# Week 7 revision notes

# IFB240 Week 7 - Privacy and Identity Theft

## Overview

This week's focus is on **privacy**, **threats to privacy**, and **identity theft**. We explore privacy concepts, the impact of privacy legislation, threats to privacy from both technology and human factors, and the methods and consequences of identity theft. The discussion also includes surveillance, data collection methods, and legal protections.

## 1. What is Privacy?

### Definition of Privacy

- **Oxford Dictionary**: Privacy is "a state in which one is not observed or disturbed by other people; the state of being free from public attention."
- **Roger Clarke**: Privacy is "the interest that individuals have in sustaining personal space, free from interference by other people and organizations."

### Dimensions of Privacy (Roger Clarke)

1. **Privacy of the Person**: Concerned with bodily integrity and consent to physical procedures.
2. **Privacy of Personal Behavior**: Includes political, religious, and sexual practices.
3. **Privacy of Personal Communications**: Ability to communicate without monitoring.
4. **Privacy of Personal Data**: Control over personal data, even when held by other organizations.
5. **Privacy of Personal Experience**: Concerns monitoring and analyzing one's experiences, such as reading, viewing, or interactions.

### Privacy Legislation in Australia

- **Commonwealth Privacy Act 1988**: Federal legislation that regulates the collection, use, and disclosure of personal information, with various amendments over time:
  - **Privacy Amendment (Private Sector) Act 2000**
  - **Privacy Amendment (Enhancing Privacy Protection) Act 2012**
  - **Privacy Amendment (Notifiable Data Breaches) Act 2017**

### Global Privacy Legislation

- **GDPR (General Data Protection Regulation)** in the European Union:
  - Based on **seven principles**, including **lawfulness, fairness, and transparency**; **purpose limitation**; **data minimization**; and **integrity and confidentiality**.
  - Recognizes individual rights such as the right **to be informed**, **to access**, **to rectify**, and **to be forgotten**.

## 2. Threats to Privacy

### How Personal Information is Collected

- **Directly**: Information like name, DOB, and address provided to an organization.
- **Indirectly**: Data collected from your interaction with technology.
  - **Web Browsing History**, **Search History**, **Transaction Records**.
  - **IoT Devices**: Smart TVs, home assistants, and other connected devices.
  - **Wearable Health Devices**: Track health-related metrics and contribute to personal data profiles.

### Examples of Privacy Threats

- **Real-World Privacy Breaches**:
  - **Red Cross Data Breach (2016)**: Unauthorized disclosure of patient information.
  - **Optus Cyber Attack (2022)**: Affected 10 million customers, highlighting vulnerabilities.
  - **Pareto Phone Breach (2023)**: Donor information from multiple Australian charities was leaked on the dark web.

### People and Their Actions

- **Accidental Actions**:
  - **Human Error**: Such as the insecure disposal of medical records or accidental email leaks.
  - **Social Media Disclosure**: Sharing sensitive information unintentionally.
- **Deliberate Actions**:
  - **External Criminals**: Motivated by financial gain (e.g., identity theft).
  - **Insider Threats**: Employees with access to sensitive information can intentionally misuse it.
- **Technology-Driven Threats**:
  - **Malware**: Trojans and keyloggers are commonly used to capture personal information.
  - **Social Engineering**: Techniques such as phishing to trick individuals into providing sensitive data.

### Surveillance and Privacy

- **Government Surveillance**: Often justified as being "in the national interest." For instance, COVID-19 tracking.

- **Technology and Data Collection**:
  - **Location Data**: Collected from GPS and IoT devices.
  - **Social Media**: Monitors interactions, inferring relationships and behaviors.
  - **Keystroke Loggers**: Captures everything typed on a keyboard, used by attackers to gather passwords and personal information.

# 3. Identity Theft

## What is Identity Theft?

- **Definition**: Identity theft is a crime where someone uses another person's key personal information to impersonate them fraudulently.

## Reasons for Identity Theft

- **Gain Benefits**: Obtain loans, use credit cards, access services.
- **Avoid Penalties**: Use someone else’s identity to avoid legal repercussions.

## Methods to Steal Personal Information

- **Dumpster Diving**: Digging through rubbish to find personal documents.
- **Raiding Mailboxes**: Gaining access to important identification details.
- **Social Engineering and Phishing**: Fake emails, phone calls, online quizzes.
- **Malware Attacks**: Using trojans or other software to gain access to a user’s information.

## Real-World Examples

- **Melbourne Bank Scam (2022)**: A woman was sentenced for stealing identities to carry out bank fraud.
- **Jim's Case (2023)**: A person had their identity stolen, leading to emptied bank accounts, forcing them to consider changing their name.

## Consequences of Identity Theft

- **Financial Loss**: Victims may face debt accrued in their names.
- **Damage to Reputation**: Victims may be blamed for actions they didn’t commit, leading to legal complications.
- **Emotional Stress**: Dealing with identity theft often takes a toll on the mental well-being of victims.

## How to Detect Identity Theft

- **Unexpected Bills**: Receiving bills or fines for things you didn’t purchase.
- **Bank Statement Monitoring**: Regular checks can reveal unauthorized transactions.

- **Scamwatch**: Online tools like SCAMWatch can help identify potential phishing scams and other suspicious activities.

### What to Do If It Happens

- **Data Breach Notification Requirements**: Under Australian Privacy Law, organizations are required to notify affected individuals.
- **Reporting**: Report the incident to relevant authorities like the **Australian Information Commissioner** and **ACSC** (Australian Cyber Security Centre).
- **Seek Support**: Organizations like **IDCare** can provide assistance in recovering your identity.

## 4. Privacy Tools and Threats from Technology

### Cookies

- **Definition**: Small text files stored on a user's device by a website.
- **Persistent Cookies**: Remain after the browser is closed.
- **Non-Persistent Cookies**: Active only during a session.
- **Use Cases**:
  - **Session Management**: Track user sessions for continuity.
  - **Personalization**: Customize content and ads based on user preferences.

### Web Bugs (Pixel Tags)

- **Definition**: Small, often invisible images used to track user behavior.
- **Purpose**: Helps website owners understand how visitors interact with the site.

### Browser Fingerprinting

- **Alternative to Cookies**: Uses device characteristics (e.g., screen resolution, plugins) to identify users.
- **Implication**: Even without cookies, users can be tracked across the web.

### Government Surveillance and Metadata

- **Data Retention Laws (2017)**: Requires telecom companies to keep metadata for government access.
  - **Metadata**: Data about data; e.g., information about phone calls or emails but not the content itself.
- **Surveillance Implications**:
  - **National Security**: Helps law enforcement track activities.
  - **Privacy Concerns**: Raises questions about privacy and individual rights.

## 5. Summary

- **Privacy** is about controlling personal information and protecting it from unauthorized access.
- **Threats to Privacy** include deliberate and accidental human actions and the use of surveillance technologies.
- **Identity Theft** is a growing concern, with significant consequences for victims, requiring vigilance in how personal data is handled and monitored.
- **Technology's Role**: Cookies, web bugs, and other tracking tools help in personalization and business operations but also pose privacy threats.

### Key Takeaways

- Understand **privacy rights** and stay informed about **privacy legislation**.
- Regularly **monitor financial statements** and **data usage** to detect identity theft.
- Use privacy-enhancing tools like **ad blockers**, **incognito browsing**, and be cautious with **personal data** shared online.

These enhanced notes aim to provide a solid understanding of privacy and identity theft, emphasizing how individuals can protect their information and the broader implications of privacy in technology and surveillance.