PPIT SHEET – **FINALS**

Rayyan Minhaj (20K-0143 | BCS-7F)

----------CASE STUDIES----------

FACEBOOK – CAN ETHICS SCALE IN DIGITAL AGE?

Facebook valued at $750bn in 2021 faced success AND increasing scrutiny. With over 2.8bn users, 7mil advertisers and significant volumes of data, it had to deal with **data privacy, anti-trust, and content moderation issues.** The Cambridge Analytica scandal, acquisitions of potential competitors like Instagram and WhatsApp, and debates on antitrust regulations fueled criticism, raising concerns about governance, user consent, and societal impact.

THE PATH TO USER AS PRODUCT

Facebook's evolution began in 2004 as a Harvard student network, **quickly expanding with venture capitalist investments** and opening to the public in 2006. Facing **competition from Myspace and Twitter**, Facebook introduced the **News Feed** in 2005, later enhancing sharing with the **Share button**. The platform's mobile presence grew in 2007, and by 2011, it focused on smartphone users, capitalizing on addictive engagement. The Facebook Platform in 2007 allowed third-party apps, leading to a robust ecosystem. Microsoft's investment and Facebook Beacon marked strategic moves in 2007. Sheryl Sandberg joined in 2008, steering Facebook towards advertising as a revenue model. **The "Like" button in 2009 and Open Graph API in 2010 expanded user interactions and data accessibility**. Acquisitions of Instagram in 2012 and WhatsApp in 2014 strengthened Facebook's position. By 2018, **Facebook and Google formed a digital duopoly, dominating online advertising.** Facebook's financial success continued, reaching $84 billion in revenues in 2020. However, concerns persisted, with plans for **an Instagram version for children** raising ethical questions.

THE ULTIMATE SURVEILLANCE MACHINE

The misuse of Facebook data, focused on the **Cambridge Analytica scandal**. Researchers initially **used Facebook data for personality prediction**, but later, GSR and Cambridge Analytica **exploited** the platform **to collect and sell data from 87 million users for political advertising**. The revelation led to public outrage, a #DeleteFacebook movement, and scrutiny from industry leaders. **The incident prompted Facebook to implement a six-point plan to enhance data protection**, including reviewing the platform and turning off access for unused apps. The company **also faced criticism for granting device manufacturers, including Chinese firms, access to user data**. In response, Facebook released a **privacy-focused plan in 2019**, aiming to integrate and encrypt communications across its platforms.

PLATFORMS & ANTI-TRUST

The concerns about the **digital duopoly of Facebook and Google**, suggested that they should be **split up or restricted from acquiring potential competitors**. Facebook's **acquisition strategy**, including **copying features from emerging apps and acquiring companies like Instagram and WhatsApp**, has raised **antitrust concerns**. Analysts question whether the U.S. government missed an opportunity to review the Instagram acquisition more closely. In 2019, legal scholar Lina Khan argued that **Facebook, despite offering free services, constituted a monopoly by extracting user data**. Antitrust investigations were initiated by the Federal Trade Commission, state attorneys general, the U.S. Department of Justice, and the European Union. In 2020, a German court ruled Facebook violated antitrust laws, and in December 2020, the U.S. federal government and state attorneys general filed an antitrust lawsuit against Facebook, focusing on its acquisitions and alleged pattern of neutralizing competitors. **Facebook proposed building a potential competitor, but regulators rejected the idea.**

CONTENT MODERATION AND POLITICS: "THE IMPOSSIBLE JOB"

Facebook's struggles with content moderation, included issues like the **Russian interference** in the 2016 U.S. election where 13 military Russian officers and 3 Russian entities **purchased $46,000 worth of Facebook ads** in hopes of tampering with election campaigns and the broader challenge of **managing false campaigns and hate speech**. One study showed that **lies spread faster than the truth** on Twitter. "On average, it took true claims about six times as long as false claims to reach 1,500

people, with false political claims traveling even faster than false claims about other topics, such as science, business, and natural disasters," It mentions the emergence of startups, including **New Knowledge, addressing these concerns**. New Knowledge utilized a team of **former intelligence workers** to develop **AI software that could extract indications of manipulation within user accounts**. It could monitor how bad actors could "plant seeds" in individual accounts and paid advertisements, it could inform companies and social media platform clients that bad influencers were attempting to manipulate their customer base. Clients could then be shown how to prevent such manipulation. In 2018, **criticisms faced by Facebook**, ranging from **allegations of bias** to the **spread of hate speech and fake news**. The Court of Justice of the European Union's 2019 ruled that **Facebook must globally remove hateful content**. Facebook's **response** involves significant efforts, **including increasing content moderation staff, investing in AI, publishing transparency reports, and spending billions on platform safety**. The creation of a "Supreme Court" for content moderation was done. **Despite these measures, the persistent nature of the challenges, such as livestreaming violent acts continued (Christchurch, NZ)**. Facebook's ongoing struggles to maintain a secure online environment are still providing insights into the company's mismanagement of personal data.

POTENTIAL FORCES FOR CHANGE

The multifaceted landscape surrounding Facebook focused on the responses and considerations of both **internal and external stakeholders** in the face of significant challenges, particularly the **Cambridge Analytica scandal and escalating regulatory concerns**.

A key aspect was the ongoing debate surrounding **Facebook's business model**. **Some stakeholders propose a shift to a subscription-based approach**, aiming to align user interests more closely with the platform. However, the feasibility of such a transition raised questions, as compensating for the substantial advertising revenue (reported at $40 billion in 2017) would be essential for sustained growth.

The dissent within Facebook's ranks, featuring notable figures like Sandy Parakilas, who **expressed doubts about the company's prioritization of data collection over privacy**. Andrew Bosworth's **controversial memo emphasizing growth at all costs**, Alex Stamos's **push for greater disclosure on interference**, Elliot Schrage's **critique of underinvestment in protections**, and Chris Cox's **call for a shift in the company's approach** all underscore internal tensions.

The passage sheds light on **societal perceptions**, drawing attention to a UK survey where two-thirds of respondents **expressed concerns** about **inadequate regulation, transparency, and inappropriate user data sales by online companies**. Over half felt these companies **exploited user loneliness**, while a third **viewed social media negatively**. Calls for stronger government regulation (64%) coexist with a lack of trust in the government (36%).

Psychographic profiles and their potential invasiveness with **users feeling vulnerable** due to the **intimate nature of this data**. Concerns about **informed consent**, especially given the **complexity** of Facebook's **terms of service**, were raised. Legal actions in Germany and the passage of the GDPR in the EU further illustrate the global challenges related to privacy and data sharing.

Various regulatory approaches are explored, from **fines and the Honest Ads Act to implementing data protection legislation**. The potential adoption of GDPR-like regulations in the U.S. is considered, despite **concerns about its impact on smaller players**. The passage also introduces the idea of creating a **Digital Protection Agency** and highlights debates around antitrust issues, with suggestions to break up Facebook into multiple companies.

Investors, particularly large institutional ones like BlackRock, Vanguard, and State Street **held 20% of Facebook together**. The **Cambridge Analytica scandal** led to a **significant drop** in Facebook's market capitalization, prompting **increased scrutiny** from shareholders. Proxy advisory services consistently gave Facebook **poor marks** on governance, compensation, and shareholder rights.

The impact on advertisers and app developers emphasized the **shift away from traditional media platforms** toward digital advertising on Facebook. Brands are noted for **pressuring social media for better user protections**, although actual spending cuts post-Cambridge Analytica were limited. The digital duopoly's dominance, especially in the context of psychographic marketing, is acknowledged as a challenging dynamic for advertisers.

TIME TO HIT RESET

The aftermath of the challenges faced by Facebook, notably the Cambridge Analytica scandal led to subsequent **scrutiny from regulators and the public**. Mark Zuckerberg and Sheryl Sandberg expressed openness to regulation, and despite an initial stock gain after the Congressional testimony, Facebook **faced a significant drop in its market value** in July 2018 due to missed earnings projections, public perception issues, and stagnant user growth.

Despite the setback, Facebook's **stock price eventually recovered**, reaching an all-time high in June 2018. The company reported growth in revenue, EBITDA, and user engagement, especially with the integration of Instagram and WhatsApp. However, challenges persisted, including the announcement of the LIBRA cryptocurrency, met with withdrawal intentions from high-profile partners.

Questions about the management style of Sandberg and the turnover in her team were raised and whether Facebook's mission aligns with how social media is actually being used and if Zuckerberg and Sandberg are reevaluating priorities to restore user trust and privacy protection. The growing call for regulations globally and locally, coupled with the influx of new users and the influence on them, poses challenges and opportunities for Facebook's leadership. The passage concludes by prompting consideration of how Zuckerberg and Sandberg will navigate these complexities and what their legacy will be.

----------X----------X----------X----------

HOW INDIA PLANS TO PROTECT CONSUMER DATA

The Indian government wants to set a legislate called **Personal Data Protection bill (DPB)** to **control the collection, processing, storage, transfer, protection, and disclosure of personal data** of Indian residents. It will attract numerous global players who must comply with DPB. Previously, India has followed the EU bill (GDPR) to allow global companies to operate within India under certain conditions but with the **DPB, India will be able to carry additional provisions beyond the EU regulations**. India being a nation state, it treats its citizen's data as a **national asset** and hence upholds the responsibility of storing and safeguarding it within national boundaries, along with reserving the rights to use the data in its defense and strategic interests.

Some features of the DPB which will force companies to change their business models, practices, and principles in hopes **of increasing data protection regulation** include:

1. PRIVACY AS A FUNDAMENTAL RIGHT

In 2017, the Supreme Court of India recognized **privacy as a constitutional right for Indian citizens**. The DPB aims to safeguard this right by **regulating the collection, security, storage, sale, and exploitation of private data generated by citizens in the digital realm**. The proposed regulations could impact the business models of digital firms **that provide free services but rely on profits from selling and exploiting user data**. These companies may need to reassess their strategies if the new regulations make **data collection and exploitation less profitable.**

2. USER CONSENT

Under the DPB, digital companies **will require explicit user consent** before collecting data which should state why that data is being collected (**purpose**). This consent should be **asked at every stage of data processing**. The problem is that companies use user data to generate **new information from that data** for ex. Uber analyzing traffic patterns and Amazon assessing feedback. Sometimes, **raw data is sent to third-party** processors for analysis, creating new information when combined with data from other sources. This redefines digital companies as **"data fiduciaries"** under the DPB, **requiring them to take on the responsibility of obtaining user permission for both initial collection and subsequent processing of data**.

3. OWNERSHIP OF PERSONAL DATA

DBP proposes that **data provider is the owner of their personal data**. This places a burden on digital companies. In the physical world, property owners can ask to have their properties returned whereas in digital world, **companies will have to figure out how to comply with the erasure and deletion of all their personal information**. Digital companies will also have to think outside of their own ecosystem **if they have provided the data to any third party.**

4. THREE CLASSES OF DATA

The Data Protection Bill (DPB) identifies **3 classes of data** with **specific regulations** for each: **sensitive data**

(involving financials, health, sexual orientation, genetics, transgender status, caste, and religious belief), **critical data** (government-deemed exceptionally important, such as military or national security data), and a **general category encompassing other data**. DPB mandates that **sensitive and critical data must be stored in India**, with **sensitive data allowed for processing abroad but requiring storage in India**. **Critical data cannot leave the country. There are no restrictions for general data**. This shift from the current global cyber environment could impose additional costs on digital companies, potentially leading to suboptimal storage and processing capacities, and contributing to the concept of a "splinternet" or the fragmentation of global digital supply chains.

4. DATA SOVEREIGNTIY

DPB reserves the right to **access locally stored data to protect national interests**. This implies that DPB would **treat citizens' data as a national asset**, **no different than control over citizens' physical properties**. In this respect, DPB differs from GDPR, which imposes no locational storage requirements or preferential access to data for protecting national interests. Currently, digital companies practically own the data if they can address the privacy concerns and meet the user-acceptance requirements. One implication of the new policy is that when the government demands its citizens' data, in case of foreign attacks and surveillance, digital companies would have to abide and assist the Indian government's defense policy.

5. NATIONAL INTERESTS

The Data Protection Bill (DPB), while prioritizing citizens' privacy, **exempts government agencies from certain provisions. DPB does not apply to government agencies processing personal data for reasons related to national security**, **detection of unlawful activity or fraud, and epidemic or medical emergencies**. This means that public sector entities can obtain personal data from individuals without their consent in these situations. Furthermore, **the government can direct digital companies to provide non-personal or anonymized data for research or planning purposes**. Critics express concerns about potential **misuse** of such data for **political surveillance,** and there are debates over the effectiveness of anonymization. Compliance with these requirements may prompt digital companies to revise their policies, **similar to past controversies such as Apple's refusal to unlock an iPhone for an FBI investigation**, raising questions about whether such refusals would be possible under DPB.

6. VERIFICATION TAG

DPB requires that all digital **companies must identify their users and tag them into three categories to reduce trolling** (e.g., an anonymous user or a bot trying to incite violence by posting incendiary comments): **Users who have verified their registration and display real names**; **users who have a verified registration but have kept their names anonymous**; **and users that have not verified registration**. This would be a first regulation of its kind in global social media. This implies that **digital companies must put in place procedures for collecting and verifying the real identities of their users**. Note that **Facebook has more that 100 million fake account**s and faces the dilemma of continuing as is, attempt to verify them, or delete those accounts.

7. COMPLIANCE AND ENFORCEMENT

DPB proposes steep **penalties for noncompliance**. In case of **a data breach or inaction** by the fiduciary upon data breach or a minor violation, the penalties could reach $ 700,000 or 2% of a company's global revenues, whichever is higher. For **major violations, such as data shared without consent**, the penalties would double. These penalties, which are based on multinationals' global income, and potential **jail sentences for officers of digital companies**, imply that DPB regulations cannot be taken lightly. Its provisions must be complied with in order to do business in India.

8. TAXING DIGITAL COMPANIES

As we note in a previous article, multinational digital companies can easily transfer their income to tax havens and avoid paying taxes to local governments, with no fear of confiscation of their properties. **Physical control over data and fear of enforcement penalties might give the Indian government additional leverage to collect taxes and dues from digital companies**. This would lower the likelihood that digital companies can get away with paying little or no taxes to the local governments.

9. OTHER ISSUES

The DPB applies to all businesses that collect personal data, not just digital businesses. For example, John Deere collects and processes data obtained from its farm equipment. Whether DPB applies to tractors with sensors, whether the collected data belongs to the farmers, and how the benefits of farm data are shared becomes a debatable point.

----------X----------X----------X----------

DOLCE & GABBANA: RACISM, STEREOTYPE, OR BEING FUNNY

In 2018, D&G came under heavy scrutiny and boycott after some controversial advertisement videos and racist personal messages by Stefano Gabbana himself went viral.

THE CONTROVERSIAL VIDEOS

Dolce & Gabbana (D&G) faced controversy **over three 40-second videos** promoting "The Great Show" as a tribute to China. The videos, **depicting an Asian model struggling to eat Italian food with chopsticks, were perceived as patronizing and racist**. Social media outrage ensued, with some considering the videos **intentionally provocative for profit**. D&G's official apology and removal of the videos did not quell the controversy. Stefano Gabbana's Instagram response, alleging **hacking**, **added to the backlash** as he appeared to make **derogatory remarks about China**. D&G's claims of hacking were met with **skepticism**, with many finding their apologies insincere, suggesting a **pattern of making offensive remarks and issuing inadequate apologies.**

COMPANY BACKGROUND

Dolce & Gabbana (D&G), established in 1985, had gained international prominence as a **luxury fashion house** producing high-end clothing, accessories, and beauty products. Owned by the D&G Group, the company was divided into **three divisions**: production, distribution, and licenses. Founders **Domenico Dolce** and **Stefano Gabbana** played key roles in the brand's creative direction and global strategies. The duo, with roots in small clothing businesses, founded D&G after a successful runway debut in 1985. Over the years, the company expanded its product lines, collaborated with the Onward Kashiyama Group for distribution in Japan, and launched fragrances, eyewear, and children's collections. D&G's success was fueled by its use of Italian cultural elements, and Madonna's friendship notably contributed to its international fame. As of 2018, the brand continued its global expansion, opening a flagship store in Miami.

CONTROVERSIAL MARKETING STRATEGIES

Dolce & Gabbana (D&G) has a history of **controversial marketing strategies**, often involving **negative advertising and offensive campaigns**. The brand, **not constrained by the need to appease investors, retains direct control** and has been criticized for making politically incorrect statements. D&G's wealthy clientele, perceived as distant from everyday citizens, may contribute to its perceived insensitivity. The brand has **faced backlash for incidents** such as labeling a shoe as a "slave sandal" in 2016 and portraying poor working-class citizens as "normal" in a 2017 Beijing campaign. Despite canceling "The Great Show" in 2018 amid **accusations of racism**, D&G's controversies have sparked discussions about racism and cultural sensitivity in the fashion industry. Some argue that the issue is rooted in a "cult of personality" within the fashion power structure, where celebrity designers with massive followings contribute to the industry's controversies and are amplified by social media.

BOYCOTT FROM CHINESE CUSTOMERS

D&G faced a **significant boycott** from Chinese customers after the controversial videos. Chinese-French model Estelle Chen **withdrew from D&G's planned show in Shanghai**, denouncing the brand's actions **as racist and accusing the designers of prioritizing money over China**. Other **brand ambassadors, models, and agency** China Bentley announced their boycott, with some even **burning D&G products in protest**. The backlash extended beyond individuals, with major Chinese e-commerce platforms, including Alibaba's Taobao and JD.com, **ceasing to carry D&G products**. Smaller platforms in China and even global platforms like Yoox Net-A-Porter Group joined the boycott. The criticism also affected D&G in European and North American markets, with

consumers denouncing the brand on social media and **returning items to department stores**. The **model** in the ads **faced personal backlash**, with accusations of makeup manipulation and derogatory comments about her appearance.

FINANCIAL COSTS

The controversy surrounding D&G is expected to have **significant financial repercussions**. D&G stores in Shanghai were **vandalized**, and considering China's enormous consumer base, the **backlash from millions could have substantial consequences**. Chinese consumers accounted for nearly **one-third of global luxury goods spending** in 2017, representing a substantial portion of D&G's estimated **profits** of €1.3 billion in 2018, with **30% attributed to China**. Women's Wear Daily estimated **potential losses for D&G at €400 million**, excluding additional impacts from canceling the show and potential Western consumer boycotts. Brand Finance **estimated that 20% of D&G's brand value could be eroded**. As Chinese consumers played a significant role in luxury spending, D&G's setback contrasted with other brands actively courting the Chinese market with culturally sensitive approaches. The controversy was viewed as a **crisis**, and experts emphasized the need for global brands to be attuned to local sensitivities for successful recovery.

CONCLUSION

In conclusion, there had been **no significant change in Dolce & Gabbana's (D&G) behavior or marketing following the cancellation of the Shanghai show**. The brand's response included **a video apology** and **messages on social media platforms**, **attributing inflammatory messages and videos to supposed hacks**. Despite these efforts, the **damage** to D&G's reputation was **substantial**, especially given **the size and importance of the Chinese luxury market**, which experts predicted could significantly impact the brand's profits. The question remained about what mitigation strategies or actions D&G could undertake to repair the harm caused to its reputation.

----------X----------X----------X----------

CAN FACEBOOK EVER BE FIXED?

Facebook, notorious for **privacy scandals and data leaks**, faces criticism as CEO Mark Zuckerberg proposes **four new ideas to regulate the internet**. Despite the company's history of privacy shortcomings, Zuckerberg's **proposals are deemed superficial in comparison to the scale of the problems Facebook confronts**. The **consistent pattern of privacy issues contrasts with the company's public assertions that it is committed to making amends**, prompting scrutiny of Zuckerberg's latest attempt at change. The article questions the **sincerity** and **effectiveness** of the **proposed solutions** in addressing Facebook's persistent challenges in **data collection**, **storage**, and **analysis**.

Mark Zuckerberg's **four proposals** for regulating the internet include.

- a call for governments to **define harmful content** online.
- expanding **laws on political advertising** beyond elections.
- **standardizing global privacy regulations** like the General Data Protection Regulation (GDPR).
- **advocating for data portability** to enable users to **move their data between services** easily.

However, critics argue that many of **these proposals are already in practice or are being mandated by regulators worldwide**. For instance, GDPR already requires data portability in the EU, and major regulations in countries like Germany, China, and Australia are addressing harmful content. Zuckerberg's proposals may **lack a sense of sacrifice or genuine atonement for past data-related mistakes** and could **potentially benefit Facebook in the long run.**

Three major predicaments stemming from **Facebook's interests** that **diverge** from its **users' interests**.

- First, Facebook's business model relies on **user engagement and monetizing gathered data through targeted advertising**. Users often don't fully grasp the scale of data they provide, while Facebook promotes a sense of social connection and community.
- Second, Facebook's **immense scale**, with 2.32bn monthly users and a very small employee count (1 employee for 65,000 users), makes **effective governance and protection challenging**, leading

to inevitable **failures** in areas like **cybersecurity and privacy.**

- Lastly, a **cultural problem within Facebook**, marked by **consistent privacy missteps**, suggests a **lack of prioritization for user security and privacy.** Unforced errors erode user trust, hindering the company's ability to address its core issues.

Its globally acknowledged that **Facebook is not solely responsible for the current digital discomfort**, as many tech **giants face similar issues**. It highlights how the adoption of digital technologies happened quickly without a full understanding of their downsides and risks.

The **suggested solutions involve crafting new legislation to enhance privacy and security standards for all software systems, slowing down the adoption of digital technology**. Limiting the power of companies like Facebook by **restricting data collection** and **service aggregation** is proposed, possibly involving the physical separation of different services. The long-term evolution of **Facebook's business model should prioritize trust** by making user privacy and data security as **crucial as monetization.**

However, in the short term, **Facebook is distant from achieving these goals**. Despite appeals to governments, the company is **yet to fully grasp the depth of the problems**. The ongoing struggle between Facebook and its users to **redefine their relationship may persist until governments intervene more forcefully**. Zuckerberg's **recent proposals are seen as another episode in this prolonged struggle** for reframing the user-company bargain.

----------X----------X----------X----------

Complaints and Offences in Personal Data Protection:

48. Unlawful processing of personal data:

- Processing, disseminating, or disclosing personal data against the Act's provisions is an offence.
- Fine up to $125,000 USD for the first offence, may increase to $250,000 USD for subsequent violations.
- Higher fines for sensitive and critical personal data violations - up to $500,000 USD and $1,000,000 USD respectively.

49. Failure to adopt data security measures:

- Failure to implement adequate data security measures, as per the Act, results in a fine up to $50,000 USD.

50. Issue enforcement orders and impose penalties:

- Failure to comply with Commission or court orders incurs a fine up to $50,000 USD.
- Data controllers/processors violating Act provisions may face fines up to $2,000,000 USD or suspension/termination of registration.
- Legal entities may be fined up to 1% of annual gross revenue in Pakistan or $200,000 USD, whichever is higher.

51. Complaint:

- Individuals can file complaints with the Commission for personal data protection violations.
- Complaints cover breaches of consent, obligations, false information, or any matter related to personal data protection.
- Complaint filing involves reasonable fees, online submission, acknowledgment within three days, and disposal within 30 days.
- The Commission can seek explanations from involved parties and issue directives to prevent data protection breaches.

52. Appeal:

- Appeals against Commission decisions go to the High Court or a designated Tribunal.
- The High Court or Tribunal decides appeals within ninety days.

- Appeals against Commission officers' decisions must be filed with the Commission within thirty days, with the Commission deciding within thirty days.

**Pakistan's Prevention of Electronic Crimes Act, 2016

The law dealing with cyber crimes in Pakistan is Prevention of Electronic Crimes Act, 2016 ("Act") which is applicable to every citizen of Pakistan wherever he may be and to every other person who is stationed in Pakistan for the time being.

The law address to following types of cyber crimes under the Act:

1. Access or interfere the data or information system and copying or transmission of data; (Section 3, 4 and 5 of the Act).
2. Unauthorized access, unauthorized copying, unauthorized transmitting or unauthorized interfering with the critical infrastructure OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Sections 6, 7 and 8 of the Act).
3. Prepare or disseminate information through any information system or device with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Section 9 of the Act).
4. Whosoever prepares or disseminates any Hate Speech, information that invites motivation of people to fund or recruits for terrorism through any information system or device (Sections 11 & 12 of the Act).
5. Electronic forgery and electronic fraud committed by interfering with any information system, device or data with the intent to cause damage or injury to the public; or to make any illegal claim; or title or to cause any person to part with property; or to enter into a contract; to commit fraud; alteration, deletion or suppression of data etc. (Sections 13 & 14 of the Act).
6. An act to manufacture, generate, adapt, export, supply, offer to supply or import any information system, data or device, with an intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act. (Section 15 of the Act).
7. Unauthorized use of another person's identity information or to obtain, sell, possess or transmit such information. (Sections 16 of the Act).
8. Issuance of SIM (subscriber identity module); R-IUM (re-useable identification module); or UICC (universal integrated circuit) or any other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices without obtaining and verification of the subscriber's antecedents. (Section 17 of the Act).

9. **Dignity of Natural Person**: Public exhibit or display or transmission of any information knowingly that such information is false and intimidate or harm the reputation or privacy of a natural person through an information system. (Section 20 of the Act).
10. **Modesty of Natural Person**:, Intentional and public display or exhibition or transmission of any information which superimposes a photograph over any sexually explicit image or video of a natural person; includes a photograph in sexually explicit conduct of a natural person; intimates a natural person with sexual act; sexually explicit image or video of a natural person; or entices or induces a natural person to engage in sexually explicit act; through an information system to harm a natural person or his reputation, take revenge, create hatred or blackmail a natural person. (Section 21 of the Act).
11. **Child Pornography**: Produce, offer or make available, distribute or transmit through an information system or to procure for himself or for any other person or without lawful justification possesses material in an information system any material which contain the elements of child pornography. (Section 22 of the Act).
12. Writing, offering, making available, distributing or transmitting **malicious code** through an information system with an intent to cause harm to any information system or data resulting in the corruption, destruction, alteration suppression, theft or loss of information system. (Section 23 of the Act).
13. Doing **Cyber Stalking** with an intent to coerce or intimidate or harass any person by using information system, information system network, internet website, electronic mail or any similar means of communication. The term Cyber Stalking includes: **(a)** foster personal interaction repeatedly to a person who clearly indicates a disinterest from the stalker; **(b)** monitor the internet, electronic mail, text message or any other form of electronic communication of another person; **(c)** watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress in mind of such persons; and **(d)** take photograph or make video of a person and display or distribute such video in a manner without his consent that harms a person. (Section 24 of the Act).
14. **Spamming**: A person commits the offence of spamming who with an intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (Section 25 of the Act).

Intellectual property rights

Introduction

- Property such as bicycles or computers is called **tangible property**, that is, property that can be touched. It is protected by laws relating to theft and damage.
- Property that is intangible is known as **intellectual property**. It is governed by a different set of laws, concerned with **intellectual property** rights, that is, rights to use, copy, or reveal information about intellectual property.
- **Intellectual property** crosses national borders much more quickly than tangible property and the international nature of intellectual property rights has long been recognized.

Copyright

Copyright protects:

- original literary, dramatic, musical and artistic works;
- sound recordings, films, broadcasts and cable transmissions;
- the typographical arrangement of published editions.
- Things protected by Copyright are called "works".

Software copyright

- The 1988 Copyright, Patents and Designs Act states that the phrase 'literary work" includes a table or compilation, a computer program and preparatory design material for a computer program
- The EU directive 91/250 states that “Member States shall protect computer programs, by copyright, as literary works. For the purposes of this Directive, the term ‘computer programs’ shall include their preparatory design material.”

Owner’s rights

Copyright gives five exclusive rights to the owner of the copyright:

- the right to copy the work;
- the right to issue copies to the public;
- the right to perform, play or show the work to the public;
- the right to broadcast the work or transmit it on a cable service;
- the right to make an adaptation of the work.

How long do the rights last?

- **In the EU**, 70 years from the death of the author (in the case of a literary or artistic work, or software);
- **In USA**, the same is true for works published after 2002, but can be 95 years after the date of publication in some cases, for earlier works;
- **In Canada**, it is 50 years from the death of the author.

Database right (Copyright and rights in databases regulations1997)

- If a database is the author’s “own original intellectual creation”, it is treated as a literary work and it is subject to the copyright protection.
- If there has been “substantial investment in obtaining, verifying or presenting the contents of the database”, then it is also protected by the database right. (**This lasts for 15 years**, much less than copyright which is much longer than the database is likely to be useful.)

Who owns the copyright?

- If the author is an employee and the work is an original literary, dramatic, musical or artistic work created in the course of employment, then the copyright belongs to the employer.
- An independent contractor is not an employee and so will own the copyright in work he does unless agreed otherwise.
- Copyright can only be transferred in writing.
- Copyright does not need to be registered. It comes into existence at the moment the work is recorded, in writing or otherwise.

Infringement of copyright

- Anyone who, without consent, does any of the five things that are the exclusive right of the owner of the copyright has committed primary infringement of copyright.
- Secondary infringement occurs when an infringement is performed knowingly and in the course of business.
- Primary infringement is purely a civil matter. Secondary infringement can be a criminal offence.

Registering Copyright

- In Britain and Europe, full copyright protection comes into effect immediately, when the work is ‘fixed’, i.e. recorded in some form.
- In the USA, protection is very limited unless copyright has been registered with the US Copyright Office.

When is a copy a “copy”?

- Copyright is breached by copying ‘the whole or a substantial part of the work’.
- ‘Substantial’ can also mean just a key part, which could be quite small.
- Non-literal copying, e.g. using the same design to produce a similar system written in a different language.

Licensing

- A license allows (the licensee), to use a work for some or all purposes but the owner retains ownership.
- Licenses can be exclusive or non-exclusive.
- The license may be for a fixed period or it may be in perpetuity.
- In an assignment, the copyright owner transfers some or all of the rights of ownership to someone else (the assignee).

Examples of licenses

- **Retail software:** a license is perpetuity to use one copy of the software on a computer of your choice. Non-exclusive.
- **Professional packages:** one year license, renewable, to run the software on a server with a specified maximum number of simultaneous users. Non-exclusive.
- **Marketing agreements:** exclusive license to sell sub-licenses in a specified geographical area.

Open-source licenses / free software

- An **open-source license** allows the source code to be used, modified or shared, subject to certain conditions. It is not necessarily free.
- Free software can be used without payment, but the source code may not be necessarily available, and modifying it may not be permitted.

Assignment

- Copyright may be assigned for a limited or unlimited period. It may be assigned for future works as well.
- Assignments must be in writing and signed by the copyright owner.

What you can do

fair dealing, copying for:

- private study or research;
- criticism or review
- reporting current events

making back-up copies

error correction.

How can copyright owners enforce their rights?

- Search and Seizure;
- Injunctions – court orders restraining people from infringing copyright;
- Claim damages;
- Claim for profits.

Large Companies who own copyright, often prevent illegal publication of copies by threatening action or suing, that a small publisher cannot afford to defend.

Patents

- A patent is a temporary right, granted by the state, enabling an inventor to prevent other people from exploiting his invention without his permission.
- Unlike copyright, it does not come into existence automatically; the inventor must apply for the patent to be granted. However, the protection it gives is much stronger than copyright, because the grant of a patent allows the person owning it (the patentee) to prevent anyone else from exploiting the invention, even if they have discovered it for themselves.
- Patents were originally intended to encourage new inventions, and in particular to encourage the disclosure of those new inventions.
- Inventors are often hesitant to reveal the details of their invention, for fear that someone else might copy it.
- A government-granted temporary monopoly on the commercial use of their invention provides a remedy for this fear, and so acts as an incentive to disclose the details of the invention.
- After the monopoly period expires, everyone else is free to practice the invention. And because of the disclosure made by the inventor, it is very easy to do so.
- Patent holders receive exclusive rights to make, use, or sell a utility, design, or plant.
- The patentee must file a detailed description of the invention which is published by the government.
- Public disclosure provides a reservoir of technical information.
- Some companies prefer to protect their inventions called ***Trade Secrets*** kept private to maintain a company's competitive advantage.

Patent may only be granted if:

- The invention is new
- It involves an inventive step
- It is capable of industrial application
- The subject matter of the invention does not fall within an excluded class

Excluded class

- A scientific theory e.g. law of physics cannot be patented.
- A mathematical method e.g. method of calculating a square root.

- A literary work, dramatic, musical or artistic work.

Parts of the patent

Typical patent includes:

- INID Codes (Internationally agreed Numbers for the Identification): international system that allows elements on the patent cover page to be identified in all languages
- Claims - phrases that precisely define the invention and outline the boundaries of the claimed invention (prevents infringement)

Types of patents

- **Utility patents** which may be granted to anyone who invents a machine, vital process, composition of matter, article of manufacture or any useful improvement thereof.

- **Design patents** may be granted to anyone who creates a new, original design for an article of manufacture

- **Plant patents** may also be granted to anyone who creates or discovers or reproduce any distinct and new variety of plant (Genetic Modification).

TRADEMARKS AND TRADE NAMES

- A **trademark** is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, that identifies and distinguishes the source of the goods of one party from those of others. Examples – *Reebok*, *Mc Donald's*, *Nike*, *Levis* etc.

To register a trade mark, the mark must be: -

- distinctive, and**,** not deceptive, or contrary to law or morality, and,
- It must not be identical or similar to any earlier marks for the same or similar goods.

Selecting a Mark!

- **Generic terms:** common name of the article or services to which they are applied. They are not protectable as standalone trademarks. (Examples: *computer*, *automobile*, *shuttle*.)
- **Suggestive Marks:** suggest, rather than describe, the goods or services or some characteristic thereof. Consumer must use imagination or hindsight to understand the connection.
- Although suggestive marks are self-advertisers and, thus, easier to promote than arbitrary marks, they are subject to more conflict and may be afforded a narrower scope of protection.
- **Arbitrary Marks:** created from existing words, but have no meaning in relation to the goods or services with which they are used. Fanciful and arbitrary marks are easier to protect but can be more expensive to promote. (Examples: *APPLE* for computers and *TIDE* for detergent).
- **Fanciful Marks:** created from words that are coined or made up, and have no meaning in relation to the goods or services. (Examples: *KODAK* for film and *EXXON* for petroleum products).

Difference between Trademarks and Service mark

- The main difference between service mark and trademark is that trademark is applicable for use only to identify products or goods produced by a business. On the other hand, a service mark is used to exclusively identify a service.

Domain Names

- *ICANN* [Internet Corporation for Assigned Names and Numbers] is an internationally organized, non-profit making corporation. Its main responsibility is ensuring the 'universal resolvability' of internet addresses.
- That is, ensuring that the same domain name will always lead to the same internet location wherever it is used from and whatever the circumstances.
- In practice, *ICANN* delegates the responsibility for assigning individual domain names to other bodies, subject to strict rules.
- Domain names were originally meant to be used just as a means of simplifying the process of connecting one computer to another over the internet.
- However, because they are easy to remember, they have come to be used as a way of identifying businesses. Indeed, they are frequently used in advertising.
- Conversely, it is not surprising that companies would want to use their trademarks or their company names as their internet domain names.
- The potential for conflict between trademarks and domain names is inherent in the two systems. Trademarks are registered with public authorities on a national or regional basis.
- The owner of the trade mark acquires rights over the use of the trade mark in a specific country or region. Identical trademarks may be owned by different persons in respect of different categories of product.
- Domain names are usually allocated by a private organization and are globally unique; they are normally allocated on a first come, first served basis.
- This means that if different companies own identical trade marks for different categories of product or for different geographical areas, only one of them can have the trade mark as domain name, and that will be the one who has applied first.
- The inconsistencies between two different systems of registration have made it possible for people to register, with their own domain names, for the trademarks belonging to some other company.
- This is sometimes known as *cybersquatting*. They then offer to sell these domain names to the owner of the trade mark at an inflated price.
- It is usually cheaper and quicker for the trade mark owner to pay up than to pursue legal remedies, even when these are available.

****

DATA PROTECTION, PRIVACY & FREEDOM OF INFORMATION

Why is privacy an important issue?

- In recent years there has been a growing fear about the large amount of information about individuals held on computer files.
- In particular it was felt that an individual could easily be harmed by the existence of computerized data about him/her which may be inaccurate or misleading and which could be transferred to an unauthorized third party at high speed and very little cost.

The Data could be

> Healthcare records > **Criminal justice** investigations & proceedings > Financial institutions & transactions

> Biological traits, such as genetic material > **Residence** and geographical records > **Ethnicity**

> Privacy breach **>** Location-based service and geolocation

Data mining: "We may use information about you that we collect from other Facebook users to supplement your profile"

- Inability to voluntarily terminate accounts (previously)
- Photo recognition and face tagging 2011
- Timeline
- Psychological effects

What is the Data Protection Act?

- Freedom to process data vs. privacy of individuals.
- 1984 act was repealed by the 1998 act.
- Anyone who processes personal information must comply with the eight principles
- It provides individuals with important rights, including the right to find out what personal information is held about them

Data protection act 1998

Main objective of Data Protection Act was designed to protect individuals from:

- the use of inaccurate personal information or information that is incomplete or irrelevant;
- the use of personal information by unauthorized persons;
- Use of personal information other than the intended purpose

Terms of the data protection Act

- **Personal data:** It's an information about a living individual
- **Data users:** are organizations or individuals who control the contents of files of personal data – i.e. who use personal data which is covered by the terms of the act
- **A Data subject:** is an individual who is the subject of personal data
- **Data controller:** means a person who determines why or how personal data is processed. This may be a legal person or a natural person.

Rules of Data Processing

Processing means obtaining, recording or holding the information or data or carrying out any operations on it, including:

- organization, adaptation or alteration of the information or data,
- retrieval, consultation or use of the info or data
- disclosure of the info or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

How can the Data Protection Act help us?

- It gives us the right to see our files
- It says those who record and use personal information must be open about how the information is used.
- It must follow the 8 principles of '*good information handling'*

Main principles of the 1998 Act

Personal data must be:

First data protection principle: fairly and lawfully processed

- Personal data shall be processed fairly and lawfully and in particular shall not be processed unless:
- at least one of the conditions in Schedule 2 is met and
- in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Second data protection principle: processed for limited purposes

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Data controllers must notify the Information Commissioner of the personal data they are collecting and the purposes for which it is being collected.

Third data protection principle: adequate, relevant and not excessive

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Many violations of this principle are due to ignorance rather than to intent to behave in a way contrary to the Act.

- Local government has a bad record of compliance with this principle, for example shops that demand to know customers' addresses when goods are not being delivered are also likely to be in breach of this principle.

Fourth data protection principle: processed in line with your rights

- Personal data shall be accurate and, where necessary, kept up to date.

Fifth data protection principle: held securely

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time.

Sixth data protection principle: measures shall be taken against unauthorized or unlawful processing of personal data & against accidental loss or damage

- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

Seventh data protection principle: transferred to countries with adequate data protection

- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth data protection principle: transferred to countries with adequate data protection

- Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Rights of Data Subjects

The 1998 Act extends this right of access so that data subjects have the right to receive:

- a description of the personal data being held;
- an explanation of the purpose for which it is being held and processed;
- a description of the people or organizations to which it may be disclosed;
- an intelligible statement of the specific data held about them;
- a description of the source of the data.

Data protection Act in Pakistan

The following Data Protection acts Exists in Pakistan:

- The electronic data protection and safety act 2005
- Prevention of Electronic Crimes Ordinance, 2007, 2008, 2009, 2012.
- Prevention of Electronic Crimes Act, 2014

Freedom of Information

- The primary purpose of the Freedom of Information Act is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information.
- The Act also provides an enforcement mechanism if the information is not made available.
- The legislation applies to Parliament, government departments, local authorities, health trusts, doctors' surgeries, universities, schools and many other organizations.

Freedom of Information Ordinance 2002

- Under the Freedom of Information law, any citizen can seek any information or record from any public body, except for information categorized by law as exempt from disclosure.
- The Right to Information Act (RTI) is an Act of the Parliament of India "to provide for setting out the practical regime of right to information for citizens" and replaces the erstwhile Freedom of information Act, 2002.
- In Pakistan, KPK and Punjab assemblies have also passed RTI acts in 2013.

****

INTERNET ISSUES

The Internet

Benefits that the internet:

- The access to all sorts of information is much easier
- It has made communications between people much cheaper and convenient
- Many types of commercial transactions are simplified and faster due to the internet
- These benefits have been made available to very many people, not just to a small and privileged group

Disadvantages of Internet:

- Illegal or inappropriate materials
- Addiction to online social networks
- Spread of Spam or Viruses

Internet related issues:

Lack Of Creativity	Abandonment Of Family	Lack Of Face To Face Communication
Internet Addiction	Privacy Disrupted	Cheating
Cyber Bullying	Insomnia	Moral Corruption
Waste Of Time	Physical Inactivity	

Laws:

- Every country has laws governing what can be published or publicly displayed
- Typically, such laws address/handle defamation, that is, material that makes unwelcome allegations about people or organizations
- They may also cover other areas such as political and religious comments, incitement to racial hatred, or the depiction of violence
- Every country has different laws
- In some countries, publication of material criticizing the government or the established religion is effectively forbidden
- While in others it is a right guaranteed by the constitution and vigorously defended by the courts
- The coming of the internet (and satellite television) has made these differences much more apparent and much more important than they used to be
- Since material flows across borders so easily, it is both much likelier that material that violates publication laws will come into a country and more difficult for the country to enforce its own laws
- The roles and responsibilities of ISPs are a central element in the way these issues are addressed
- In Europe, the position is governed by the European Directive 2000/31/EC. In the UK this directive is implemented through the Electronic Commerce (EC Directive) Regulations 2002
- According to EC Directive, Roles that an ISP may play: **mere conduit, caching, and hosting**

Role of mere conduit:

- ISP does no more than transmit data
- ISP does not:
  - initiate transmissions
  - select the receivers of the transmissions
  - select or modify the data transmitted
- ISP can store the information temporarily, provided this is only done as part of the transmission process.
- In case an ISP is acting as a mere conduit, the regulations won't hold it liable for damages or for any other criminal sanction as a result of a transmission.

Role of caching:

Caching role arise when:

- Information is subject of: automatic, intermediate and temporary storage
- for the sole purpose of increasing the efficiency of the transmission of the information to other recipients of the service upon their request
- An ISP acting in the caching role is not liable for damages or for any criminal sanction as a result of a transmission, provided that it:
  - Does not modify the information
  - Complies with conditions on access to the information
  - Complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by the industry.
  - Does not interfere with the lawful use of the technology, widely recognized and used by the industry, to obtain data on the use of information
  - Acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of transmission has been removed from the network, or access to it has been disabled, or the court or an administrative authority has ordered such removal or disablement.

Role of hosting:

- Where an ISP stores customer information, it is acting in a hosting role.
- In this case ISP is not liable for damage or criminal sanctions provided that:
  - It did not know that anything unlawful was going on
  - Where a claim for damages is made, the ISP did not know anything that will lead to something unlawful
  - When it found out that that something unlawful was going on, it immediately tried to remove the info or prevented access to it
  - The customer was not acting under the authority or the control of the service provider

Internet Service Providers:

- In the UK, the ISP is allowed to release the information and can be compelled to do so by a court
- In the USA, ISPs cannot in general be required to release the information, although they may be required to do so in the case of serious crimes

Law across National Boundaries

Criminal Law:

- Suppose that you live in country A and on your website, you publish material that is perfectly legal & acceptable in country A, but it is a criminal offence to publish in country B. In that case you can't be prosecuted in country A and it is very unlikely that you would be handover to country B. To avoid getting into trouble, you might however, be careful in not visiting country B voluntarily.

Civil Law:

- For some parts of the civil law where the position is reasonably clear cut. Any contract that involves parties from more than one country should, and usually will, state explicitly under which jurisdiction (that is, which country's laws) it is to be interpreted.
- Where **intellectual property law** is concerned, there are international agreements to which most countries are signatories so that there is a common framework, though it can be very difficult to enforce the rights in certain countries.

Defamation:

- Defamation means making statements that will damage someone's reputation, bring them into contempt, and make them disliked, and so on.
- In British law, spoken offence is called **slander** and written is called **libel** (It could be email).
- Defendant needs to prove that:
  - He was not the author, editor or publisher of the statement complained of.
  - He took reasonable care in relation to its publication
  - He did not know and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.
- If any objectionable material is published on, for example, newspaper, website etc. the complainant can take action against the publisher of the newspaper, and the editor etc.
- What if something objectionable is posted on a forum of a university?
  - When the libel is published on a web page, on the university site, the university can reasonably argue that it cannot possibly vet everything that every one of its 1,000 students puts on their personal web page.
  - It is not, in fact, publishing the pages, it is only providing an infrastructure that allows students to publish their own web pages. In the terminology used in the 2002 Regulations it is acting in a hosting role.
  - Provided, therefore, that it removed the offending material as soon as it had reason to suspect its presence and that the student was not acting under its authority or control, the university cannot be subject to an action for damages
- The First Amendment to the **United States Constitution** guarantees a right to free speech that the US courts have always been eager to defend.
- The result is that many statements that might be considered defamatory in the UK would be protected as an exercise of the right of free speech in the USA

Organization for Cybercrime:

Council of Europe approved a draft convention on 'cybercrime':

- It deals with objectionable material on the internet, criminal copyright infringement, computer-related fraud and hacking.
- There is an additional protocol relating to incitement to religious or racial hatred, to which signatories to the protocol may also sign up.

Internet Watch Foundation:

- In the UK, the Internet Watch Foundation (IWF) was set up in 1996 to monitor and, where desirable and possible, take action against illegal and offensive content on the UK internet.
- It has the support of the UK government, the police and the ISPs.

The Internet Content Rating Association:

- The Internet Content Rating Association (ICRA) is an international, independent organization whose mission is to help parents to protect their children from potentially harmful material on the internet, whilst respecting the content providers' freedom of expression.

Spam:

- Unsolicited email sent without the consent of the addressee and without any attempt at targeting recipients who are likely to be interested in its contents.
- In the UK, the directive was implemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Unsolicited email can only be sent to individuals (as opposed to companies) if they have previously given their consent.
- Sending unsolicited email that conceals the address of the sender or does not provide a valid address to which the recipient can send a request for such mailings to cease is unlawful.
- In the USA it is the responsibility of the recipient to inform the spammer that he doesn't want to receive the spam. It is legal to send spam if:
  - The person sending the spam has not been informed by the receiver that they do not wish to receive spam from that source.
  - The spam contains an address that the receiver can use to ask that no more spam be sent.
- Registration of Phone numbers:
  - Both the USA and the UK operate successful schemes that allow individuals to register their phone numbers as ones to which unsolicited direct marketing calls must not be made.
  - This should act as a model for preventing spam; indeed, the CAN SPAM Act specifically requires the Federal Trade Commission to produce plans for such a register within six months.
  - Unfortunately, the technical differences between the internet and the telephone network makes this model unlikely to work with spam.
- Spamming is easy due to forging the sender's address on an email, and also using other people's mail servers to send you mail. Due to this fact there are no reliable records that can be used to identify where the spam really came from or to stop it completely.

In most cases, use of the internet is not charged on the basis of individual communications but on the basis of connect time, so there is no recording of individual emails and it costs the same to send an email from Australia to the UK than it does to send an email to one's colleague in the next office.

COMPUTER MISUSE

Background

- In recent years, the public has been much more concerned about the misuse of the internet than about the more general misuse of computers.
- Nevertheless, crimes committed using computers form a significant proportion of so-called **white-collar crime** and it has been necessary to introduce legislation specifically aimed at such activities

Cyber Crime

- An act against the public good
- Each statute/Law that defines a crime must specifically explain the conduct that is forbidden by that statute.

- No act can be considered a crime unless it is prohibited by the law of the place where it is committed and unless the law provides for the punishment of offenders.

Computer Crime

- Computer crimes refer to the use of information technology for illegal purposes or for unauthorized access of a computer system where the intent is to damage, delete or alter the data present in the computer. Even identity thefts, misusing devices or electronic frauds are considered to be computer crimes.

The Misuse of Computers Act 1990

Categories of Misuse:

- computer fraud;
- unauthorized obtaining of information from a computer;
- unauthorized alteration or destruction of information stored on a computer;
- denying access to an authorized user;
- unauthorized removal of information stored on a computer.

Computer Fraud

Computer Fraud categories:

- Input fraud **>** Output fraud **>** Program fraud (salami-slicing)

The Law Commission defined computer fraud as:

- conduct that involves the manipulation of a computer, by whatever method, dishonestly obtain money, property, or some other advantage of value, or to cause loss.

The main offences currently covering computer fraud:

> fraud and theft; > obtaining property by deception; > false accounting;

Unauthorised Obtaining of Information

The Law Commission identified three particular abuses:

> computer hacking; >eavesdropping on a computer; >making unauthorised use of computers for personal benefit.

Historically, it has been difficult to convict anyone of computer hacking.

Under Section 1 of the Computer Misuse Act 1990, a person is guilty of an offence if:

- he causes a computer to perform any function with intent to secure access to any program or data held on any computer;
- the access he intends to secure is unauthorised;
- he knows at the time when he causes the computer to perform the function that this is the case.

SECTION 1: THE MAIN PURPOSE OF THIS SECTION IS TO DETER HACKERS!

SECTION 2: SECTION 1 + FURTHER OFFENCE

Eavesdropping involves:

– secret listening; – secret watching.

- The aim is the acquisition of information.
- Historically, there has been no right to privacy in the UK.
- The recently introduced UK Human Rights Bill incorporates the European Convention on Human Rights into UK law.
- Privacy is now recognised as a basic human right. For instance, listening to mobile telephone calls is now illegal.
- Most people who misuse computers for personal benefit are in some form of legal relationship with the owner of the computer.
- For example, an employee who does private work on their employer's computer.
- Here **employment law** can be applied. The unauthorised use of the computer is not a special issue.

Unauthorised Altering or destruction of Information

Computers store vast amounts of information about us:

>what we have in the bank; > who we call on the telephone; > what we buy in the shops; >where we travel;

Criminals who **alter or destroy** such information can be dealt with by

>the law on Criminal Damage; **>** the Computer Misuse Act 1990 section 3

The law on Criminal Damage seems to apply to physically stored data for example:

> Damage or Delete data belonging to someone **>** writing a program that damages the data on a hard disk.

But not:

>switching off a monitor so that the display can't be seen.

Unauthorised Modification

Section 3 of the Computer Misuse Act 1990 provides that a person is guilty of a criminal offence if:

- he does any act which causes unauthorised modification of the contents of a computer
- at the time when he does the act, he has the requisite intent and the requisite knowledge.

The requisite intent is an intent to cause a modification to the contents of any computer and by doing so:

- to impair the operation of any computer;
- to prevent or hinder access to any program
- to impair the operation of any such program or the reliability of any such data.

Forgery

The unauthorised alteration or destruction of data may amount to forgery.

The Forgery and Counterfeiting Act 1981 says:

- A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it, to do or not to do some act to his own or any other person's detriment.

An "instrument" is usually a written document. However, it can also be "any disk, tape, sound-track or other device on which information is stored by mechanical, electronic or other means."

E.g., A forged electronic mail message

Denying Access to an Authorised User

There are many ways to deny access to an authorised user of a computer:

- shut the machine down;
- overload the machine with work;
- tie up all the machine's terminal/network connections;
- encrypt some system files…. etc;

Various offences deal with:

- hacking;
- unauthorised obstruction of electricity;
- improper use of telecommunications services;
- unauthorised modification of computer material;

Unauthorised removal of Info. stored on a computer.

- Under the Theft Act 1968, only property can be stolen, and information is not property.
- A floppy disk is protected by law, but the information stored on it is not.

Examples 1

- A student hacks into a college database to impress his friends - **unauthorised access**
- Later he decides to go in again, to alter his grades, but cannot find the correct file - **unauthorised access with intent**...
- A week later he succeeds and alters his grades - **unauthorised modification of data**

Examples 2

- An employee who is about to be made redundant, finds the Managing Director's password; logs into the computer system using this and looks at some confidential files- **unauthorised access**
- Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - **unauthorised access with intent...**
- After asking a friend, he finds out how to delete files and wipes the main customer database - **unauthorised modification**

Reasons for Cyber Crime not being reported

It is tough to punish a Cyber-crime criminal because:

- Offences are difficult to prove
- Evidences are difficult to collect - firms usually do not cooperate with the police
- Firms are embarrassed or scared about their reputation due to hacking - particularly banks
- Employees are normally sacked or demoted
- Police lack expertise; time; money
- The Cyber-Crime is perceived as 'soft crime', as no one gets physically injured or hurt

Current situation

- Hacking has increased with time, both as a prank and as a professional crime

- A few high-profile cases are reported in the past
- **Offenders are often in other countries with no equivalent legislation**
- Some ‘international task forces’ set up but no real progress

Pakistan Cyber Crime Bill-2016

- Electronic Transaction Ordinance 2002
- Electronic / Cyber Crime bill 2007

Electronic Transaction Ordinance 2002

■ Overview

- The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
- A first step and a solid foundation for legal sanctity and protection for Pakistani E-Commerce locally and globally.
- Laid the foundation for comprehensive Legal Infrastructure.
- It is heavily taken from foreign law related to cyber crime.

Electronic/ Cyber Crime Bill 2007

Overview

- "Prevention of Electronic Crimes Ordinance, 2007" is in force now
- It was promulgated by the President of Pakistan on the 31st December 2007
- The bill deals with the electronic crimes included:
  > Cyber terrorism > Data damage > electronic fraud > electronic forgery > Unauthorized access to code
  > Cyber stalking > Cyber Spamming

Sections

Data Damage

- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section

Punishment

- 3 years
- 3 lacs

Electronic Fraud

- People for illegal gain get in the way use any data, electronic system or device or with intent to deceive any person, which act or omission is likely to cause damage or harm

Punishment

- 7 years
- 7 lacs

Electronic Forgery

- Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not.

Punishment

- 7 years
- 7 lacs

Spamming

- Whoever transmits harmful, fraudulent, misleading,
- illegal or unsolicited electronic messages in bulk to any person
- without the express permission of the recipient,
- involves in falsified online user account registration
- falsified domain name registration for commercial purpose commits the offence of spamming.

Punishment

- 6 Months
- 50,000

Types of Cyber Crimes in Pakistan

1. **Unauthorized Data Access and Interference (Sections 3, 4, and 5):**
   Criminalizes unauthorized access, interference, copying, or transmission of data through an information system.
2. **Cyber Crimes against Critical Infrastructure (Sections 6, 7, and 8):**
   Prohibits unauthorized actions or threats against critical infrastructure with the intent to coerce, intimidate, or create fear in the public.
3. **Glorification of Terrorism (Section 9):**

Penalizes the preparation or dissemination of information glorifying terrorism, or threatening to do so with the intent to coerce or create fear.

4. **Hate Speech and Terrorism-Related Information (Sections 11 & 12):**
   Criminalizes the preparation and dissemination of hate speech or information motivating terrorism, with the intention to coerce or intimidate.
5. **Electronic Forgery and Fraud (Sections 13 & 14):**
   Prohibits electronic forgery and fraud involving damage to the public, illegal claims, or fraudulent activities through interference with information systems.
6. **Manufacture or Supply of Tools for Offenses (Section 15):**
   Criminalizes the production or supply of information systems or devices intended for or believed to assist in committing offenses under the Act.
7. **Unauthorized Use of Identity Information (Section 16):**
   Addresses the unauthorized use, sale, possession, or transmission of another person's identity information.
8. **Misuse of Telecommunication Modules (Section 17):**
   Prohibits the issuance or use of certain communication modules without proper verification and authorization.
9. **Dignity of Natural Person (Section 20):**
   Criminalizes the public display or transmission of false information with the intent to harm the reputation or privacy of a natural person.
10. **Modesty of Natural Person (Section 21):**
    Addresses intentional and public display of sexually explicit content to harm or blackmail a natural person.
11. **Child Pornography (Section 22):**
    Criminalizes the production, distribution, or possession of material containing elements of child pornography.
12. **Malicious Code Distribution (Section 23):**
    Prohibits the distribution of malicious code with the intent to harm information systems or data.
13. **Cyber Stalking (Section 24):**
    Criminalizes various forms of cyber stalking, including unwanted personal interaction, monitoring, and distribution of personal content without consent.
14. **Spamming (Section 25):**
    Criminalizes the transmission of harmful, fraudulent, or unsolicited information for wrongful gain without the recipient's permission.

Summary of All Cyber Crimes:

The law addresses a range of cybercrimes, including unauthorized data access, interference with critical infrastructure, terrorism-related offenses, electronic forgery and fraud, tools manufacturing for offenses, unauthorized identity use, telecommunication module misuse, dignity and modesty violations, child pornography, malicious code distribution, cyber stalking, and spamming.