Professional Skills and Issues

Definitions

- Computer misuse: unauthorised access to any computer
- Anonymisation: decoupling identification from information (hard af)
- Generalisation: reducing precision of data to reduce the likelihood of informing identity
- Suppression: making less data available to an attacker to reduce inferences
- Dummy addition: adding fake data points to data sets, prior to providing to another party
- Perturbation: adding noise to data to reduce the ability of another party to form inferences
- Internet Service Provider (ISP): provides access to the Internet for its customers
- Defamation: communication of a false statement which harms the reputation of an individual, group or organisation
- Spam: unsolicited email, sent without consent of recipients, and with no attempt to target only recipients likely to be interested
- Cyber squatting: registering someone else's trade mark as your own domain name, then offering to sell them the domain name at an inflated price
- Negative rights: rights demanding someone to not perform an activity
- Contract: agreement between two or more parties that can be enforced in court
- See Data Protection Act Terminology
- See CIA Traid
- See Risk Management
- See Intellectual Property Rights

EU Law

- EU law deems adult pornography as lawful, given it is non-violent, consensual and inaccessible to children

European Directive on Data Protection 1995

- Fuck all covered, but was mentioned

Directive 2000/31/EC

- Define 3 types of Internet Service Provider
  - Mere Conduit: simply transmits data uploaded/downloaded by the customer
  - Caching: temporarily caches downloaded data for faster future downloads
  - Hosting: permanently stores data uploaded by customer
- Liability for damages and criminal actions
  - Conduit: not liable at all
  - Caching: not liable given cached data is removed/blocked if an authority orders its removal/blocking, or the original data has been removed/blocked
  - Hosting: not liable given:
    - it is unaware that unlawful data has been uploaded
    - it removes/blocks unlawful data as soon as it is discovered
    - the customer who uploaded the unlawful data was not acting on Internet Service Provider's authority
- Unlawful data's definition is determined by the government of the country is Internet Service provider is based (e.g. the Internet Watch Foundation in the UK)

EC Directive on Privacy and Electronic Communications 2002

- Unsolicited emails can be sent to individuals only with prior consent
- Unsolicited emails must not conceal the sender's true address

Directive 2013/40/EU

- On attacks against information systems
- Establish minimum rules and regulations across members states

Directive 2016/934

- Provide protection of undisclosed know-how and business info (trade secrets)

General Data Protection Regulation 2018

- GDPR
- Data protection and privacy law
- Covers all individuals in the EU and European Economic Area
- Supersedes European Directive on Data Protection 1995
  - Since not directive, becomes enforcible without national legislation
- 99 articles, in 11 chapters

Principles

- lawfulness, fairness & transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity & confidentiality
- accountability

Rights of Data Subjects

1. Right to be informed
    - Specifically about collection & processing of personal data, as well as retention period and shared access
2. Right to access
    - Specifically the confirmation of the existence of their personal data and a copy of it
3. Right to rectification
    - Specifically inaccurate personal data can be altered and completed
4. Right to erasure
    - Specifically data no longer required for collected purposed can be erased, or placed beyond use in backups
5. Right to restrict processing
    - Specifically restrict processing for time period while data is adjusted or verified
6. Right to data portability
    - Specifically personal data can be obtained and utilised across services by the individual
7. Right to object
    - Specifically to the processing of data
8. Rights in respect to automated individual decision making including profiling
    - Specifically individuals must be made aware of such processes and have to opportunity to challenge or request human involvement

Scope

- Covers both automated digital processing, but also structured data on paper
- Applies to controllers and processors established in the EU, even if processing occurs elsewhere
- Applies to data subjects in the EU, even if the processor or controller are elsewhere
- Does not cover all aspects of personal data
- Does not apply when activities are outside the EU

- Does not apply when activities concerning foreign policy held by public authority
- Does not apply to individuals in day-to-day private activities

Restricted transfer

- Non-EU countries have restricted transfer of data from the EU

Adequacy Decision

- If country has adequacy decision, data transfer is permitted to the country
- European Commission determines if non European Economic Area countries have appropriate safeguards
- Largely boils down to abides by GDPR
- New Zealand and Switzerland have such decisions

Exceptions

- Data transfer can be permitted to country without Adequacy Decision if transfer meets an exception and is not a normal operations
- Exceptions include:
  1. Individuals have given explicit consent after being advised of the risks from the lack of adequacy decisions and appropriate safeguards.
  2. Contract between parties and a restricted transfer may occur to fulfil the contract
  3. Contract between parties, that benefits other, than a restricted transfer may occur to fulfil the contract
  4. Restricted transfer necessary in the public interest
  5. Restricted transfer necessary for initiation, exercise or defence of legal clam
  6. Restricted transfer necessary to protect vital interests of individual and they must be incapable of giving consent (e.g. threat to life)
  7. Restricted transfer from a public register (e.g. criminal convictions)
  8. One-off restricted transfer for which you have compelling and legitimate interests

European Patent Convention

- Areas excluded from patent:
  - anything covered by copyright
  - scientific theories
  - mathematical methods
  - methods and programs

UK Law

- No particular law for computer fraud as covered by existing anti-fraud laws

Unfair Contract Act 1977

- Liability-limiting terms are enforcible by law if they are reasonable
- If a person is injured by a fault in safety-critical software, the supplier of the software is **always** liable

Sale of Goods Act 1979

- Sold goods must be fit for purpose
- This includes software
- Unclear with software downloaded over the Internet

Data Protection Act 1984

- Protect individuals from large organisations misusing data
- Protect from use of:
  - inaccurate personal data
  - incomplete personal data
  - irrelevant personal data
  - personal data by unauthorised persons
  - personal data for purposes other than those for which it was collected

Terminology

- Data: information that is collected or processed
- Personal data: data what relates to a living person who can be identified
- Data subject: person that data refers to
- Data controller: person within an organisation who determines how or why personal data is processed
- Processing: obtaining, recording or holding information or data, or carrying out operations on it
- Information Commissioner: government-appointed official responsible for enforcing DPA
- Sensitive personal data (has stricter rules for processing):
  - racial group
  - ethnic group
  - political views
  - religious views
  - physical health
  - mental health
  - sexual orientation
  - criminal record - including allegations

- genetic information

Principles

1. Personal data shall be processed fairly and lawfully and in particular shall not be processed unless (a) [the data subject grants consent], and (b) in the case of sensitive data, [the data subject grants explicit consent].
   - Opting out is **not** explicit consent
2. 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.
   - E.g. individuals' medical records may not be used in research without explicit consent.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to data.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose
   - E.g. Financial data must be kept for 7 years, for auditing and taxation.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
   - Data subjects are entitled to be told
     - what data is held about them
     - why the data is held
     - which other organisations may have access to the data
7. Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.
   - E.g. secure backups of personal data.
8. Personal data shall not be transfered 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 processing of personal data.
   - Safe-harbour agreements are no valid for this

Computer Fraud and Abuse Act 1986

- Covers
  - unauthorised access to any protected computer
  - distribution on malicious code
  - denial of service attacks
  - trafficking in passwords
- Has harsh penalties
  - Up to 10 years for first offence
  - Up to 20 years for repeat offences
  - Can be treated as terrorism

Copyright, Design and Patents Act 1988

- CDPA
- Copyright infringement is:
  - a civil offence if done for individual reasons
  - a criminal offence if done for commercial reasons
- Protects the following for up to 70 years after the author's death:
  - original literary works
  - original dramatic works
  - original musical works
  - original artistic works
  - sound recordings
  - films
  - TV Programmes
- Software is deemed to be literary work (not including boilerplate code)
- If authorised to sue a program, one can:
  - make **1** backup copy of the program
  - decompile the program to fix bugs
  - decompile the program to understand how to create a program to inter-operate with the original program
- Database special cases:
  - protected if contents are author's own intellectual creation
  - protected for up to 15 years if contents are purely factual, but required substantial investment in order to collect the data
- Patents can only be granted if the invention is:
  - new
  - inventive
  - capable of industrial application
  - not in an excluded area (See European Patent Convention)

Computer Misuse Act 1990

- 3 new criminal offences
  1. unauthorised access to any program/data held in any computer
  2. as above, with intent to commit a serious crime
  3. unauthorised modification of the contents of any computer
- Applies to anyone who accesses a UK computer, even if the person accessing is not in the UK
- Applies to anyone in the UK accessing a non-UK computer
- Infrequent convictions with lenient penalties so far
- Companies often hide attacks to avoid drawing attention to their security weaknesses
- Can be exempted if have a warrant

Trade Marks Act 1994

- Defines trade mark as "any sign capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from those of other undertakings. A trade mark may, in particular, consist of words (including personal names), designs, letters, numerals or the shape of goods or their packaging."
- Must be registered with the UK Intellectual Property Office

Data Protection Act 1998

- Covers stored data and Internet data
- Conforms to European Directive on Data Protection 1995
- Doesn't only apply to large organisations

Public Interest Disclosure Act 1998

- PPIDA
- Provides protection for the disclosure of:
  - criminal offenses
  - failure to comply with legal obligations
  - danger to health and safety
  - environmental damage
  - concealment of the above
- Protects the "whistle-blower"
- Whistle-blower must first approach employer, then professional body or public official
- Must not approach the media
- This overrides obligation of confidence

Regulation of Investigatory Powers Act 2000

- Regulate monitoring of postal, phone and computer communication
- Public agencies (police, intelligence,...) can intercept communications, only if preventing or detecting serious crimes
  - Requires warrant from senior official
- Communication service providers (ISPs, Mobile carries,...) can intercept communications, only for specific legitimate reasons
  - Ensuring compliance with organisation's regulations and procedures
  - Upholding standards (monitoring calls for training purposes, ...)
  - Preventing or detecting crime
  - Investigating or detecting unauthorised use of communication systems
  - Etc...
  - Users must be informed interceptions may take place
- Has be criticised for both being to invasive and not invasive enough

Freedom of Information Act 2000

- Provides clear rights of access of information held by bodies in the public sector
- Allow anyone to apply for access to said information

Police and Justice Act 2006

- Increase max penalties for Computer Misuse Act
- Amend Computer Misuse Act to cover:
  - intent to impair operation of any computer
  - software tools intended to facilitate computer misuse
- Add 2 new offences
  1. Denial-of-service attacks
  2. Building or selling hackers' toolkits

Investigatory Powers Bill 2015

- Extends Regulation of Investigatory Powers Act
- Covers all types of electronic communication
- Communication service providers must retain data for 12 months
- Warrants must be approved by a judge

UK Data Protection Act 2018

- Supplements GDPR
- Does **not** transpose GDPR into UK law

Internet Watch Foundation

- Judges if data is unlawful
- Unlawful data includes:
  - defamatory material
  - child abuse images
  - unlawful adult material
- If hosting Internet Service Provider is outside the UK, the Internet Watch Foundation asks UK Internet Service Providers to block access to its unlawful content

US Law

- No comprehensive data protection law
- Patchwork of state law
- Safe-harbour agreements
  - Since 2010
  - US companies sign up to abide by EU data protection laws

  - Annual manual self-certification
  - Deemed invalid in 2015 by EU
- EU-US Privacy Shield
  - US companies self-certify, demonstrate EU data protection law compliance and cooperate with EU authorities
  - The EU aims to provide greater transparency about data transfer to the US
- US law has no distinction between a hosting Internet Service Provider and a mere conduit
- US law protects pornography under its right to freedom of speech

CIA Triad (ISO/IEC27000)

- Confidentiality: information is not made available or disclosed to unauthorised individuals, entities or processes
- Integrity: Accuracy and completeness
- Availability: being accessible and usable upon demand by an authorised entity

Economic Espionage Act 1996

- Counter trade secret theft

CAN-SPAM Act 2003

- Spam is lawful if the sender has not asked the sender to stop and the email contains a valid email address to request the sender to stop
- Does not require prior consent
- Spammers can be imprisoned, fined and sued

Risk Management

- Activities to coordinate efforts and employees with regards to risk
- Build atop frameworks and principles

Possible outcomes

- Intolerable risk: elements need to be abandoned, replaced or evolved to reduce vulnerabilities
- Tolerable risk: risks have been reduced using solutions to as long as reasonably possible
- Acceptable risk: risk reduction not needed

Risk types

- Routine risks: normal decision process that makes use of stats and data to inform decisions
- Complex risks: less obvious, may need to gather more evidence and perform cost analysis
- Uncertain risks: lack of predictability, need to monitor impact and possibly role back any solutions
- Ambiguous risks: stakeholders interpret risk differently, need to ensure participatory decision making

Plan, Do, Check, Act

- PDCA
- Allows continuous improvement
- Steps:
  1. Understand problem by collection & analysing data
  2. Devise a plan to address the problem
  3. Develop a solution to the problem and deploy it
  4. Collect measurements to understand effectiveness
  5. Check if solution actually addresses the problem
  6. Produce a report and communicate changes
  7. Identify next set of problems
  8. goto 1

Intellectual Property Rights (IPR)

- They are negative rights
- 4 types
  - Copyright: right to copy documents, images, audio/video, programs, etc
  - Obligation of confidence: protection for confidential information
  - Patent: temporary monopoly on exploiting an invention
  - Trade mark: sign intended to identify a particular product
- Registered IPRs are approved/granted by states
  - patents
  - trade marks
- Unregistered IPRs are not approved/granted by states, but are still valid
  - copyright
- Something without IPR is in Public Domain

Copyright

- Author own the copyright, unless the author did the work for their employer
- Copyright owner has exclusive rights:
  - to make copies of the work

    - to sell, rent, lend, or give away copies of the work
    - to adapt the work
- Other must seek permission before using the work
- Permission can be implicit, e.g. downloading a webpage temporarily
- Comes into effect upon creation
- The scope is restricted to the expression of the idea, not the idea itself
- See Copyright, Design and Patents Act 1988 for specifics on software copyright

Obligation of Confidentiality

- Revealing information obtained under an obligation of confidence, the offender can be sued in civil court
- Can be overridden by public interest disclosure

Patents

- Must be applied for through a national patenting office
- Requires details of an invention to be published
- Software patents exist but each country has their own policy for acceptance

Trade Marks

- Must be registered with a national office
- Criminal offence to sell anything with an unauthorised trademark
- See Trade Marks Act 1994
- Software must display a trade mark prominently when it runs

Trade Secrets

- Protected under general tort law
    - reasonable attempt to keep their secrets secret
- See the US's Economic Espionage Act 1996 and the EU's Directive 2016/943
- Can be protected indefinitely if kept secret
- Once public, a patent is unlikely to be approved
- Reverse engineering is a lawful method of obtaining trade secrets

First Sale

- An IP owner can protect against reverse engineering until the first sale of an item
- From then, individuals have the right to modify, use and resell

Domain Names

- Domain names are managed by Internet Corporation for Assigned Names and Numbers (ICANN) cunts

- National domain-name registrars distribute domain names nationally on first-come-first-serve
- Domain names are as important as a trade mark, but have no protection, so cyber squatting exists
- In 1999, the World Intellectual Policy Organisation (WIPO) recommended ICANN to instate a dispute resolution policy, which they did
- In 2001, WIPO recommend a policy to address conflicts between domain names and other identifiers like personal or place names

Software Licences

- Terms and conditions of use

Retail software licence

- Intended for mass market
- Price is modest (up to £500)
- Buyer receives a single copy for a single installation
- Licence doesn't cover maintenance or upgrades
- Bulk licence allows multiple installations for an increased licence cost

Corporate software licence

- Intended for large organisations
- Allows many installations
- Very high up-front fee (£10,000 - £1,000,000)
- Annual maintenance fee
- Provides high quality support

Open-source software licence

- Software distributed as source code
- Minimal to no licence fee
- Often requires/allows:
  - Original authors' information and copyright statement retained in the source code
  - Reuse of source code
  - Possible modification of source code
  - Redistribution of source code

Free software

- Distributed completely free of charge
- Examples include Linux and the GNU project

Contracts

- Can be used to enforce security standards by defining security requirements and liability for security issues

Bespoke software development contracts

- Software is developed for the exclusive use of a single customer from a single supplier
- Contract should outline:
  - requirements
  - deliverables
  - price
  - IPR of both the customer and supplier (only applied to code specifically developed for the customer)
  - how project should be managed
    - project managers
    - surcharges if supplier is late or customer changes requirements late in development
  - acceptance procedure
- Contracts can be fixed-price or cost-plus
  - fixed-price specifies a fixed price for the product, excluding penalty clauses
  - cost-plus specifies the customer will pay the supplier's costs and a profit margin

Contract Hire

- Customer could hire contractors:
  - From an agency
    - Customer is responsible for managing staff
    - Agency responsible for supplying competent staff
  - Who are freelancers
    - Specialists
    - Not common
    - Individual
  - Who are consultants
    - Experts in their field
    - Only advise, no code
- Easier and simpler than bespoke software development contracts