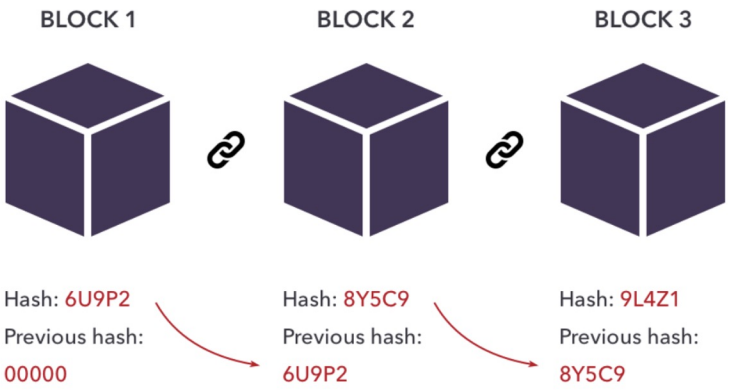
Block chains

- Ensures confidentiality through encryption and integrity through hashing
- Hash functions are mathematical algorithms that generate message summary/digest (hash value) to confirm message identity and confirm no content has changed
- Properties such as hiding, collision resistance helps block chains make transactions permanent
- Implemented as linked lists



Standards of Encryption

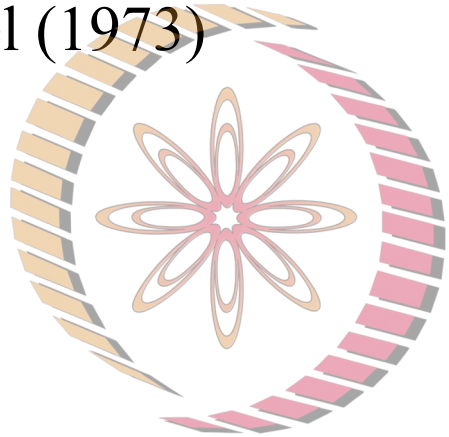
- Data Encryption Standard (DES) was developed in 1977 by IBM and is based on the Data Encryption Algorithm (DEA), which uses a 64-bit block size and a 56-bit key
- DES is a federally approved standard for non-classified data; it was cracked in 1997 when the developers of a new algorithm, Rivest-Shamir-Aldeman, offered a $10,000 reward for the first person or team to crack the algorithm
  - Fourteen thousand users collaborated over the Internet to finally break the encryption
- Triple DES (3DES) was developed as an improvement to DES and uses three keys in succession
- Advanced Encryption Standard (AES) developed with a key length of either 128, 192, or 256 bits (NIST/ISO)
- RSA standard developed based on the difficulty of figuring the prime factors of a large number

Power of the keys

Key length (bits)	Maximum Number of Operations (guesses)	Maximum Time to Crack	Estimated Average Time to Crack
8	256	0.0000000085 seconds	0.0000000043 seconds
16	65,636	0.0000022 seconds	0.00000109 seconds
24	16,777,216	0.00056 seconds	0.00028 seconds
32	4,294,967,296	0.143 seconds	0.072 seconds
56	72,057,594,037,927,900	27.800 days	13.9 days
64	18,446,744,073,709,600,000	19.498 years	9.7 years
128	3.40282E+38	359,676,102,360,201, 000,000 years	179,838,051,180,100, 000,000 years
256	1.15792E+77	122,391,435,436,027, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	61,195,717,718,013,400, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years
512	1.3408E+154	14,171,960,013,891,600, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	7,085,980,006,945,820, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years

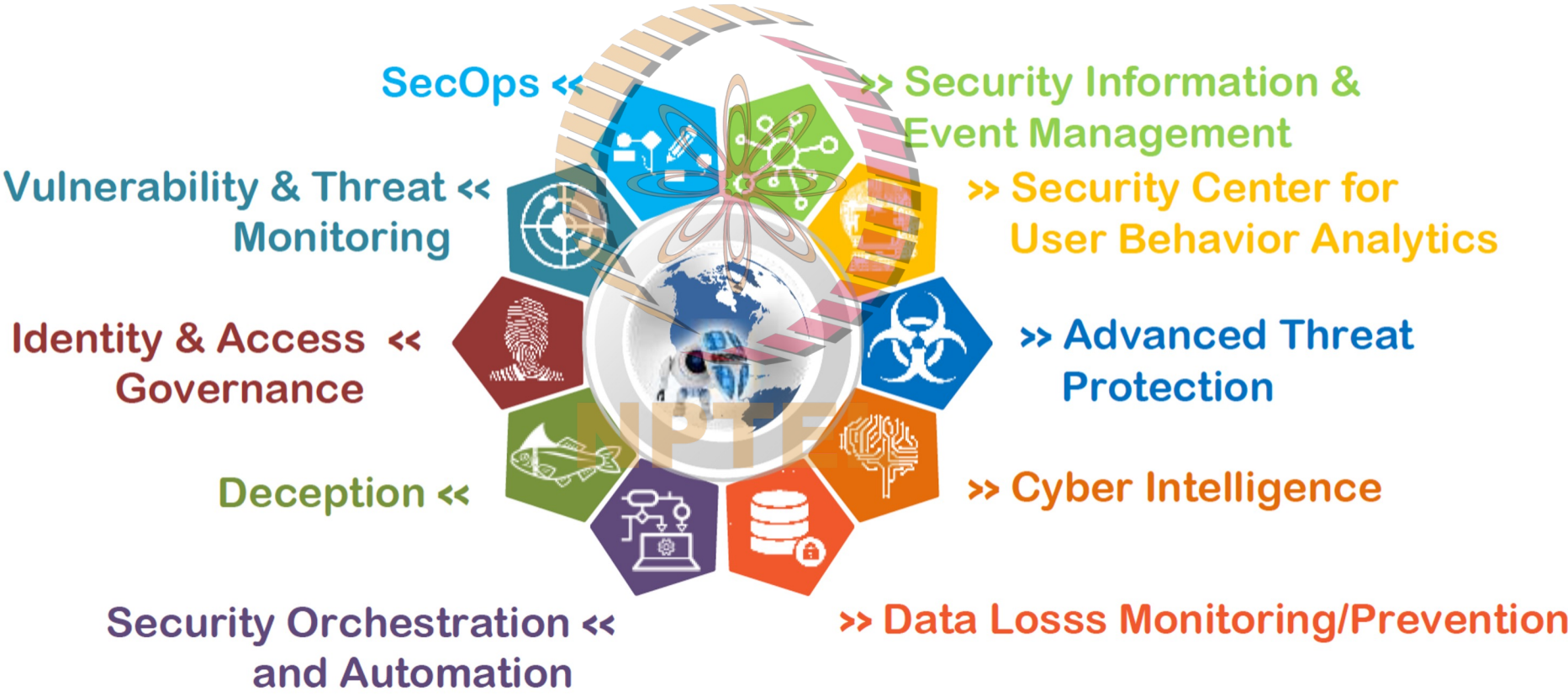
Security Models

- Bell-LaPadula Model (1973)
  - Read down, write up
  - Confidentiality focus
- Biba Model (1977)
  - Read up, write down
  - Integrity focus
- Clark-Wilson Model (1987)
  - Constrained data item (CDI), transformation procedures
  - Useful for commercial applications
- Chinese Wall Model (1989)
  - Resolves conflict of interest

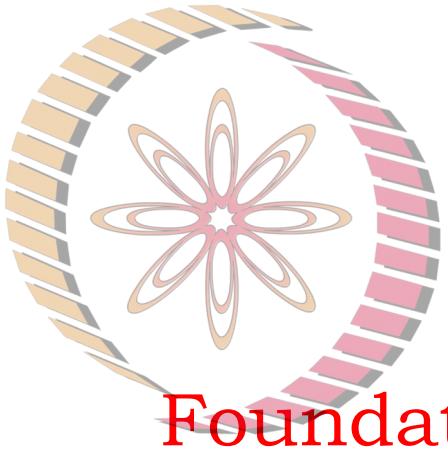


- Confidentiality
- Integrity
- Availability

Integrated cyber defense



Cyber Security and Privacy
MS6880



Foundations of privacy

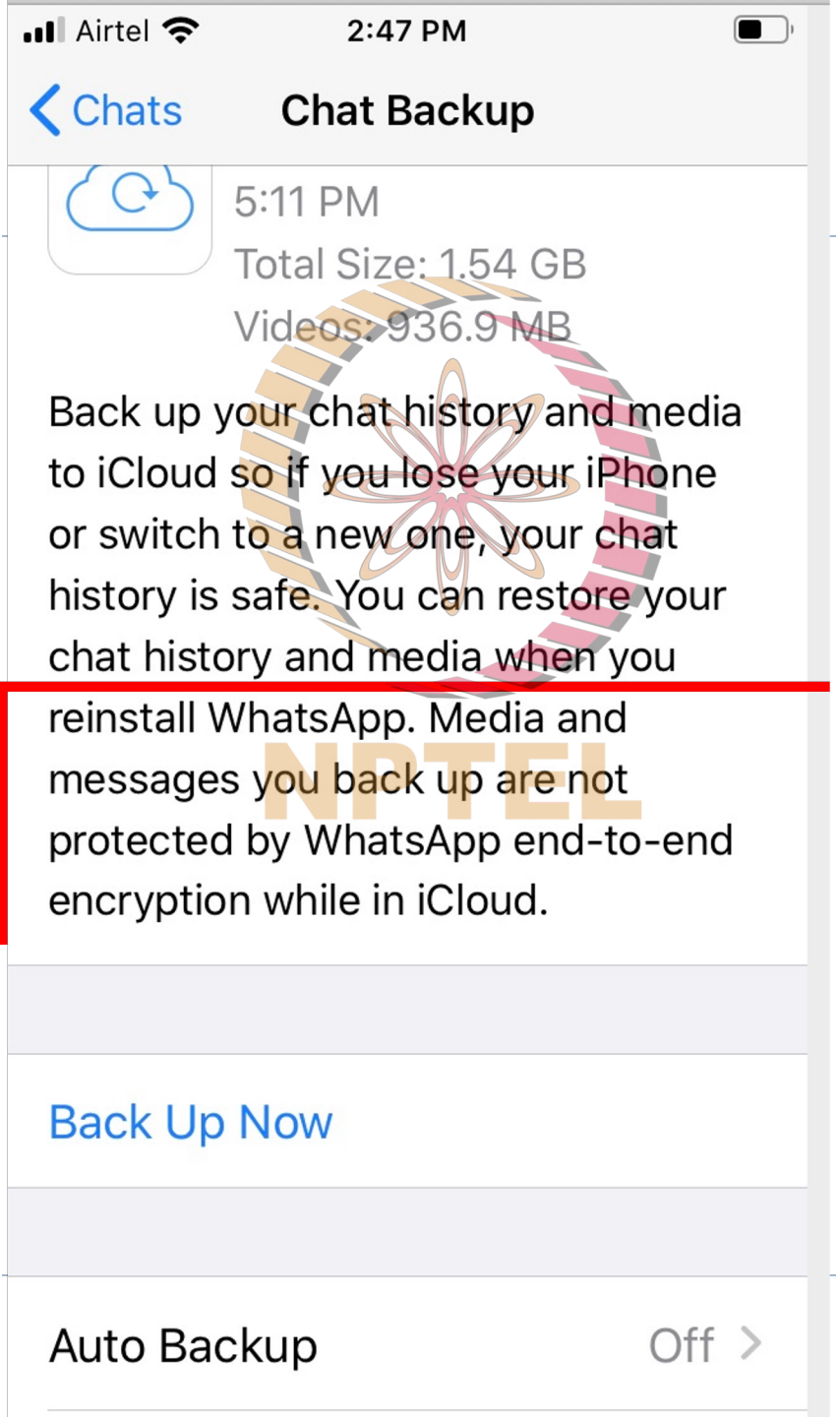
Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

Encrypted chats vulnerable?

The context

- The Narcotics Control Bureau's (NCB) probe into the drugs case in connection with actor Sushant Singh Rajput's death case has led to news channels reporting WhatsApp chats reportedly between actor Rhea Chakraborty and others and also part of a group chat from 2017, allegedly between Deepika Padukone and her manager Karishma.
- How was end-to-end* encrypted WhatsApp chats read by a third party?
- How can private chat messages be displayed in public?
- Privacy???

- Even whatsapp cannot read the encrypted message: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf


Airtel
2:47 PM
Chats
Chat Backup
5:11 PM
Total Size: 1.54 GB
Videos: 936.9 MB
Back up your chat history and media to iCloud so if you lose your iPhone or switch to a new one, your chat history is safe. You can restore your chat history and media when you reinstall WhatsApp. Media and messages you back up are not protected by WhatsApp end-to-end encryption while in iCloud.
Back Up Now
Auto Backup
Off

The caveat

- Did the Govt obtain consent for this? If privacy is a fundamental right can the state leak information that it obtained as part of an investigation to the public?
- Can the press be silent if a government source comes to the press with *information that is in the public interest?*
- Privacy vs public interest

A political party while in power will stress on "national security" and while in opposition will advocate "privacy rights"

The big brother

In India, 10 central probe and snoop agencies are empowered under the Information Technology (IT) Act to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. This list of ten includes the Narcotics Control Bureau, Enforcement Directorate and the Central Bureau of Investigation as well.

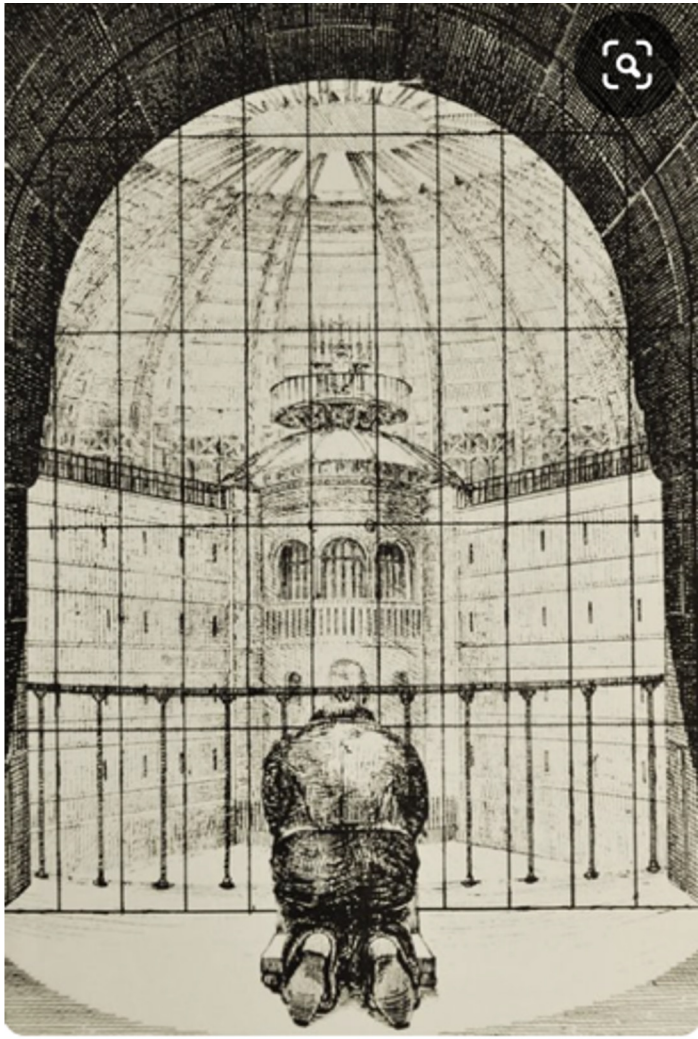
- Indian Telegraph Act 1885

Panopticon (being observed, while the subject doesn't know)

- Surveillance nation
  - Michael Foucault, George Orwell

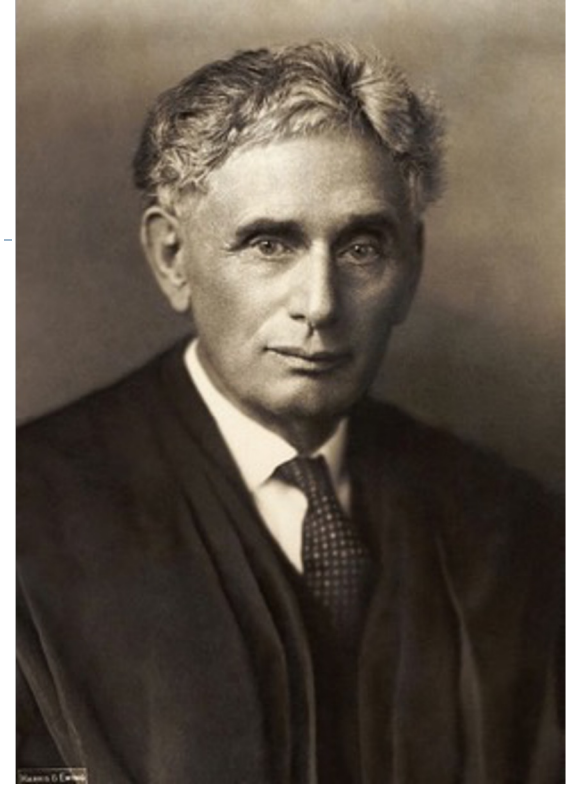
The panopticon must not be understood as a dream building. It is the diagram of a mechanism of power reduced to its ideal form

  - Michael Foucault, Discipline and punish, 1977



Privacy a created issue?

The right to be let alone



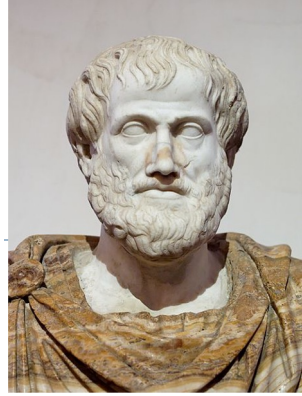
- The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle (The right to privacy, *Harvard Law Review*, Samuel Warren and Louis Brandies, 1890)

Like a freedom movement

- *Privacy as freedom*- the earliest notion of privacy
- Privacy as *autonomy*, privacy as the *right to be let alone* (Warren and Brandeis, 1890)
- Early understanding of privacy based on moral principles

The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement (William Pitt, 1763 cited in Hosein, 2004)

Public and private



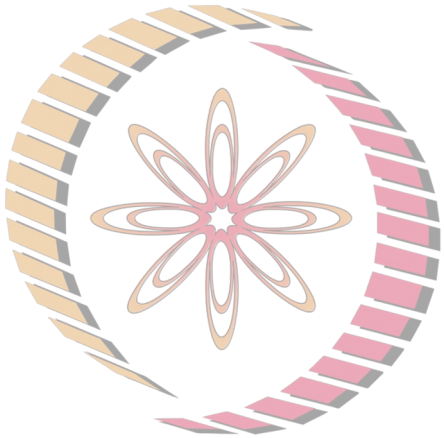
- Aristotle: *poilis* (public) and *oikos* (private)
- Aristotle distinguished between the public sphere of politics and political activity, *the polis*, and the private or domestic sphere of the family, *the oikos*, as two distinct spheres of life

Reductionism vs Coherentism

- Privacy as a derivative of fundamental rights like property rights, bodily security, right to freedom etc. (Thomson,1975)
- There is nothing called privacy!
- Cohenretism treats privacy as a distinct right

Economic view

- Privacy is not important so long as there is no economic consequence (Posner, 1975)
- If privacy affects economic value of information, it must be protected (eg. access to reco letter by applicants)
- Privacy could reduce economic efficiency


NPTEL

Feminist view

- Potential misuse in favor of dominant gender (MacKinnon,1989)

Privacy and control over information

- "*the claim of individuals, groups or institutions to determine for themselves when, how and to what extend information about them is communicated to others*"

  -Westin 1967, Privacy and Freedom

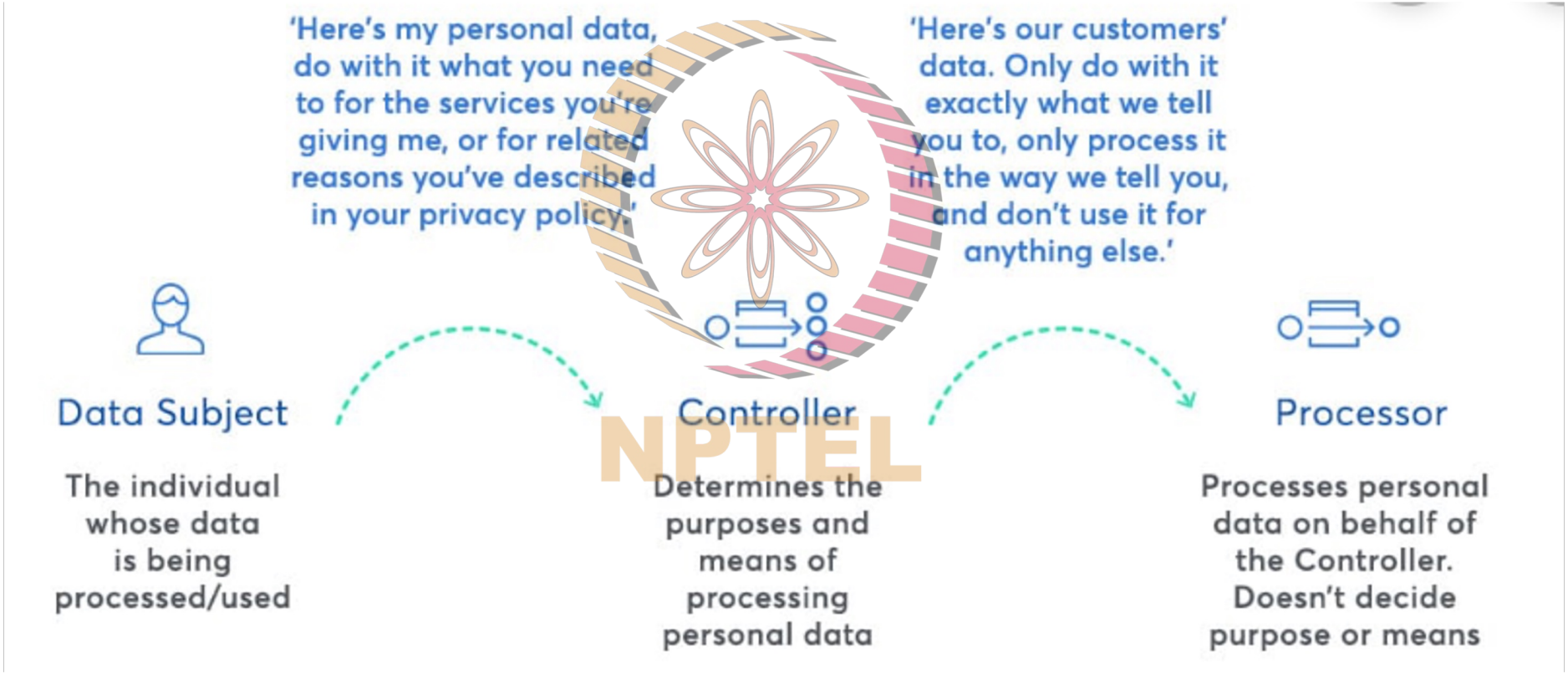
- Privacy as exclusive (restricted) access
- Privacy vs information privacy

Fair Information Practice Principles

- *US Secretary's Advisory Committee on Automated Personal Data Systems* in a 1973 report, *Records, Computers and the Rights of Citizens*

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of *identifiable personal data* must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data

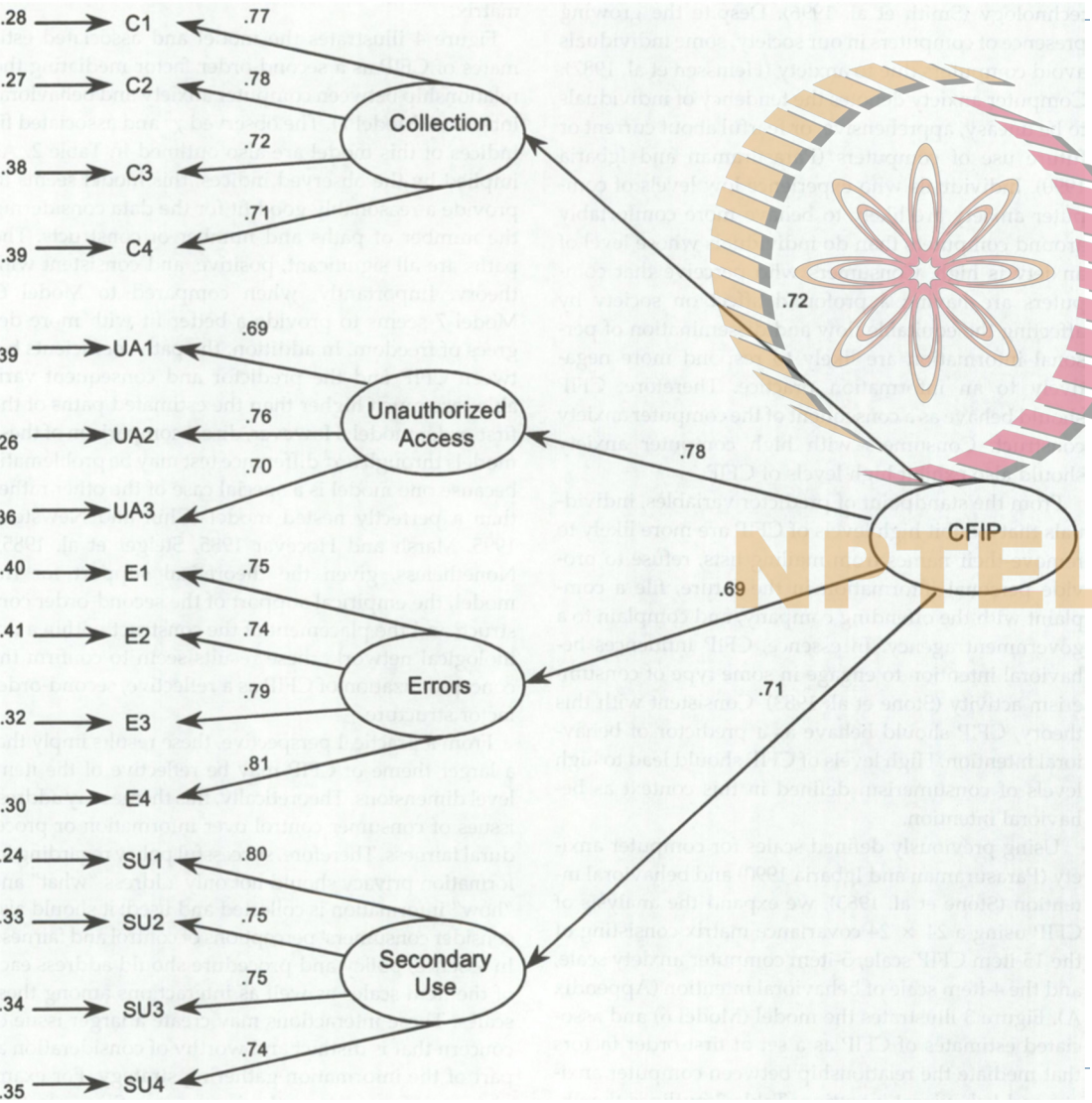
Stakeholders



"Data principal" "Data fiduciary" "Data processor"

Synonyms used in India's PDP in red

Concern For Information Privacy
(Smith et al., 1996)



Collection

C1 It usually bothers me when companies ask me for personal information.

C2 When companies ask me for personal information, I sometimes think twice before providing it.

C3 It bothers me to give personal information to so many people.

C4 I am concerned that companies are collecting too much personal information about me.

Unauthorized Access

UA1 Companies should devote more time and effort to preventing unauthorized access to personal information.

UA2 Companies should take more steps to make sure that the personal information in their files is accurate.

UA3 Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Errors

E1 All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.

E2 Companies should take more steps to make sure that the personal information in their files is accurate.

E3 Companies should have better procedures to correct errors in personal information.

E4 Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Secondary Use

SU1 Companies should not use personal information for any purposes unless it has been authorized by the individuals who provided the information.

SU2 When people give personal information to a company for some reason, the company should never use the information for any other purpose.

SU3 Companies should never sell the personal information in their computer databases to other companies.

SU4 Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Evolution of information privacy
(Westin, 2003)

Period	Important events – Characteristics
Privacy Baseline (1945-1960)	Limited IT developments, high public trust in government and business sector, and general comfort with the information collection.
1st Era of Privacy (1961-1979)	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964). Fair Information Practice
2nd Era of Privacy (1980-1989)	Rise of computer and network systems, database capabilities. European nations move to national data protection laws for private and public sectors.
3rd Era of Privacy (1990-2002)	Rise of the Internet, Web 2.0, terrorist attack of 9/11 dramatically changed the landscape of information exchange. Privacy concerns rose to new highs.

2005 Onwards - Social media, cloud computing, big data, location based services are the dominant drivers for new privacy concerns and research

Why organizations should worry?

Since January 2005 (In US)

- 857 million records with sensitive personal information exposed
- 4,586 data breaches

Lawsuits against popular websites like Facebook Beacon, Google Buzz for violation of online privacy

- ChoicePoint ~ $30 million fine
  - Fraudulent access of 145,000 consumer reports
- TJX Companies ~ $156 million fine
  - Unfair practices that resulted in compromise of 46.2 million credit cards data

International Significance

- 70 out of 400 grants given by National Science Foundation (USA), related to privacy.

Why individuals should worry?

- A super market faced with a lawsuit from one of its customers, who had slipped and fallen, threatened to use the fact that the customer was a frequent purchaser of alcohol, to damage his reputation in the court

-Simson Garfinkel (2000), Database Nation

Simson Garfinkel

Computer scientist

Simson L. Garfinkel is the US Census Bureau's Senior Computer Scientist for Confidentiality and Data Access. Previously, he was a computer scientist at the National Institute of Standards and Technology and, prior to that, an associate professor at the Naval Postgraduate School in Monterey, California. Wikipedia

Born: 12 July 1965 (age 54 years), United States

h-index: 46

Parents: Marian Garfinkel

Education: Columbia University, The Shipley School, Massachusetts Institute of Technology

The best thing about being over 50?

We did all our stupid stuff
before the invention of the internet,
so there's no proof!

Class work

- What should the Hathway Jones do: hire/not hire
  - Give rationale (three bullets)
- What should they do post decision? (three bullets)

We Googled You

Harvard Business Review

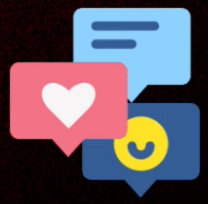
PREPARED BY :

- ANNA CATHERIN - MS21A004
- NITHISH KANNA - MS21A042
- SHRIRAAM SAHADEVAN - MS21A062

Privacy is power.
What people don't know,
they can't ruin.

As the saying goes, the first impression is everything, but with internet and social media screenings, more impressions can be assumed of a candidate

Hiring Decision-Makers



71 % Say looking at social media profiles is an effective way to screen canadiates

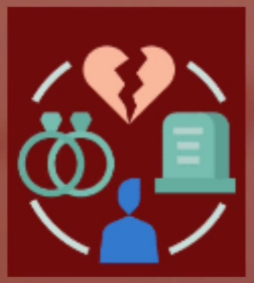
55 % Have found content that caused them not to hire the applicant

Source: Harris Poll commissioned by Express Employment Professionals

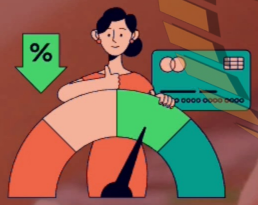
A study conducted by Rahman et al. (2020) found that social media is cost-effective and less time-consuming tool during the hiring process affecting company efficiency, productivity, and speed in recruiting.

INVASIVE BACKGROUND CHECKS

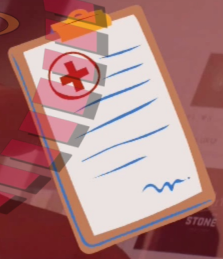
TOO MUCH OF ANYTHING MIGHT BE BAD



Relationship Status



Credit score and financial history



Medical history

Race ethnicity

HATHAWAY JONES

Luxury apparel retailer

Current Situation

- Declining sales
- Changing tastes of customers
  - younger people wanted more affordable clothing with flair
  - Brand was seen as old , clothes as expensive and stodgy

The Chinese Dream

The company wanted to enter and be succesful in China to improve revenues.

China

- luxury market growth 70% yoy
- huge aspirational middle-class , Chuppies - insatiable demand for luxury goods

CHARACTERS

Fred Westen
CEO

- Experienced in working with Luxury brands
- Is betting on Chinese market to turnaroudn the company
- Prefers to have the most qualified people on his team
- doesn't care much about procedures

Virginia Flanders
VP-HR

- Lifer at the company, member of the old guard
- Not part of Fred's inner circle
- Has problems with Fred for ignoring internal talent and downplaying HR
- Very methodical and diligent
- Analytical

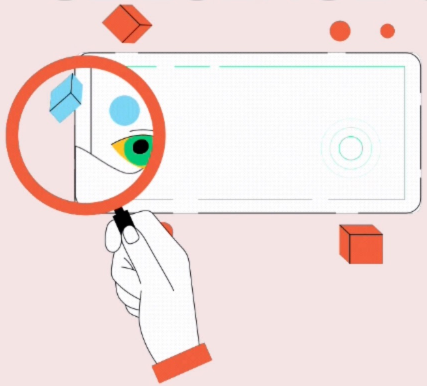
Mimi Brewster
The Canditate

- Talented
- Has good credentials and skills
- Ambitious and driven
- Expat from China and fluent in Chinese
- Good leadership capabilites and streak of activist tendencies

SEQUENCE OF EVENTS

- Fred Westen has planned to enter the Chinese market by opening 3 stores in Beijing , Guangzhou and Shanghai
- He is assembling a winning team for this and in search of a talented manger.
- His friend requests Fred give a job to his daughter Mimi Brewster.
- First impression - Fred agrees to interview her and is very impressed by her credentials and believes he has found the the right person to lead the team.

SEQUENCE OF EVENTS



- Page 9 - Virginia (VP-HR) runs a Google search for her name and comes with some issues on page 9 of the search results - where Mimi is shown to have had led a protest march against WTO and in another incident protests against the Chinese for the death of a dissident journalist.

- She brings this to the notice of Fred. He acknowledges that the if we search deep enough we can get dirt on any person including himself. But realises that he better call Mimi for another interview to explain herself.

- Virginia points oiut that Google seatrching might not be entirely legal and asks for lawyers to be present and to figure the legalities.

Questions to Ponder

- Whether the company was right to dig deep on the Internet to scan Mimi ? Is it a violation of her privacy ?
- Should Mimi be hired? Why (or) why not ?

Possible Business Impact

- Fred aims to target China's luxury goods market, which was growing 70% a year
- Possibility of targeted attack on company by using Mimi's past activities might affect their image and reputation
- Cost of undoing the damage would be very high
- Candidates might sue employers under civil law that protects employees from prejudice on the basis of discrimination, racism, idealogies and favoritism during the recruitment process

Questions to Ponder

- Whether the company was right to dig deep on the Internet to scan Mimi ? Is it a violation of her privacy ?
- Should Mimi be hired? Why (or) why not ?

Whether the company was right to dig deep on the Internet to scan Mimi ? Is it a violation of her privacy ?

Virginia's Words :

" We are still studying the legal and privacy implications of Internet searching practices in an attempt to define an appropriate position for the company. It's a bit risky letting her know that we're considering not hiring her because we Googled her "

Well drafted Background screening and Internet profile screening policy that comply with :

- Data Protection and Regulations
- Individual's Privacy Rights
- Local Privacy Laws

Whether the company was right to dig deep on the Internet to scan Mimi ? Is it a violation of her privacy ?

- **Well drafted Background screening and Internet profile screening policy that comply with :**
  - Data Protection and Regulations
  - Individual's Privacy Rights
  - Local Privacy Laws

FCRA | GDPR | EEOC | NLRA | HIPAA | State and Local Laws

- **Limit their internet search to publicly available information and avoid invading the candidate's private spaces**
- **Information should be relevant to the opening position**
- **They should also be transparent about their process and inform candidates about their rights.**

Should Mimi be hired? Why (or) why not ?

OPTION 1	Hire Mimi for China's expansion plan
OPTION 2	Don't hire Mimi
OPTION 3	Confront Mimi and then take a decision

1. Don’t erase your profile
2. Use social media to your benefit
3. Google yourself
4. Creating multiple, separate social media accounts
5. Be mindful of what you post

Let's be prepared