Proffesional Practices in ICT

ITC4182

Lecture 8

Chamila Karunatilake

Chamilakarunatilake@sjp.ac.lk

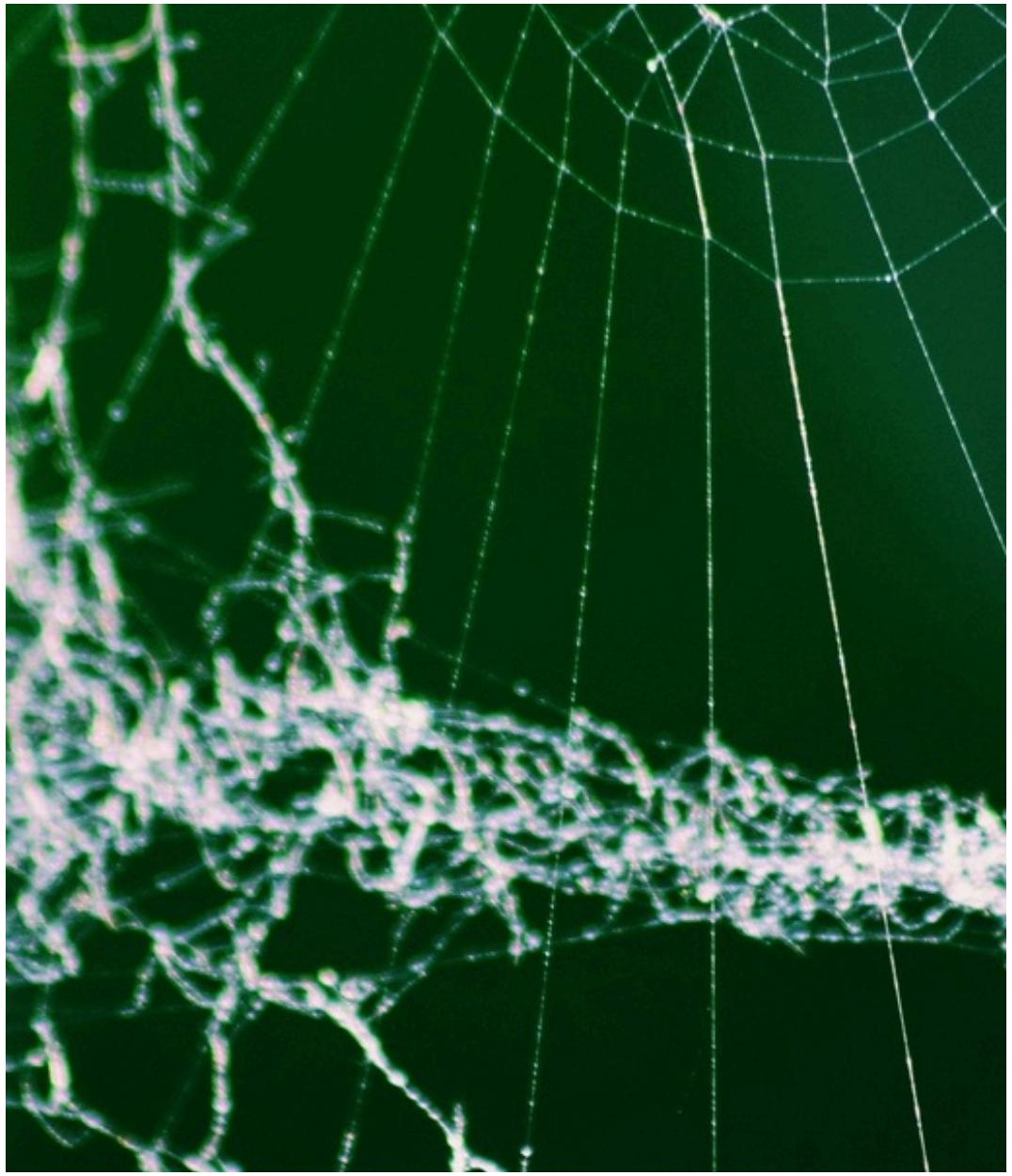
Internet Issues, Privacy, and Data Protection

"I consider data protection to be one of the most important issues of the 21st century. We need a bill of rights for the digital world!"

Tim Cook, CEO Apple, 2018

Internet Issues, Privacy, and Data Protection

The internet has become an integral part of our daily lives, connecting us to a wealth of information and services. However, with this increased connectivity, concerns about privacy and data protection have become increasingly prevalent.



Privacy in the Digital Age

Privacy on the internet and in cyberspace is a fundamental human right that has become increasingly significant as digital technologies and online activities expand.

It refers to the **ability of individuals to control their personal information and manage who has access to it, how it is used, and for what purposes.**

Data Protection

- Personal data refers to any information that can be used to identify an individual, such as their name, address, email, or phone number.
- Sensitive data, on the other hand, is a subset of personal data that requires additional protection, such as information about an individual's health, political opinions, or religious beliefs.
- The key principles of data protection, such as transparency, purpose limitation, and data minimization, ensure that personal and sensitive data is collected, used, and stored in a responsible and secure manner.

Privacy in the Internet

Personal Data

Information that identifies an individual, such as name, address, phone number, email, location data, and browsing habits. Personal data is often collected via cookies, forms, apps, and online services.

Data Collection and Usage

Organizations, governments, and cybercriminals collect data for various purposes, such as marketing, surveillance, analytics, and malicious activities. Transparency about data collection and usage is critical for maintaining trust.

Data Sharing and Third Parties

Many companies share user data with third parties, such as advertisers or affiliates, often without explicit consent from the user. This raises concerns about how securely these third parties handle data.

Digital Footprints

Every online activity, from social media posts to online purchases, contributes to a person's digital footprint. This footprint can be analyzed to reveal personal preferences, habits, and behaviors.

A digital footprint is the collection of data that a person leaves behind online

Anonymity vs. Identity

Anonymity allows users to browse or interact online without revealing their identities. Many online services, however, require identity verification, limiting users' ability to remain anonymous.

Cybersecurity Threats

Privacy breaches can occur through hacking, phishing, malware, or unauthorized access to systems. Cybercriminals often exploit weak security measures to steal personal information.

Privacy on the Internet

Importance of Online Privacy

- Online privacy is critical for safeguarding sensitive information, protecting against identity theft, and maintaining autonomy in the digital age.
- It allows individuals to express themselves freely and engage in online activities without fear of surveillance or exploitation.
- Threats to online privacy include data breaches, third-party tracking, social media surveillance, and government surveillance.
- These can lead to the loss of personal information, targeted advertising, and the compromising of individual liberties.

Challenges to Internet Privacy and Surveillance

Government Surveillance

Governments may monitor online activities for national security, leading to debates about balancing privacy and security.

Data Breaches

Organizations can suffer data breaches, exposing users' private information to unauthorized entities.

Social Media Risks

Social media platforms encourage users to share personal details, often with limited awareness of privacy risks.

Lack of Awareness

Users often consent to data collection without fully understanding the implications of their actions.

Privacy on the Internet

Privacy-Enhancing Technologies

To protect online privacy, individuals can use various privacy-enhancing technologies such as virtual private networks (VPNs), end-to-end encrypted messaging apps, and browser extensions that block trackers and advertisements.

Privacy Regulations and Policies

Governments and organizations have implemented various regulations and policies, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), to protect individual privacy rights and hold companies accountable for data privacy practices.

Protecting Privacy - Technologies and Practices

Encryption

Encrypting communications and data ensures only authorized parties can access the information.

Privacy Policies and Regulations

Laws like GDPR, CCPA, and Sri Lanka's Data Protection Act regulate how personal data is handled.

Anonymization and Pseudonymization

Techniques to protect user identities while allowing data to be used for analytics.

Privacy Tools

Tools like VPNs, ad blockers, and privacy-focused browsers (e.g., Tor) help users maintain online privacy.

Education

Teaching users about strong passwords, phishing risks, and safe online practices enhances privacy.

Privacy Regulations and Policies

- Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada
- General Data Protection Regulation (GDPR) - European Union
- California Consumer Privacy Act (CCPA) - United States
- Australia's Privacy Act 1988
- Personal Data Protection Act (PDPA) - Singapore

Key Privacy and Data Protection Cases

- **Google Spain v. AEPD and Mario Costeja González (2014)**

  The European Union's Court of Justice (CJEU) ruled that individuals have the right to request search engines to remove links to personal information that is inaccurate, inadequate, irrelevant, or excessive, establishing the 'Right to Be Forgotten' under the GDPR framework.

- **Facebook-Cambridge Analytica Scandal (2018)**

  Cambridge Analytica accessed the data of millions of Facebook users without their explicit consent to influence political campaigns, including the 2016 U.S. presidential election and the Brexit referendum. Facebook faced legal and regulatory scrutiny worldwide, resulting in a $5 billion fine by the U.S. Federal Trade Commission (FTC).

- **Schrems v. Data Protection Commissioner (Schrems I, 2015 and Schrems II, 2020)**

  Max Schrems, an Austrian privacy activist, challenged Facebook Ireland's transfer of EU user data to the U.S., arguing it lacked adequate data protection. The CJEU invalidated the Safe Harbor Agreement in 2015 (Schrems I) and the Privacy Shield Framework in 2020 (Schrems II), disrupting international data transfer mechanisms and encouraging stronger data protection measures.

- **Apple v. FBI (2016)**

  The FBI requested Apple's assistance in unlocking an iPhone used by a suspect in the 2015 San Bernardino terrorist attack. Apple refused, citing the potential creation of a 'backdoor' that could compromise the security of all iPhones, sparking a global debate about encryption, privacy, and law enforcement access.

Key Privacy and Data Protection Cases

- **Edward Snowden and PRISM Program (2013)**

  Edward Snowden, a former NSA contractor, leaked classified documents revealing global mass surveillance programs conducted by the NSA in collaboration with tech companies under the PRISM program, exposing extensive data collection practices without users' knowledge and sparking global outrage and calls for greater transparency in government surveillance.

- **Google Street View Privacy Cases**

  Google Street View cars collected Wi-Fi data (including emails and passwords) without consent while capturing images for mapping services. Governments fined Google in several countries, including Germany, Japan, and South Korea, for privacy violations, bringing attention to privacy risks associated with large-scale data collection.

- **Equifax Data Breach (2017)**

  A massive data breach exposed the personal information of 147 million people, including Social Security numbers and financial details. Equifax faced lawsuits and a $575 million settlement with the FTC, highlighting the consequences of inadequate cybersecurity measures and reinforcing the importance of corporate responsibility in data protection.

- **India's Aadhaar Privacy Case (2017)**

  The Aadhaar system, which collects biometric data for identity verification, was challenged for violating citizens' privacy. The Indian Supreme Court ruled that the Right to Privacy is a fundamental right and imposed restrictions on Aadhaar's use, shaping the discourse on privacy in developing countries and ensuring tighter regulations around biometric data usage.

Privacy Regulations and Policies in Sri Lanka

- **Sri Lanka Personal Data Protection Act (PDPA) - 2022**

  Effective Date: Gradual implementation starting 2022. Establishes a framework for processing personal data while ensuring privacy.

- **Right to Information Act (RTI) - 2016**

  Enables public access to information held by public authorities, while balancing the right to privacy.

- **Computer Crimes Act - 2007**

  Addresses unauthorized access, data breaches, and cybercrimes. Criminalizes activities like hacking and unauthorized data interception.

- **Electronic Transactions Act - 2006**

  Facilitates e-commerce and electronic communications. Ensures secure electronic records and digital signatures.

Sri Lanka's Personal Data Protection Act (PDPA) (PERSONAL DATA PROTECTION ACT, No. 9 OF 2022)

- **Protect personal data of individuals**

  The PDPA aims to protect the personal data of individuals in Sri Lanka, ensuring their privacy rights are safeguarded.

- **Establish a Data Protection Authority for enforcement**

  The PDPA creates a dedicated Data Protection Authority to monitor compliance and take action against violations.

- **Ensure responsible data processing by organizations**

  The law establishes guidelines for organizations to handle personal data ethically and transparently.

- **Align with international data protection standards**

  The PDPA seeks to align Sri Lanka's data protection regulations with global standards, such as the GDPR.

Sri Lanka's Personal Data Protection Act (PDPA) (PERSONAL DATA PROTECTION ACT, No. 9 OF 2022)

- **Comprehensive individual rights over personal data**

  The law grants individuals control over their personal data, including the right to access, correct, erase, and port their information.

- **Strict obligations for data controllers and processors**

  Organizations handling personal data must comply with legal requirements for lawful processing, security, and breach reporting.

- **Cross-border data transfer regulations**

  The PDPA restricts the transfer of personal data outside Sri Lanka, unless the receiving country has adequate data protection laws or other safeguards are in place.

- **Penalties for non-compliance**

  Violations of the PDPA can result in significant fines and legal actions, incentivizing organizations to adhere to the law.

The Computer Crime Act, No. 24 of 2007

- ## Objectives

  To define and prevent computer-related crimes. To provide a legal framework for investigating and prosecuting such offenses.

  To ensure the protection of computer systems, programs, and data from unauthorized access and misuse.

- ## Scope

  The Act applies to computer systems within Sri Lanka. Covers both citizens and non-citizens if the act involves a computer system located in Sri Lanka.

  Includes crimes committed using networks, data, and computer systems.

- ## Unauthorized Access

  Accessing a computer or computer system without authorization.

- ## Unauthorized Use of Data

  Copying, modifying, or deleting data without authorization.

- ## Unauthorized Interception

  Intercepting data in transit without the owner's consent. Penalty: Fine or imprisonment (or both).

- ## Unauthorized Modification of Data

  Modifying or deleting data to impair its integrity. Includes introducing viruses or malware into a system.

The Computer Crime Act, No. 24 of 2007

- **Denial of Service (DoS) Attacks**

  Intentionally hindering or disrupting the functioning of a computer or network.

- **Identity Theft**

  Using someone else's credentials or digital identity for illegal purposes.

- **Computer-Related Forgery**

  Forging electronic data to deceive or mislead others.

- **Computer-Related Fraud**

  Using computers to defraud others, including phishing and financial scams.

- **Violation of Confidentiality**

  Disclosing or obtaining confidential data without proper authorization.

The Computer Crime Act, No. 24 of 2007

- **Search and Seizure**

  Police can obtain a warrant to search premises and seize computers, data, or devices.

- **Access to Data**

  Authorized officers can demand access to data stored on a computer or network.

- **Preservation of Data**

  Investigators can order individuals or organizations to preserve specific data for investigation.

- **Decryption Orders**

  Individuals may be required to decrypt or provide access to encrypted data.

- **Jurisdiction**

  Offenses committed using Sri Lankan computer systems are punishable under the Act, even if the offender is outside Sri Lanka. It also applies to offenses targeting Sri Lankan systems from other countries.

- **Penalties**

  Penalties depend on the severity of the offense and may include fines and imprisonment.

- **Exemptions**

  Actions taken for legitimate security purposes or authorized penetration testing are not considered offenses.

  Exemptions also apply to cases where actions were taken in accordance with lawful instructions from authorities.

“Privacy is dead, and social media hold the smoking gun.”

Pete Cashmore, Mashable CEO

Challenges of Social Media Platforms

Privacy & Security Challenges

- **Excessive data collection**, **third-party data sharing**, and **user tracking/surveillance** lead to privacy issues.
- **Cybersecurity threats** include data breaches, identity theft, phishing, and account hacking.
- **Online harassment** and **cyberbullying**, such as trolling and hate speech, are also major concerns.

Misinformation & Fake News

- The **rapid spread of false information**, political manipulation, and health misinformation pose significant challenges.
- **Deepfakes and AI-generated content** can be used for fraud, blackmail, or propaganda, while fake profiles and bots artificially boost trends and narratives.

Psychological & Social Challenges

Social media addiction, **comparison culture**, and **FOMO** (fear of missing out) can negatively impact mental health.

Online radicalization and extremism are also growing concerns, as echo chambers and targeted recruitment by extremist groups become more prevalent.

Challenges of Social Media Platforms

- ## Business & Economic Challenges

  Negative reviews, **backlash**, and **cancel culture** can damage a company's reputation.

  Fake followers, **manipulated trends**, and **data monetization** raise ethical concerns for businesses. Targeted advertising and privacy issues also pose challenges.

- ## Legal & Ethical Challenges

  Lack of regulation, **cross-border issues**, and **platform liability** create difficulties in addressing content moderation.

  Copyright infringement, counterfeit goods, and the **balance between free speech and censorship** are other legal and ethical concerns.

- ## Emerging & Future Challenges

  AI and algorithm bias can lead to **filter bubbles** and **discriminatory content moderation**.

  The rise of the **metaverse** introduces new risks, such as **virtual harassment** and increased data collection.

  Fake and AI-generated influencers may also erode user trust in social media content.

Regulations for Social Media and the Internet

- ## Global Guidelines

  Established by international organizations such as the United Nations, these guidelines promote the responsible use of social media and the internet, addressing issues like privacy, content moderation, and data protection.

- ## Regional Regulations

  Specific policies and laws enacted by governments and regional authorities to regulate online activities, social media platforms, and internet-based services within their jurisdictions.

- ## Platform-Specific Policies

  Rules and guidelines set by individual social media and internet service providers to govern the use of their platforms, including content policies, terms of service, and community standards.

- ## User Responsibility

  Ethical principles and best practices for individuals using social media and the internet, such as respecting others' privacy, avoiding the spread of misinformation, and maintaining a positive online presence.

- ## Enforcement Mechanisms

  Processes and systems in place to monitor, investigate, and respond to violations of regulations, including reporting mechanisms, content moderation, and legal enforcement.

Safeguarding Digital Privacy and Security

Strong Passwords

Use a combination of uppercase, lowercase, numbers, and special characters to create unique and complex passwords for each account.

Two-Factor Authentication

Enable two-factor authentication on all online accounts to add an extra layer of security beyond just a password.

Secure Browsing

Use a virtual private network (VPN) and avoid public Wi-Fi networks to protect your online activities and data.

Antivirus and Anti-Malware

Install and regularly update reliable antivirus and anti-malware software to detect and prevent cyber threats.

Backup Data

Regularly backup important personal data, such as photos, documents, and financial information, to an external hard drive or cloud storage.

Safeguarding Digital Privacy and Security

Data Awareness

Understand data collection and usage, avoid unsafe links, and grant only necessary app permissions.

Responsible Engagement

Fact-check content, engage respectfully, and set boundaries for social media usage.

Organizational Measures

Implement cybersecurity protocols, practice data minimization, and ensure transparent privacy policies.

Regulatory Framework

Enact strong data protection laws, promote international cooperation, and establish content regulations.

Public Awareness

Educate the public, train professionals, and integrate digital literacy into educational curricula.

“In cybersecurity, the weakest link is often the human element.”

–Kevin Mitnick