Computer Security Law

Introduction to Computer Security

Naercio Magaia and Imran Khan

Contents

- Cybercrime and computer crime
  - Types of computer crime
  - Law enforcement challenges
  - Working with law enforcement
  - UK Computer Misuse Act
- Intellectual property
  - Types of intellectual property
  - Intellectual property relevant to network and computer security
  - UK Copyright Designs and Patents Act
  - Digital millennium copyright act
  - Digital rights management
- Privacy
  - Privacy law and regulation
  - GDPR and Data Protection Act
  - Organizational response
  - Computer usage privacy
  - Privacy, data surveillance, big data, and social media

"Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity."

--From the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the **role that the computer plays** in the criminal activity:

Computers as targets

Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Computers as storage devices

Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

Computers as communications tools

Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Cybercrimes Cited in the Convention on Cybercrime

- Budapest Convention on Cybercrime, entered into European law in 2004
- Accepted by US in 2008 and recognized by 65 countries
- Requires countries to implement **legislation** to ensure the crimes are illegal in the state

Article 2 Illegal access
The access to the whole or any part of a computer system without right.

Article 3 Illegal interception
The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference
The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference
The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices
a The production, sale, procurement for use, import, distribution or otherwise making available of:
  i A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
  ii A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and
b The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery
The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud
The causing of a loss of property to another person by:
a Any input, alteration, deletion or suppression of computer data;
b Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Cybercrimes Cited in the Convention on Cybercrime (page 2 of 2)

Article 9 Offenses related to child pornography

a Producing child pornography for the purpose of its distribution through a computer system;
b Offering or making available child pornography through a computer system;
c Distributing or transmitting child pornography through a computer system;
d Procuring child pornography through a computer system for oneself or for another person;
e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Law Enforcement Challenges

- The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution
- Law enforcement agency difficulties:
  - **Lack of investigators knowledgeable and experienced** in dealing with this kind of crime
  - Required technology may be beyond their **budget**
  - The global **nature of cybercrime**
  - **Lack of collaboration and cooperation** with remote law enforcement agencies
- Convention on Cybercrime introduces a **common terminology for crimes** and a framework for harmonizing laws globally

Cybercriminals

The lack of success in bringing them to justice has led to an **increase in their numbers, boldness**, and the global scale of their operations

Are difficult to profile

Tend to be **young and very computer-savvy**

Range of behavioral characteristics is wide

No cybercriminal databases exist that can point to likely suspects

Cybercrime Victims

Are influenced by the **success of cybercriminals** and the lack of success of law enforcement

Many of these organizations **have not invested sufficiently** in technical, physical, and human-factor resources to prevent attacks

Reporting rates tend to be low because of **a lack of confidence in law enforcement, concern about corporate reputation, and a concern about civil liability**

Working with Law Enforcement

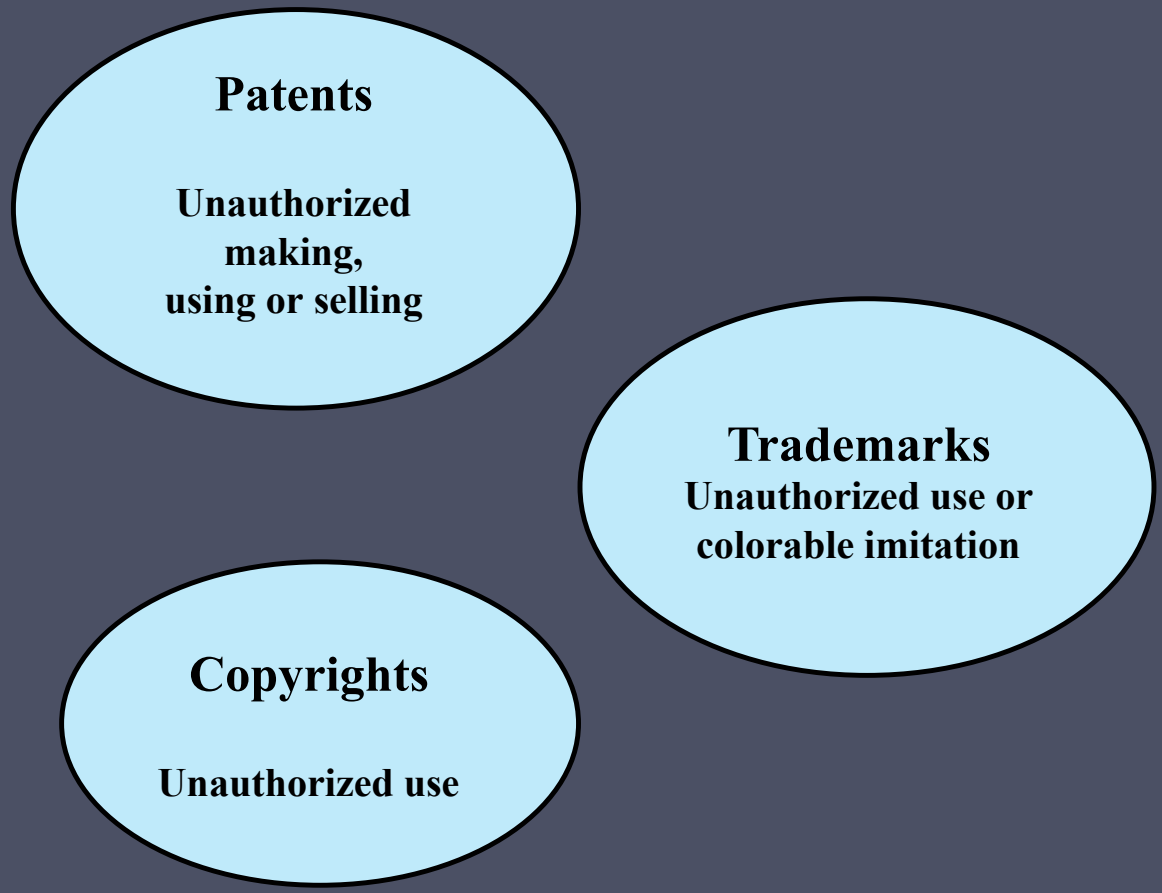
- Executive management and security administrators need to look upon law enforcement as a resource and tool
- Security practitioners needs to:
  - Understand the **criminal investigation process**
  - Understand the **inputs that investigators need**
  - Understand **the ways in which the victim can contribute** positively to the investigation

UK Computer Misuse Act 1990

- Key law to control hacking and malware
- Section 1 – causing a computer to perform a function with intent to **secure unauthorised access** to computer material, e.g., attempting to crack passwords
- Section 2 - unauthorised access with intent to **commit or facilitate commission of further offence**, e.g., phishing, fraud, etc.
- Section 3 - unauthorised acts with intent to **impair the operation** of a computer, e.g., DDoS.
- Section 3ZA - unauthorised acts **causing, or creating risk of, serious damage**, for example, to human welfare, the environment, economy or national security. This section is aimed at those who seek **to attack the critical national infrastructure**.
- Section 3A - making, supplying or obtaining articles for use in offences contrary to sections 1, 3 or 3ZA. Section 3A deals with those who **make or supply malware**.

Intellectual Property

- Much low-level cyber law breaking is around intellectual property
- Organisations will attempt to stop Intellectual Property crime such as cyber-piracy for reputational reasons



Copyright

- Protects **tangible or fixed expression of an idea** but not the idea itself
- Creator can claim and file copyright at a national government copyright office if:
  - Proposed work is original
  - Creator has put original idea in concrete form

Copyright Rights

- Copyright owner has the following exclusive rights, protected against infringement:
  - Reproduction right
  - Modification right
  - Distribution right
  - Public-performance right
  - Public-display right
- Examples include:
  - Literary works
  - Musical works
  - Dramatic works
  - Pantomimes and choreographic works
  - Pictorial, graphic, and sculptural works
  - Motion pictures and other audiovisual works
  - Sound recordings
  - Architectural works
  - Software-related works

Patent

- Grant a property right to the inventor
- "The right to exclude others from making, using, offering for sale, or selling" the invention in a region or "importing" the invention into a region
- Regional protections require registration in each region – UK, Europe, US, etc.
- Types:

Utility	Design	Plant
• Any new and useful process, machine, article of manufacture, or composition of matter	• New, original, and ornamental design for an article of manufacture	• Discovers and asexually reproduces any distinct and new variety of plant

Trademark

- A word, name, symbol, or device
- Used in trade with goods
- Indicates source of goods
- Distinguishes them from goods of others
- Trademark rights may be used to:
  - Prevent others from using a **confusingly similar mark**
  - But **not to prevent others** from making the same goods or from selling the same goods or services under a clearly different mark

adidas®

i'm lovin' it®

Intellectual Property Relevant to Network and Computer Security

- A number of forms of intellectual property are relevant in the context of network and computer security
- Examples of some of the most prominent:

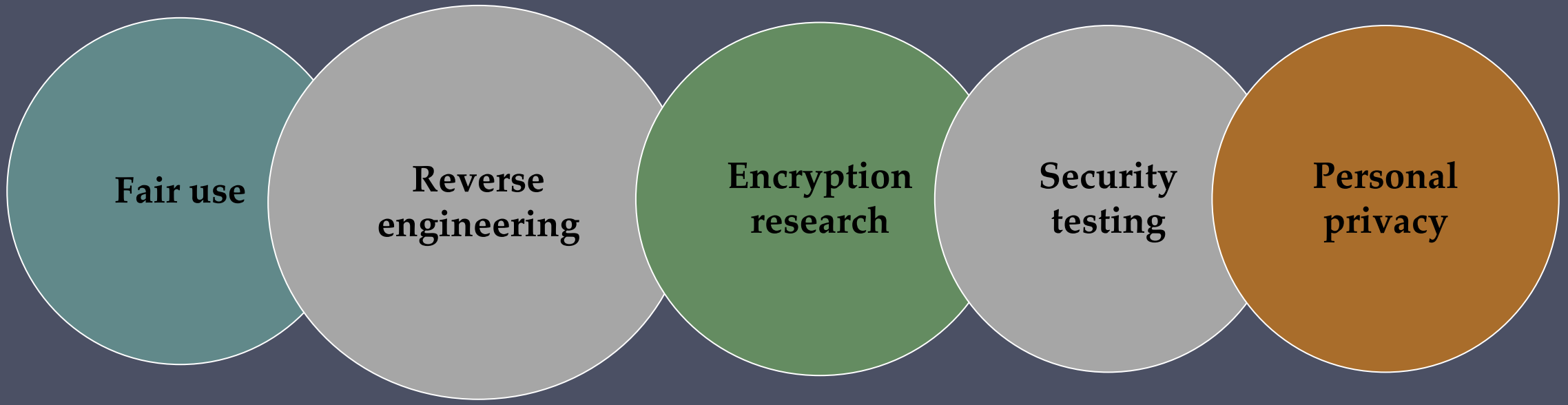
Software	Databases	Digital content	Algorithms
• Programs produced by vendors of commercial software • Shareware • Proprietary software created by an organization for internal use • Software produced by individuals	• Data that is collected and organized in such a fashion that it has potential commercial value	• Includes audio and video files, multimedia courseware, Web site content, and any other original digital work	• An example of a patentable algorithm is the RSA public-key cryptosystem

Relevant UK Acts on Intellectual Property

- **Copyright Designs and Patents Act 1988** provides protection against cyber piracy of music, films, e-books, and similar.
- **Trademarks Act 1994** provides trademark infringement protection and is the major protection against counterfeiting goods.
- **US Digital Millennium Copyright Act 1998** (**DMCA**) implements World Intellectual Property Organization (WIPO) treaties to strengthen protections of digital copyrighted materials
  - Encourages copyright owners **to use technological measures to protect** their copyrighted works
    - Measures that prevent access to the work
    - Measures that prevent copying of the work
- Used as the basis of take-down notices

DMCA Exemptions

- Certain actions are exempted from the provisions of the DMCA and other copyright laws including:



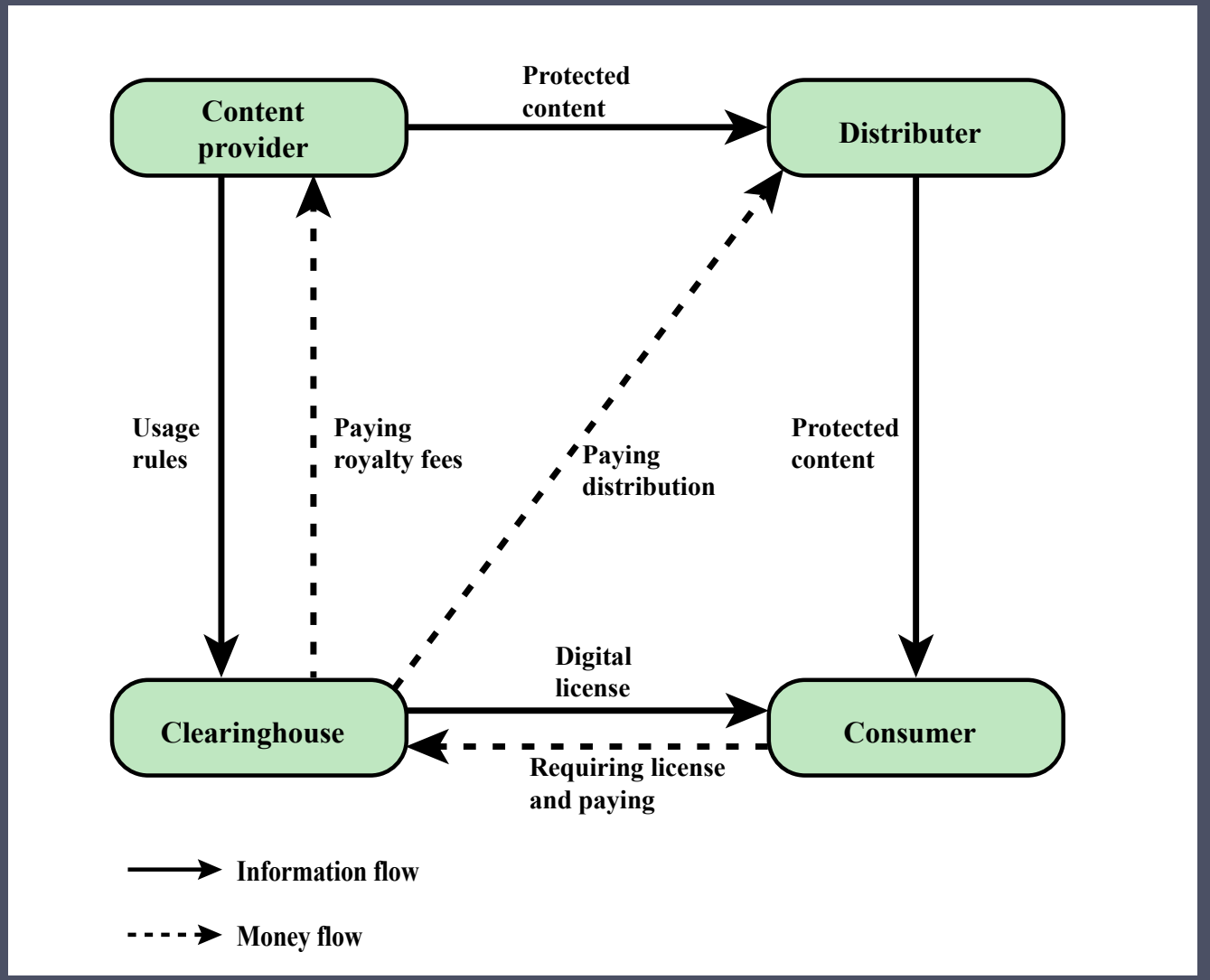
- Considerable concern exists that DMCA **inhibits legitimate security and encryption research**
  - Feel that innovation and academic freedom is stifled, and open-source software development is threatened

Digital Rights Management (DRM)

- Systems and procedures that **ensure that holders of digital rights are clearly identified and receive stipulated payment** for their works
  - May impose further restrictions such as inhibiting printing or prohibiting further distribution
- No single DRM standard or architecture
- Objective is to provide mechanisms for the complete content management life cycle
- Provide persistent content protection for a variety of digital content types (e.g., music files), platforms (e.g., mobile phones), and media (e.g., CD-ROMs)

DRM Implementation

- **Content provider**: Holds the digital rights of the content and wants to protect these rights.
- **Distributor**: Provides distribution channels, such as an online shop or a Web retailer
- **Consumer**: Uses the system to access the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license.
- **Clearinghouse**: Handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees



Privacy

- Overlaps with computer security
- Dramatic increase in scale of information collected and stored
  - Motivated by law enforcement, national security, economic incentives
- Individuals have **become increasingly aware of access and use** of personal information and private details about their lives
- Concerns about **extent of privacy compromise** have led to a variety of legal and technical approaches to reinforcing privacy rights

European Union (EU) Directive on Data Protection

- Adopted in 1998 to:
  - Ensure member states **protect fundamental privacy rights** when processing personal information
  - Prevent member states from **restricting the free flow** of personal information within EU
- Implemented as the **General Data Protection Regulation (GDPR)**, through Data Protection Act 2018
- Organized around principles of:

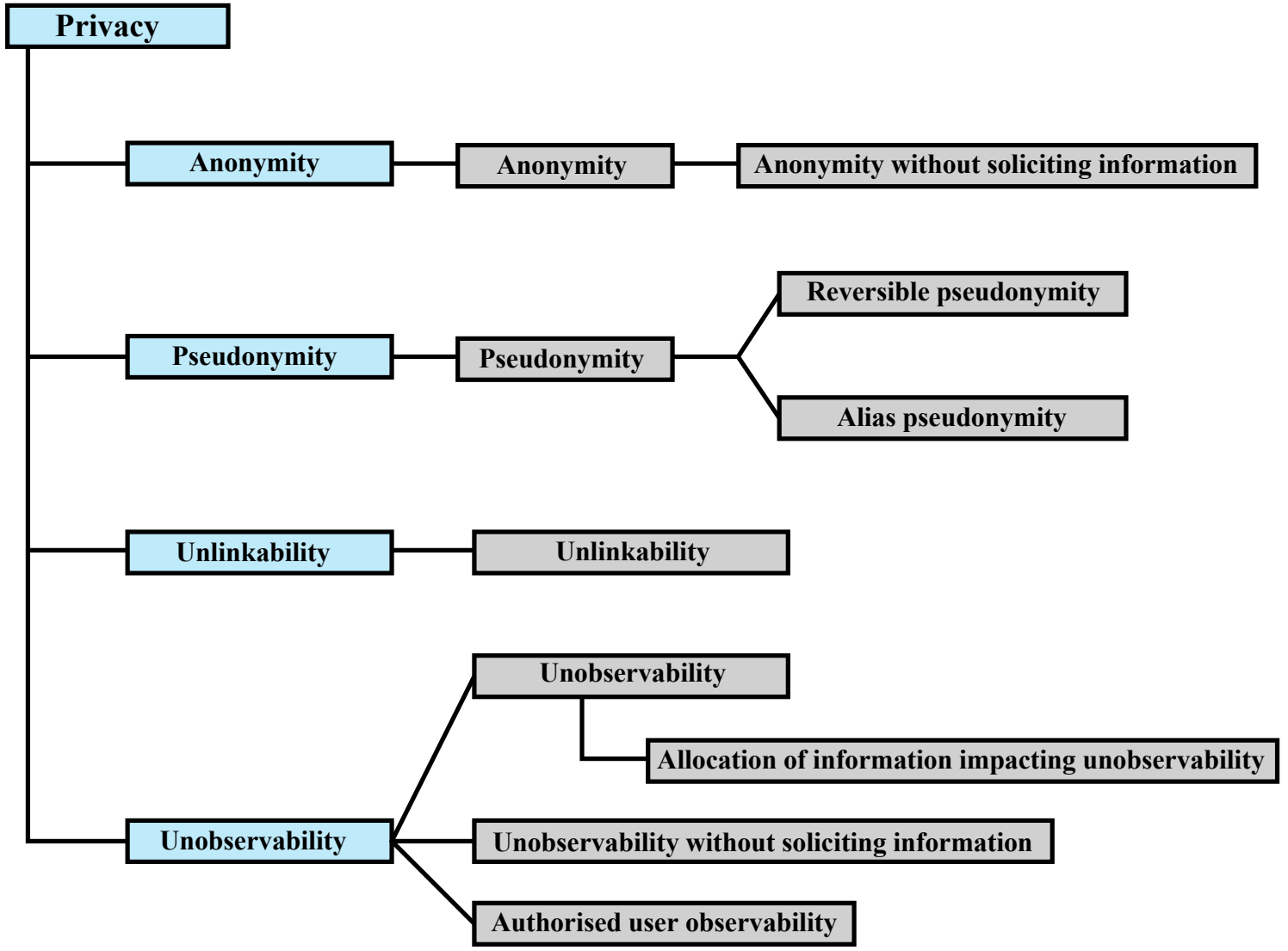
Notice	Consent	Consistency	Access
Security	Onward transfer	Enforcement	

Code of Practice for Information Security Management, ISO 27002

"An organization's data policy for privacy and protection of personally identifiable information **should be developed and implemented**. This policy **should be communicated** to all persons involved in the processing of personally identifiable information. Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires **appropriate management structure and control**. Often this is best achieved by the **appointment of a person responsible**, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles **should be dealt with in accordance** with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented."

Privacy Common Criteria

- **Anonymity:** no identity information
- **Pseudonymity:** an accountable identity indirectly linked to real identity
- **Unlinkability**: Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- **Unobservability**: Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.



Privacy and Data Surveillance

- The demands of big business, government and law enforcement have created new threats to personal privacy
  - Scientific and medical research data collection for analysis
  - Law enforcement data surveillance
  - Private organizations profiling
  - This creates tension between enabling beneficial outcomes is areas including scientific research, public health, national security, law enforcement and efficient use of resources, while still respecting an individual's right to privacy
- Another areas of particular concern is **the rapid rise in the use of public social media sites**
  - These sites **gather, analyze, and share** large amounts of data on individuals and their interactions with other individuals and organizations
  - Many people **willingly upload** large amounts of personal information, including photos and status updates
  - This data could potentially be used by current and future employers, insurance companies, private investigators, and others, in their interactions with the individual

Privacy Protection

- Both **policy and technical approaches** are needed to protect privacy
- In terms of technical approaches, the requirements for privacy protection for data stored on information systems can be addresses in part using the technical mechanisms developed for database security
- With regard to social media sites, technical controls include:
  - The provision of **suitable privacy settings** to manage who can view data on individuals
  - Notification when one individual **is referenced or tagged** in another's content
  - Although social media sites include some form of these controls, they are constantly changing, **causing frustration** for users who are trying to keep up with these mechanisms
- Another approach for managing privacy concerns in big data analysis is to **anonymize the data**, removing any personally identifying information before release to researchers or other organizations for analysis

Summary

- Cybercrime and computer crime
  - Types of computer crime
  - Law enforcement challenges
  - Working with law enforcement
  - UK Computer Misuse Act
- Intellectual property
  - Types of intellectual property
  - Intellectual property relevant to network and computer security
  - UK Copyright Designs and Patents Act
  - Digital millennium copyright act
  - Digital rights management
- Privacy
  - Privacy law and regulation
  - GDPR and Data Protection Act
  - Organizational response
  - Computer usage privacy
  - Privacy, data surveillance, big data, and social media