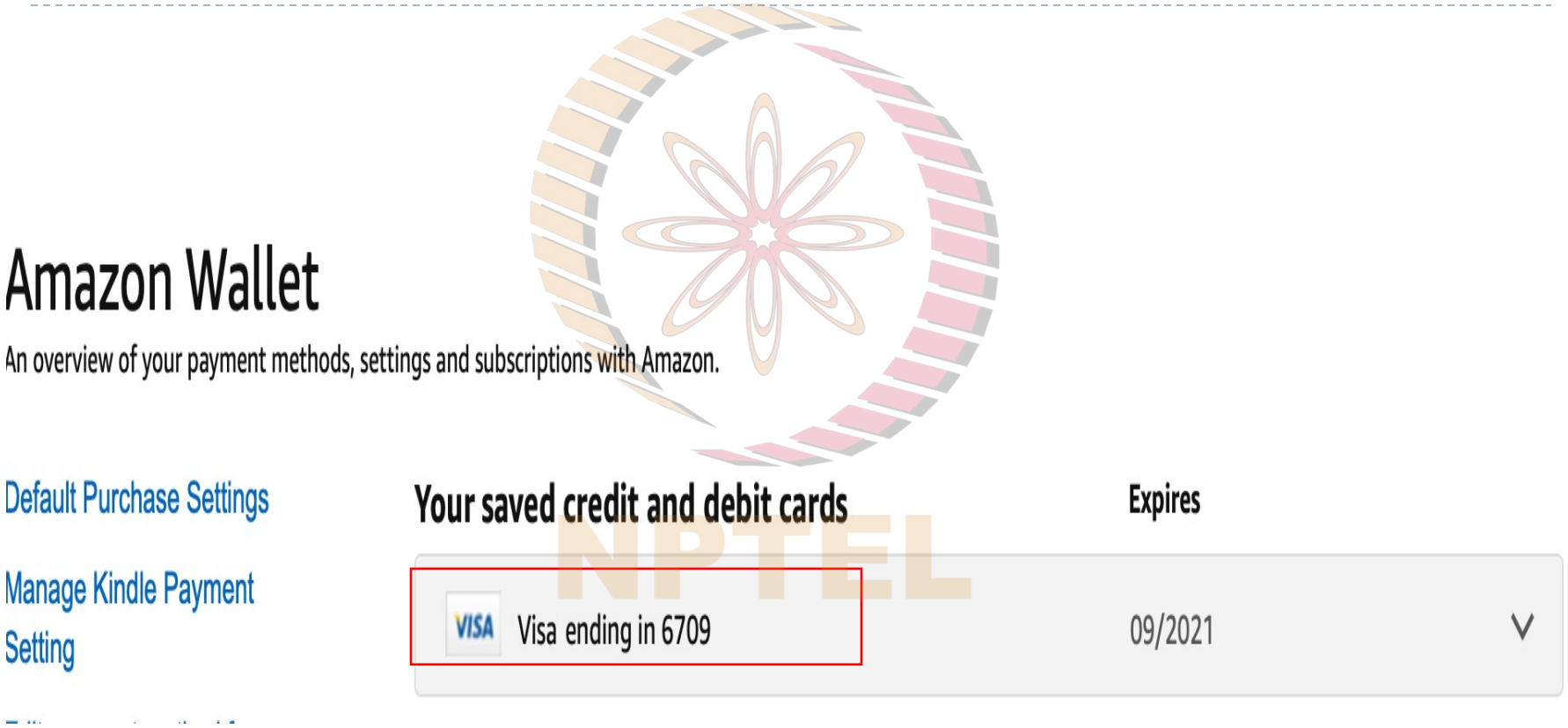
Table 1. Original table

Name	Race	Birth	Sex	Zip	Disease
Alice	Blank	1965-3-18	M	02141	Flu
Bob	Blank	1965-5-1	M	02142	Cancer
David	Blank	1966-6-10	M	02135	Obesity
Helen	Blank	1966-7-15	M	02137	Gastritis
Jane	White	1968-3-20	F	02139	HIV
Paul	White	1968-4-1	F	02138	Cancer

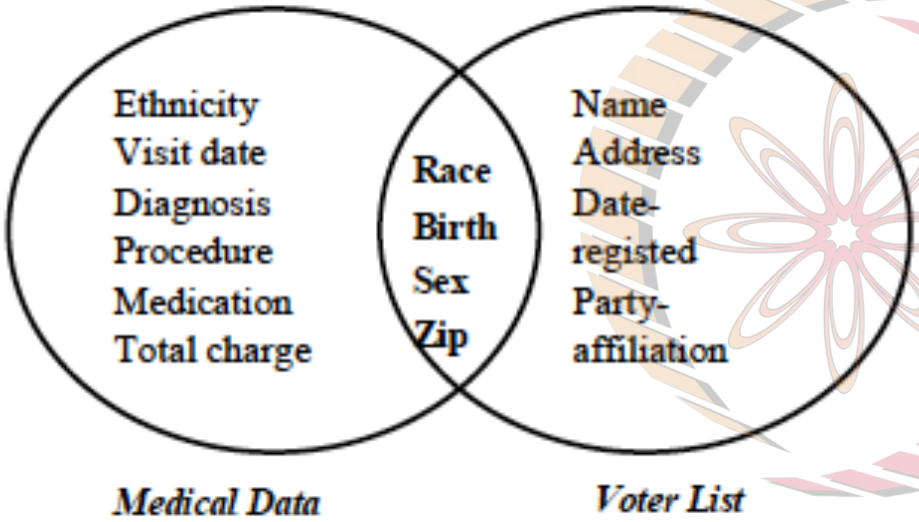
Table 2. Anonymization of table 1

Race	Birth	Sex	Zip	Disease
Blank	1965	M	0214*	Flu
Blank	1965	M	0214*	Cancer
Blank	1966	M	0213*	Obesity
Blank	1966	M	0213*	Gastritis
White	1968	F	0213*	HIV
White	1968	F	0213*	Cancer

Generalization or suppression?



Limitations



Compromising Privacy with Trail Re-Identification:

The REIDIT Algorithms

Bradley Malin

December 2002

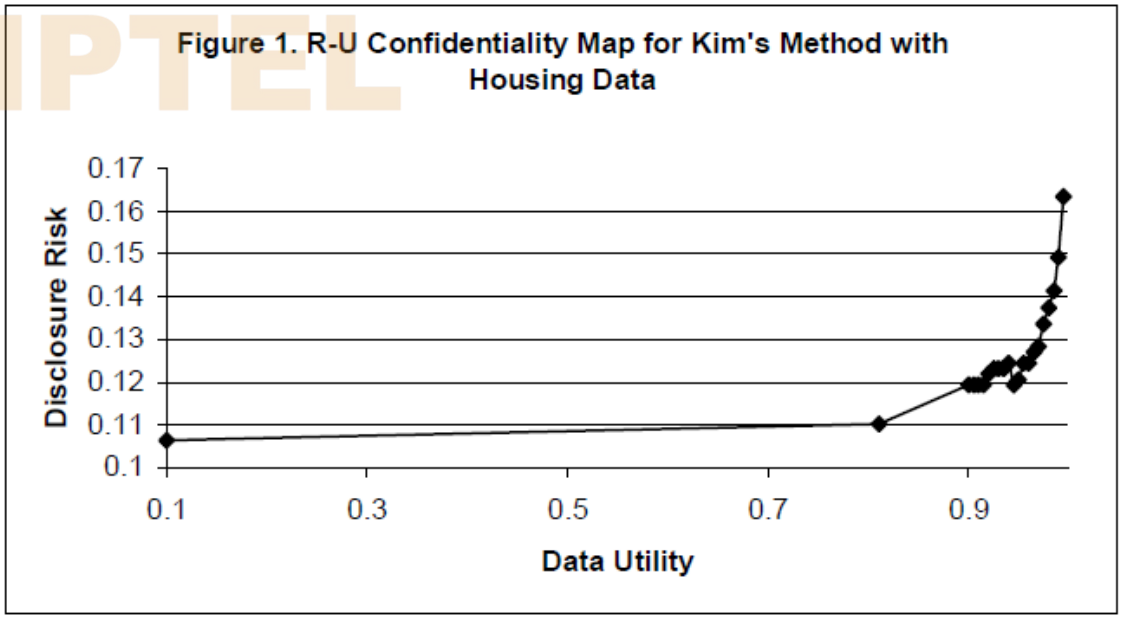
CMU-CALD-02-108

- Problem: Linking multiple sources to profile individuals/entities
- Utility of results

Risk vs. utility of data (R-U maps)

- An individual is concerned about one's privacy (Westin, 1967)
  - Personal freedom, autonomy, control, risk
- Business needs personal information for efficiency (Posner, 1981)
  - Employer needs to select the right employee
  - Relevant products to the right customer
- R-U map shows the trade off

(Duncan et al., 2001)



Regulatory frameworks

- FIPP as the foundation (1973)
  - OECD Guidelines (1980)
    - 8 guidelines, including collection and accountability, transparency
    - Defines data subject, data controller, data processor
    - Safeguards cross boarder data transfer
  - EU Data Protection Directive (1995)→GDPR (2018)
    - Accountability
  - FTC privacy principles (1998)
    - 5 points of (i)notice/awareness, (ii)choice/consent, (iii)access/participation, (iv)integrity/security, (v)enforcement/redress
    - Collection not addressed
  - APEC privacy framework
  - Similar to OECD guidelines

DATA BREACH AT EQUIFAX

GROUP 2

Group Members:

- K LOKESH - MS21A029
- SANJANA ANAND - MS21A058
- K S SUBISHA - MS21D026

ABOUT EQUIFAX

- **Founded in:** 1899
- **Business:** Credit Reporting Company
- **Location:** United States
- **Mission:** Responsible for collecting and providing information on income and creditworthiness to organizations and individuals.
- **Company's slogan:** "Powering the world with knowledge"
- **Gross Margin:** Collects consumer and business credit information from banks, analyzes it using proprietary processes and sells the credit analysis giving a **gross of 90%**
- **Customers:** 820 million and 91 million businesses around the world.

BUSINESS SEGMENTS

USIS (U.S Information Services)

- Online information services, mortgage services, mortgage solutions and financial marketing services
- Revenue through sale of consumer and commercial credit reports and scores

Workforce Solutions segment

- Customer data sold to organizations looking for individual employment and income history
- Business services for handling unemployment claims, employment based tax credits, etc.

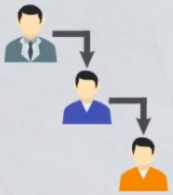
Global Consumer Solutions Segment

- Providing credit monitoring and identity theft protection products in the US, Canada and UK

CYBER SECURITY AT EQUIFAX

- Millions invested in Cyber Security measures
- Over 1% of operating revenue spent on cyber security each year between 2014-2017

- Cyber Security expert brought in as the CSO (Chief security officer)
- Who works to modernize Equifax's cyber defenses, rehearsing possible breaches
- Creating 24 hours crisis management squads



Chains of Commands

Legal/Security Group

- The CLO (Chief Legal officer) supervises the CSO (Chief security officer)
- Security group - 180-190 employees
- They define the "WHAT"
- Security engineering function by providing the ability to configure the software

Technology Group

- Headed by CIO (Chief Information Officer)
- Reported directly to the CEO
- Responsible for deploying the technology that the security team wants in the infrastructure.

Teams

GTVM

- The Global Threat and Vulnerability Management team
- Tracks threats to the security of the IT systems and notify relevant personnel across the company.

VAT

- Vulnerability Assessment Team
- Ran regular scans of IT systems for vulnerabilities

Countermeasures

- Deployed code designed to obstruct the exploitation of ongoing vulnerabilities

SECURITY ISSUES AND VULNERABILITIES:

2013-14 Hackers accessed credit report data from Equifax

2015 – Technical error caused software modifications publicly exposed consumer information

2016 – Exposed salary and tax data of 431000 employees at Equifax

-- Independent researcher warned about consumer information left exposed accessible to anyone, but Equifax didn't act on it till 2017

2017 – Equifax workforce solutions being exploited and employee tax documents were being downloaded on Equifax clients

-- Security vulnerability exposed by attackers, failed to fix on time

RECOMMENDATIONS BY CYBER SECURITY FIRMS:

- Mandiant(cybersecurity firm) warned Equifax of its unpatched systems and misconfigured security policies could indicate various problems - unpatched and misconfigured systems
- Hired deloitte to conduct security audit in 2016– identified several issues
- 2017 – Cyence (Cyber security firm) quantified the probability of equitax encountering a breach in the coming year to be 50%.

- FICO (Fair Isaac Corp) had analyzed corporate cyber risk for insurance for Equifax to be 550 out of 300-850 – websites run by Equifax had expired certificates, errors in chain of certificates or other web security issues.
- Bigsight technologies – gave Equifax an F grade (worst) for application security and D for software patching
- MSCI's ESG research team gave Equifax zero for privacy and data security–overall lowest rating of CCC

APACHE STRUTS VULNERABILITY

- **WHEN AND WHAT?** ➡ March 2017-There was a vulnerability in the Apache struts, an open source software used to build java applications and it was accessible through 2 publicly available exploits.

- **HOW SEVERE** ➡ After exploit, attackers can add their own code to web pages, disable firewalls and install malware with their IP address masked to prevent tracing, scan for servers running

PATCHING THE VULNERABILITY

- CERT (US Dept of homeland security) alerts vulnerable parties including Equifax's GVTM which instructed the patch to be implemented within 48 hours
- Most of senior Equifax members didn't attend GVTM meetings
- counter measures team at Equifax due to technical issues took delayed steps to defend attacks

TIMELINE OF EQUIFAX DATA BREACH - A

March 8

Cisco systems and the U.S. DHS CERT alert potentially vulnerable parties, including Equifax, of the Apache Struts vulnerability

March 9

Equifax shares the alert internally, but fails to patch the vulnerability on its systems

March 11

An "entry crew" first breaches Equifax's systems. A more sophisticated team comes into set up over 30 entry points to Equifax

March 15

Equifax's follow-up scan does not identify that the vulnerability is unpatched

May 13

Hackers first begin collecting PII

July 29-30

Equifax's security team first notices network traffic from the hackers and shuts down the app used by the hackers

July 31

Smith is informed by the Chief Information Officer (CIO)

August 2

Equifax retains Mandiant, contacts its law firm and the FBI

August 11

The investigation first discovers that hackers had been able to access numerous systems

August 22

Smith Notifies lead director Mark Feidler

August 24-25

The full board is notified by telephone

September 1

The board meets to discuss the scale of the breach and Equifax's response

TIMELINE OF EQUIFAX DATA BREACH - B

September 4

Equifax finalizes the initial list of 143 million consumers affected

September 7

Equifax publicly announces the breach

September 11

The New York attorney general launches the first of many investigation into the breach

September 15

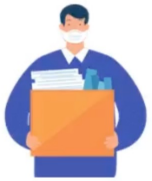
Equifax's CSO and CIO both resign

September 18

First public reports that Equifax was breached in March

September 26

Smith resigns as CEO



October 2

Equifax confirms that an additional 2.5 million had their data stolen

October 3-4

Smith testifies before several U.S. government committees

October 10

Equifax announces that 10 million in total had driver's license data stolen, 700,000 UK customers affected

October 12

The IRS suspends a contract with Equifax following backlash

THE BREACH

Created over 30 backdoors using web shells registered to unique internet address - Increasing difficulty of finding

SSL certificated needs to be renewed between every 12 to 39 months - Expired across the network

ACIS reactivated, Blocked the IP address, which caused traffic from china - ACIS Portal offline, shutdown for 11 days

Webb (CIO), did not make clear that PII had been breached

Equifax and Mandiant investigation - Hackers accessed data table containing large amount of Consumer PII

Information Stolen - Names, Social security numbers, birthdates, addresses, email ID, driver's license numbers, credit card number, passport number, tax identification information and credit card dispute documents

May 13 Hackers started collecting PII

July 29 Updated 74 Secure Socket Layers (SSL)

Aug 17 Detailed briefing in Senior leadership meeting

Sep 04 143 million people affected

SOURCES OF VULNERABILITY INSIDE EQUIFAX

Internal Controls and the Patch Management Process

- Roles and responsibilities in Patch management policy were "ambiguous"
- 2015 Audit - 8500 unpatched vulnerabilities, unresolved till 2017
- Lack of comprehensive inventory of IT assets, Payne and security personnel were unware that ACIS ran Apache Struts
- 2015, Patching was reactive rather than proactive, lead to lag in the installation of critical patches, no verification
- Reasons for weakness
  - Technology systems were not well integrated-difficult in updating
  - Antiquated systems- update themselves- Operational risk
  - did not have personnel necessary to implement the technologies and process to meet internal security goals

"Accountability Gap" in the Organizational Structure

- 2005, reporting structure CSO-CIO-CEO interpersonal conflict
- IT and Security were siloed, inconsistent and ineffective communication
- Payne testified key vulnerabilities implicated in data breach, but not resolved in time to fend off Apache struts hacks
- Monthly meetings and senior leadership meetings failed - "Clear lines of accountability for developing IT security policies and executing the policies
- Security concerns were presented by CLO, had no experience or training in information security

Technological Barriers to Effective Oversight

- Failed to identify and address potentially malicious activity on servers, ACIS 1970s
- ACIS system lacked file Integrity Monitoring(FIM) process - Scan for unauthorization, suspicious alteration in IT systems and configurations
- Web servers retained log files for 30 days, NIST recommends for at least 3 months, detected targeted attack after 98 days (avg)
- Did not have process for ensuring SSL certificated were up-to-date throughout the organization
- Jan 2017, internal audit addressed the concerns of SSLV devices missing certificates, but the problem went unaddressed - 324 expired SSL certificates, 79 in critical business domain

BREACH ANNOUNCEMENT AND RESPONSE

PR ANNOUNCEMENT:

- Sep 7, 2017 – announced the data breach publicly- 143mn American's data exposed
- website to help customers determine if they were attacked by the breach
- engaged Mandiant to assess the risk

IMPACT ON STOCK PRICES:

- Fell from a high of 143$ to 93$ in a week
- decline of 35 pc

OTHER IMPACT:

- 10mn driver licence data stolen
- 7 Lakh UK customers details breach
- passport details also compromised but MOTIVE not found

STEPS TAKEN:

- Credit file monitoring
- Equifax credit lock
- Identity theft insurance
- SSN 'dark web' scanning for one year
- these were free for one year provided they agreed to controversial clause which caused uproar

MISSTEPS TAKEN

- Controversial clause
- charging customer for credit freezes
- identity theft protection only for an year
- breach time announced was mid may but reports detailed it as march
- Equifax's twitter directed consumers to fake website

BOARD OF DIRECTORS

Board

- 11 member board with 9.3 year avg tenure
- Equifax was the only credit reporting agency with separate technology committee

Technology Committee

- 5 Members
- It reviewed company's technology investments and infrastructure associated with risk management, including policies relating to information security disaster recovery and business continuity

Equifax's board of Directors

- 2006 Robert D Daleo
- 2007 Walter W Driver Jr
- 2007 Mark L Feidler
- 2016 G Thomas Hough
- 1992 L Phillip Humann
- 2013 Robert D Marcus
- 2006 Siri S Marshall
- 2008 John A McKinley
- 2005 Richard F Smith
- 2017 Elane B Stock
- 2008 Mark B Templeton

Members of the technology committee

FALLOUT

Steep decline in stock price

Loss of jobs - CSO, CIO, CEO and Chairman

Considering clawing back of compensation from the two employees

New director - McGregor, who has extensive data security experience

Lawsuits and government inquiries - Formal investigation by different parties

Freedom from Equifax Exploitation Act - Enhancing fraud alert procedures & providing free access to credit freezes

Change to Win (CtW) Investment Group

An investment advisor and shareholder activism group affiliated with Ctw

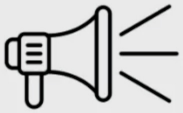
Provided 6 proposals to Equifax:

- Improve governance & hold executives accountable
- Removal of chairman of the audit & technology committees
- Permanently separating the CEO and Chairman positions
- Considering legal settlements in determining executive compensation

CtW threatened to withdraw support the reelection of directors if they failed to implement the proposal

DISCLOSURE

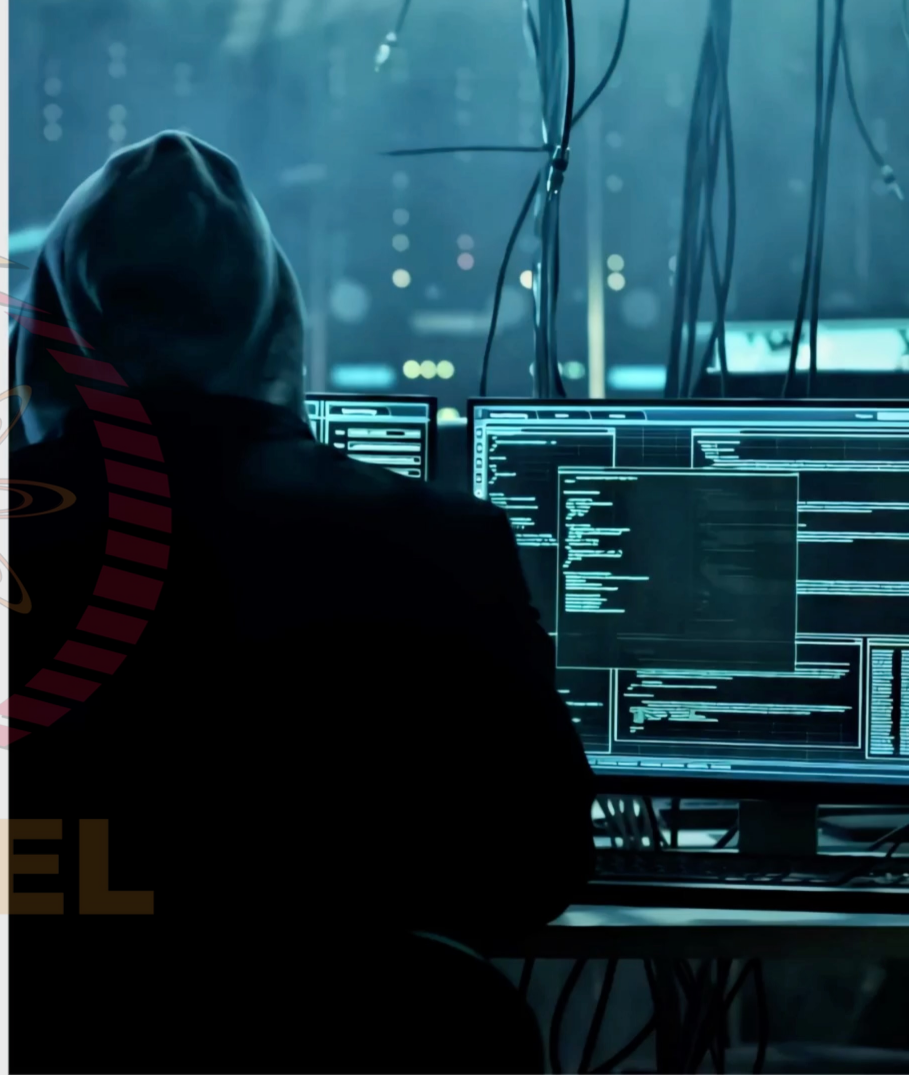
Longstanding criticisms of data breach disclosure laws.



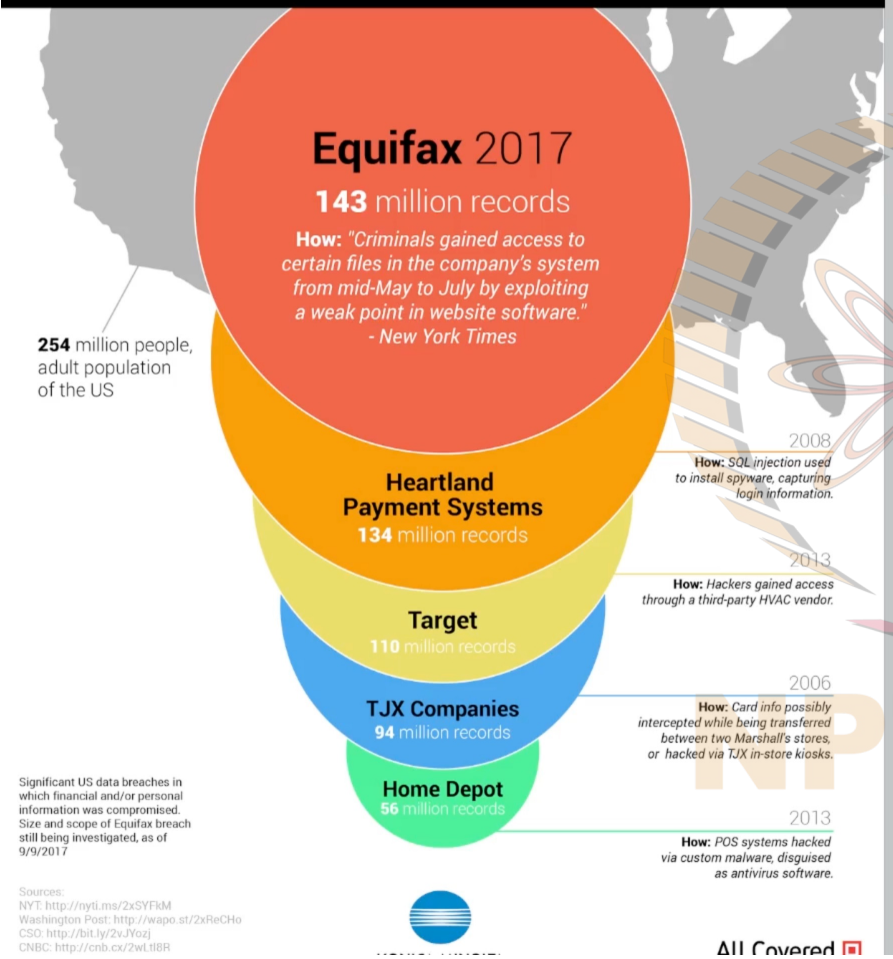
6 weeks between discovery and disclosure of breach.

Proposal of bills that would create a unified 30- day timeframe for alerting consumers.

Holding Equifax to stricter disclosure requirements - Alerting breach within 72 hours to state regulators



How **BIG** is the **Equifax Hack?**



CONCLUSION & TAKEAWAYS

- Profits fell by 27 pc year on year
- 90mn$ breach related costs
- 240 customer lawsuits
- Separate investigations by FTC, CFPB, SEC, British and Canadian regulators

Was Equifax Alone?

- 2017- 3785 Corporate victims of cyber attack in the US
- Cisco found 55% of the surveyed corporate had a data breach in 2017
- Large cap corporations lost 498mn$ in market capitalization for major cyber attack on average

Was Equifax negligent or just unlucky?