CINEC CAMPUS
Beyond A Graduate

BSc (Hons) in Software Engineering

Course Code: GS3207
Privacy
Ethics & Professionalism

Privacy

Objectives

Introduction

privacy issues

privacy protection and the law

terminology

code of conduct and privacy issues

Learning Outcomes

- Define the concept of privacy and its significance in contemporary society.
- Recognize common privacy challenges and threats.
- Explain the legal frameworks governing privacy protection.
- Understand key privacy-related terminology and concepts.
- Analyze the consequences of privacy breaches for individuals and organizations.
- Recognize the importance of privacy in maintaining a free and democratic society.

ANONYMITY, PRIVACY, AND CIVIL LIBERTIES

Topics to be covered :

- Anonymity
- Privacy
- Ethical and social issues

The Impact of Technological Advancements on Digital Communication

- High digitalization of information and increasing bandwidth.
- Declining costs of digital communication.
- Increased miniaturization of portable computers and other communications equipment.
- Greater public awareness by the news media of the potential abuse of digital communication, especially the Internet.

Anonymity

Anonymity is the absence of identity.

Types of anonymity:

- Pseudo Identity:
  - An individual is identified by a certain pseudonym, code, or number (similar to a writer's pen name).
  - Example: Witness Protection Program.

- Untraceable Identity:
  - One is not known by any name, including pseudo names.
  - Offers a higher level of anonymity.

Anonymity

- Anonymity with a Pseudo Address:
  - Use of a pseudo address to send and receive correspondence with others.
  - Commonly used in anonymous remailers, user groups, and news groups.

Anonymity

- Internet provides two channels through which anonymous acts can be carried out:
  - Email
  - Postering

Anonymity

- Email
  - Advancements in software and hardware have enabled assured anonymity through the establishment of anonymous servers on the Internet.
  - Anonymous remailers, software programs on Internet servers, allocate users anonymous identities or pseudo addresses, ensuring anonymity.

Anonymity

- Posting
  - Anonymity can also be achieved through postings on user groups, such as bulletin boards and chat rooms.
  - Sensitive and highly personal information is sometimes posted to user groups, news groups, and chat rooms.
  - Data transmission protocols like Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP) accept messages with arbitrary field information, ensuring anonymity.

Privacy- Definition

- Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively. (wikipedia)

Definition

Privacy is a human value consisting of four elements which calls rights.

1. Control of external influences:
    - Solitude: The right to be alone without disturbances
    - Anonymity: The right to have no public personal identity
    - Intimacy: The right not to be monitored

2. Control of personal information:
    - Reserve: The right to control one's personal information including the methods of dissemination of that information

Definition

Definition of privacy depends on :

- culture,
- geographical location,
- political systems,
- religious beliefs
- and a lot more.

Type of Privacy

- Personal Privacy
- Informational Privacy
- Institutional

Personal Privacy

Individual has to keep their personal attributes confidential and free from unwanted intrusion.

- Data Privacy
  - personal information, such as name, address, phone number, financial records, and medical history.
- Physical Privacy
  - physical searches, surveillance, or eavesdropping.
- Communication Privacy
  - phone calls, emails, text messages, and video calls
- Privacy of Personal Activities
  - engage in lawful activities
- Privacy of Personal Space
  - Home or other space
- Online Privacy
  - social media profiles, online purchases, browsing history

Personal Privacy

Discuss a few of these statues and acts.

Personal Privacy Act

European Union - General Data Protection Regulation (GDPR):

- GDPR is one of the most comprehensive privacy regulations globally.
- It grants individuals significant control over their personal data, including the right to know what data is collected, how it's used, and the right to have it deleted.
- It also imposes strict requirements on organizations handling personal data, whether they are located in the EU or processing data of EU residents.

Australia - Privacy Act:

- The Privacy Act regulates the handling of personal information by Australian government agencies and some private sector organizations.
- It includes the Australian Privacy Principles (APPs), which cover the collection, use, and disclosure of personal information.

Personal Privacy Act

Japan - Act on the Protection of Personal Information (APPI):

- APPI governs the handling of personal information by businesses and government agencies in Japan.
- It establishes principles for the collection, use, and disclosure of personal data.

United Kingdom - Data Protection Act 2018:

- The UK Data Protection Act 2018 enforces the GDPR in the UK and provides additional provisions for data protection.
- It covers the processing of personal data and individual rights regarding their data.

Personal Privacy Act

India - The Right to Privacy:

- While not a specific act, the Indian Supreme Court recognized the right to privacy as a fundamental right in a landmark judgment.
- This decision has significant implications for data protection and privacy in India, leading to discussions about comprehensive privacy legislation.

Sri Lanka: The Personal Data Protection Act No. 9 of 2022 ('PDPA')

- This was passed in the Parliament of Sri Lanka ('the Parliament') in 2022.
- The PDPA provides for the mechanism and specific periods by and on which the PDPA would gradually come into force.

Issues in Personal Privacy

In today's digital age, personal information is readily shared on social media platforms. People willingly post details about their lives, but this openness comes with risks. The dilemma revolves around the tension between enjoying the benefits of social media and safeguarding one's privacy.

1. Users willingly share personal information on social media. Should individuals be held responsible for the information they choose to disclose?
2. Social media companies collect vast amounts of user data. Should there be stricter regulations on what data can be collected and how it can be used?
3. What responsibilities do social media companies have in protecting user data from breaches or misuse?

Issues in Personal Privacy

1. Users willingly share personal information on social media. Should individuals be held responsible for the information they choose to disclose?

   Yes, individuals should be responsible for what they share on social media. While platforms should protect user data, users also need to exercise discretion.

2. Social media companies collect vast amounts of user data. Should there be stricter regulations on what data can be collected and how it can be used?

   Yes, stricter regulations are needed to ensure that social media companies don't excessively collect and misuse user data without consent.

3. What responsibilities do social media companies have in protecting user data from breaches or misuse?

   Social media companies have a significant responsibility to protect user data, and stronger measures are necessary to prevent breaches.

Informational Privacy

- the protection of unauthorized access to information itself.
  - Personal information
    - religion, sexual orientation, political affiliations, or personal activities.
  - Financial information
    - Sales, income statements, cash flow, Tax records
  - Medical information
    - Medical Records, Patient health information, Diagnostic Tests and Reports
  - Internet
    - Web sites, social medias

Institutional Privacy

privacy of institutions and organizations

- for business advantages and for life of the business
- Ex: research data, the sales and product data, the marketing strategies and the activities

Value of Privacy

- Privacy is important in the information age because it guards an individual's personal identity, preserves individual autonomy, and makes social relationships possible.
- Your identity is not a secret anymore.
  - Telephone number
  - Transaction by Credit card
  - National Identification Number

Attributes of privacy

- Personal identity
  - Personal identity is valuable as it defines and distinguishes individuals from others.
  - Protecting personal identity helps maintain privacy and control over one's information.
- Autonomy
  - The level of personal information known about an individual affects their autonomy.
  - Autonomy in decision-making empowers individuals to make choices aligned with their values and desires.
- Social relationships
  - Social relationships play a significant role in various societies and cultures worldwide.
  - Individuals use this information to assess compatibility and long-term potential.

Information Gathering, Databases, and Privacy

Do you have experiences writing your NIC and telephone number and put into small box?

Do you know they have your data in their database?

Do you know most companies sell those data to third party company?

Information Gathering, Databases, and Privacy

Three requirements that the institutions must disclose to us:

- *Privacy Policy:* through which the institution is bound to tell us the types of information the institution **collects** and **has** about us and **how it uses** that information.
- *Right to Opt-Out*: through which the institution is bound to explain our r**ecourse to prevent the transfer of our data to third party beneficiaries.**
- *Safeguards*: through which the institution must put in place policies to prevent fraudulent access to confidential financial information.

Privacy Violations and Legal Implications

Fundamental right is violated every day in many ways.

Internet has accelerated the rate and scale of violations

Causes of violations

- Consumers willingly provide personal information for incentives like prizes and promotions.
- Lack of awareness about how small information disclosures can lead to significant privacy invasions.
- Inadequate privacy policies on websites and platforms.
- Companies and institutions not adhering to their own privacy policies.
- The attraction of the internet for businesses to rapidly reach individuals in the comfort of their homes or office

Major privacy violators

1. Internet companies
   - DoubleClick
   - Yahoo!, Inc
   - Universal Image, Inc
   - Universal sued Yahoo!

Type of privacy violations

- Intrusion
  - Intrusion is an invasion of privacy by wrongful entry, seizing, or acquiring possession of the property of others.
    - Ex hackers
  - With computer network globalization, intrusion is only second to viruses among computer crimes, and it is growing fast.
- Misuse of information
  - Information is used for unauthorized purposes.
  - Company collected data and sell for high bidders.

Type of privacy violations

- Interception of information
  - Unauthorized access to private information via eavesdropping
    - third party gains unauthorized access to a private communication between two or more parties
  - Information can be gathered by eavesdropping in the following areas:
    - At the source and sink of information: someone can use client or server intrusion software to intercept or "listen in" on the data being transmitted from the source (where the data originates) and the sink (where the data is received)
    - Between communication channels: It involves tapping into these channels, like intercepting telephone calls or monitoring data transmitted over a network, and then "listening in" to gather information.

Type of privacy violations

- Information matching
  - linking individual records in different databases.
  - There is no limit to what one can do with the collected information, and no one knows what the profiles built from the matched information will be used for and by whom.
  - NIC as the search key, all these databases can very easily be linked together.

Case study:

A couple of programmers at the city of Chicago's computer center began matching tape files from many of the city's different data processing applications on name and I.D. They discovered, for example, that several high-paid city employers had unpaid parking fines. Bolstered by this revelation they pressed on. Soon they uncovered the names of several employees who were still listed on the register but who had not paid a variety of fees, a few of whom appeared in the files of the alcoholic and drug abuse program. When this finding was leaked to the public, the city employees, of course, were furious. They demanded to know who had authorized the investigation. The answer was that no one knew. Later, city officials established rules for the computer center to prevent this form of invasion of privacy from happening again

Civil Liberties

- criminal justice that includes police powers, personal liberty, and the right to a fair trial;
- basic freedoms of speech, assembly, association, movement, and no discrimination;
- freedom of information;
- communications and privacy.

But there is No Civil Libertie…Due to….

- sophisticated network scanning
- spying software such as STARR, FreeWhacker, Stealth Keyboard Logger, Snapshotspy, Surf Spy, Net Spy, PC Activity Monitor

But good for law enforcement agencies like local police and FBI to track down criminals, and to banks to prevent fraud.

Structures and guidelines that safeguard and protected privacy rights.

Technical

Technical

Through the use of software and other technically based safeguards, and also by education of users and consumers to carry out self-regulation.

- Do not reveal personal information inadvertently.
- Turn on cookie notices in your Web browser, and/or use cookie management software or informdiaries.
- Keep a “clean” email address.
- Don’t reveal personal details to strangers or just-met “friends.”
- Realize you may be monitored at work. Avoid sending highly personal emails to mailing lists, and keep sensitive files on your home computer.
- Beware of sites that offer some sort of reward or prize in exchange for your contact or other information.
- Do not reply to spammers, for any reason.
- Be conscious of Web security.
- Be conscious of home computer security.
- Examine privacy policies and seals.
- Remember that you alone decide what information about yourself to reveal—when, why, and to whom.
- Use encryption!

Contractual

- Contractual and technological protection ensure which Information, such as electronic publications, and how the information can be disseminated, agai unauthorized reproduction or distribution.
- enhance security.
- beneficial for protecting special information, like publications.

Legal

Through the enactment of laws by national legislatures and enforcement of such laws by the law enforcement agencies.

legal protection instruments.
USA

- Children's Online Privacy Protection Act.
- Consumer Protection Act.
- Freedom of Information Act (1968) as amended (5 USC 552).
- Fair Credit Reporting Act (1970).
- Privacy Act (1974)
- Family Educational Right and Privacy Act (1974)
- Tax Reform Act (1976)

Legal

Sri Lanka

- Personal Data Protection Act No: 09 Of 2022
- Electronic Transaction Act
- Computer Crimes Act
- Cyber Security Bill
- Information and Communication Technology Act No.27 of 2003
- Intellectual Property Act No. 36 of 2003 (Sections related to Copyright)
- Electronic Transactions Act No. 19 of 2006
- Computer Crimes Act No. 24 of 2007
- Payment And Settlement Systems Act, No. 28 of 2005
- Payment Devices Frauds Act No.30 of 2006
- Mobile Payment Guidelines – 13_mobile_payment_2011_1e
- Mobile Payment Guidelines – 14_mobile_payment_2011_2e
- Electronic Payments to Government Institutions PF447E
- Electronic Payments by Government Institutions 02_2013E
- Use of Electronic Documents and Electronic Communication for Official Use -Circular
- Use of E-Mail and ICT in general in Government Business

Ethical and Legal Framework for Information

Ethics and Privacy

- Rapid advances in computer technology, especially the Internet, have raised ethical and privacy concerns.
- The Internet has introduced new challenges to confidentiality and data security.
- Previously, trust was placed in postal carriers, but electronic communication demands greater confidentiality.

Ethical and Legal Framework for Information

Privacy in Electronic Communication

- Confidentiality in electronic communication is a significant concern.
- The security of information transmitted over public communication channe is in question.
- Encryption protocols are crucial but raise questions about their effectivenes and strength.

Ethical and Legal Framework for Information

The Need for Frameworks

- An ethical framework is essential for addressing moral issues in information management.
- A legal framework is necessary to establish rules and regulations that protect privacy and data security.
- Both frameworks complement each other in addressing the complex issues surrounding information ethics.

Ethical and Legal Framework for Information

Development of Frameworks

- The question of who will develop these frameworks arises.
- Collaboration between governments, technology experts, legal professionals, and ethicists is required.
- Multidisciplinary efforts can lead to comprehensive and balanced frameworks.

Ethical and Legal Framework for Information

Enforcement of Frameworks

- Ensuring adherence to these frameworks is crucial for their effectiveness.
- Law enforcement agencies, regulatory bodies, and international cooperation play vital roles in enforcement.
- Properly defined penalties for violations are necessary to deter unethical or illegal behavior.

Brief of the Next Lecture

Security

Reference

Joseph Migga Kizza, Ethical and Social issues in the information age,1997

Q & A

Thank You.