Dr. Ajay Shriram Kushwaha
Associate Professor

Cyber Law

Unit 5

Corporate Espionage

- Corporate espionage — sometimes also called **industrial espionage**, **economic espionage** or **corporate spying** — is the practice of using espionage techniques for commercial or financial purposes.
- We usually think of "espionage" in terms of spies working on behalf of one government trying to get information about another.

Types of Industrial Espionage:

- Trespassing onto a competitor's property or accessing their files without permission
- Posing as a competitor's employee in order to learn company trade secrets or other confidential information
- Wiretapping a competitor
- Hacking into a competitor's computers

How it's done

- Though most organizations are improving their methods of controlling security, data still leak through the cracks.
    - Simple Key logger
    - USB drive
    - Internet
    - Wi-Fi Phishing techniques
    - Employee
    - Malware

Forms of Corporate Espionage

- Economic or industrial espionage takes place in two main forms.
- In short, the purpose of espionage is to gather knowledge about (an) organization(s).
- It may include the acquisition of intellectual property, such as information on industrial manufacture, ideas, techniques and processes, recipes and formulas.
- Such as that on customer datasets, pricing, sales, marketing, research and development, policies, planning or marketing strategies or the changing compositions and locations of production.
- It may describe activities such as theft of trade secrets, bribery, blackmail and technological surveillance.
- As well as orchestrating espionage on commercial organizations, governments can also be targets — for example, to determine the terms of a tender for a government contract so that another tenderer

Avoiding Espionage

- Though espionage is not completely unavoidable, there are certain things companies, individuals and corporations can do to keep thieves from stealing data and other important information.
  - For example, they should never expose any internal network to outsiders and make sure all storage areas are secure.
  - Additionally, data at rest should always be encrypted and not readable when not in use.
  - Data inside storage should also be tamper-proof, which can be done by creating access controls where only the individual user can access his files.
  - Overall, companies should regularly monitor the data to assess how it is being used and remain vigilant.

Few Terminology in Cyber Forensics Laws Glance

iNURTURE Education Solutions Tomorrow's here

Inculpatory Evidence	**Inculpatory evidence is evidence that shows, or tends to show, a person's involvement in an act, or evidence that can establish guilt.** **i.e.,** Any evidence favorable to the prosecution is Inculpatory
Exculpatory Evidence	**Exculpatory evidence** is evidence favorable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt i.e., any evidence showing that the defendant is not guilty is considered exculpatory.
Police blotter	Information which is related to an crime and status storage place.
Cyber Stalking	Cyber stalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium.
Cyber Terrorism	The politically motivated use of computers and information technology to cause severe disruption or widespread fear

Chain of Custody

https://www.nist.gov/document/sample-chain-custody-formdocx

Digital Evidence Handling Procedure

- Establishing a computer forensic team
- Acquisition on incident alert
- Incident/Crime scene protocols
- Identification
- Collection
- Acquisition
- Preservation
- Analysis
- Reporting
- Persuasion and testimony
- Returning evidence

The Information Technology Act, 2000
and
The Information Technology (amendment) Act, 2008

A Comparative analysis

iNURTURE Tomorrow's here
Education Solutions

- The United Nations General Assembly have adopted the Model Law on Electronic Commerce on 30th January 1997.

- It is referred to as the **"UNCITRAL Model Law on E-Commerce".**

iNURTURE Education Solutions

- India passed the **Information Technology Act, 2000** on *17th October, 2000.*

- Amended on *27th October 2008.*

Amended Act is known as -

The Information Technology (amendment) Act, 2008.

Electronic authentication

- The IT Act, 2000 specified **“digital signatures”** as the means of electronic authentication.
- This approach was not a technology neutral approach and the law was bound by a specific technology.

Electronic authentication

- The IT Act, 2008 introduces the concept of **"electronic signatures"** in addition to *digital signatures.*
- Electronic signatures is the wider term covering **digital signatures, biometric authentication, etc.**
- It has a **technology neutral** approach and not bound by any specific technology.

Types of electronic signatures

- **Passwords, personal identification numbers (PINs)**

  i.e. based on the knowledge of the user.

Types of electronic signatures

- **Biometric authentication -**

  i.e. method based on the physical features or personal trait of the user

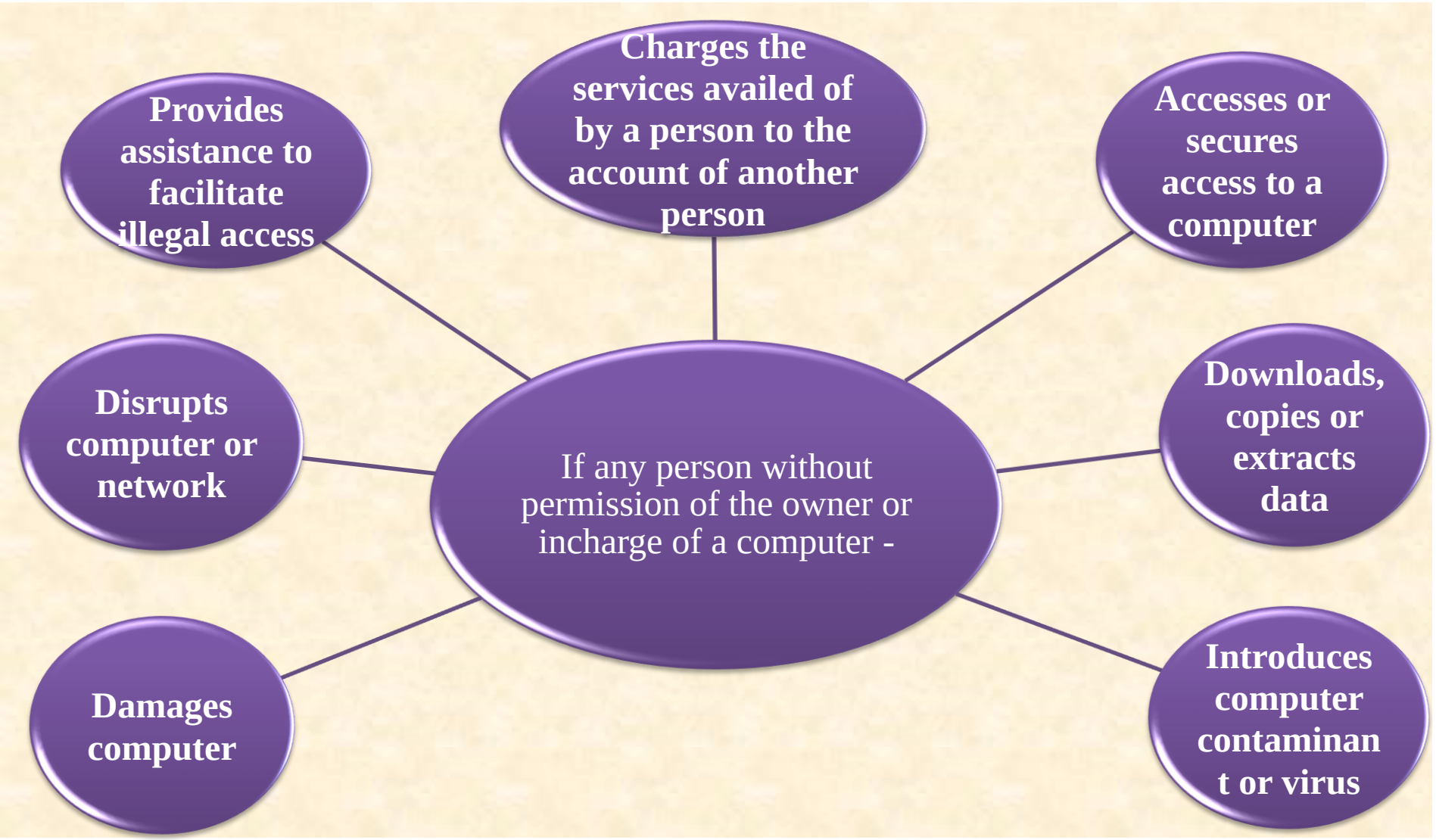
Types of electronic signatures

- Scanned handwritten signatures.
- Signature by means of a digital pen.
- “OK” or “I accept” boxes.
- Secure Sockets Layer (SSL) certificates.

- **Section 43 - Unauthorized Access**

  - Under the IT Act, 2008 **no limit on amount of compensation** for offences under Section 43

iNURTURE Education Solutions Tomorrow's here



- **Section 43(A)** – new provision
  - Corporate bodies handling sensitive personal information in a computer resource are under an obligation to ensure adoption of reasonable security practices to maintain its secrecy.

iNURTURE Tomorrow's here
Education Solutions

- Even mobile companies to respect privacy of customers **u/ Sec. 43(A).** *(Rutuja Tawade v/s Vodafone)*

  - **Nadeem Kashmiri's case (credit card fraud)**
  - **Liability on call centers, BPOs**

iNURTURE Tomorrow's here
Education Solutions

Adjudication of Civil offences

- Under the IT Act, 2008 **"Adjudicating Officers"** to try cases where the claim is **upto Rs. 5 crore.**
- Above that the case will have to be filed before the **"Civil Courts".**
- Under the IT Act, 2000 civil courts did not have jurisdiction to try civil suits.

iNURTURE Tomorrow's here
Education Solutions

Section 66

- Provision has been significantly changed.
- Under IT Act, 2008 all the acts referred under section 43, are also covered u/Sec. 66 if they are done *"dishonestly"* or *"fraudulently"*.
- Many cybercrimes on which there were no express provisions made in the IT Act, 2000 are now included in the IT Act, 2008.

- **Sending of offensive or false messages -** new provision
  - Also known as "**Cyber Stalking**"
  - Covers sending of menacing, offensive or false messages via **SMS/EMAIL/MMS**
  - Punishment – imprisonment upto 3 years and fine

- **Dishonestly receiving stolen computer resource or communication device** - new provision
  - Also covers **use of stolen Computers, mobile phones, SIM Cards, etc**
  - Punishment – imprisonment upto 3 years or fine upto Rs. 1 lakh or both

- **Identity theft** - new provision
  - Fraudulently or dishonestly using someone else's electronic signature, password or any other unique identification feature
  - Punishment - imprisonment upto 3 years and fine upto Rs. 1 lakh

- **Cheating by impersonation -** new provision
  - Cheating by pretending to be some other person
  - Punishment – imprisonment upto 3 years and fine upto Rs. 1 lakh

- **Violation of privacy -** new provision
  - Popularly known as **Voyeurism**
  - Pune spy cam incident where a 58-year old man was arrested for installing spy cameras in his house to ‘snoop’ on his young lady tenants
  - Covers acts like hiding cameras in changing rooms, hotel rooms, etc
  - Punishment –imprisonment upto 3 years or fine upto Rs. 2 lakh or both

Section 66(F)

- **Cyber terrorism** - new provision
  - Whoever uses cyberspace with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people
  - Punishment - Imprisonment which may extent to life imprisonment

Preservation of information by intermediaries

- **Section 67(C)** – new provision
  - Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

Government's power to intercept

- **Section 69** – new provision
  - Government to intercept, monitor or decrypt any information generated through any computer resource if it thinks to do so in the interest of the sovereignty or integrity of India.

Government's power to intercept

- Punishment for **refusing to hand over passwords to an authorized official of the Central or State Government**

- Punishment – imprisonment upto 7 years and fine

Liability of Intermediary not to disclose any personal information

- **Section 72(A) -** new provision
  - Intermediary to act as per the terms of its **lawful contract** and not beyond it.
  - Punishment – imprisonment upto 3 years or fine upto 5 lakh or both

Liability of Intermediary

- **Section 79**

  - An intermediary not to be liable for any third party information, data, or communication link made available or hosted by him.

iNURTURE Tomorrow's here
Education Solutions

Liability of Intermediary

- Intermediary need to prove that he didn't –
  - Initiate the transmission,
  - Select the receiver of the transmission, and
  - Select or modify the information contained in the transmission and
  - The intermediary observes due diligence while discharging his duties under the Act.

- **Section 84(B)** – new provision

  ✓ **Abetting to commit an offence is punishable**

  ✓ Punishment – Same punishment provided for the offence under the Act

iNURTURE Tomorrow's here Education Solutions

iNURTURE Tomorrow's here
Education Solutions

- **Section 84(C)** – new provision

  - **Attempt to commit an offence is punishable**

  - Punishment – Imprisonment which may extend to one-half of the longest term of imprisonment provided for that offence

iNURTURE Tomorrow's here Education Solutions

- **Section 78** – new provision

  - As per the IT Act, 2008 Cyber crime cases can be investigated by the **"Inspector"** rank police officers.

  - U/ the IT Act, 2000 such powers were with the **"DYSP/ACP".**

Compounding of Offences

- **Section 77 (A)** – new provision
  - Compounding – ***"Out of court settlement"***
  - Offences

    "*for which less than three years imprisonment has been provided*"

    can be compounded.

Compounding of Offences

- Such offence should not affect the socio economic conditions of the country or

- has been committed against a child below the age of 18 years or a woman.

iNURTURE Tomorrow's here
Education Solutions

Guidelines for Report writing

- Don’t Procrastinate
- Include analysis
- Be cautious of absolutes
- Create a template
- Break it up
- Title page
- Table of contents
- Exclusive summary
- Objectives
- Evidence analyzed
- Steps taken
- Relevant findings
- Timeline
- Conclusion
- Signature
- Exhibits