Computers and the law

Disclaimer

Material presented here should be used with caution.

It is written with no legal expertise.

If in doubt, ask a professional!

theme

Personal privacy
& information rights

vs

The “public good”
& law enforcement

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain societal behavior
- Ethics: define socially acceptable behavior
- Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

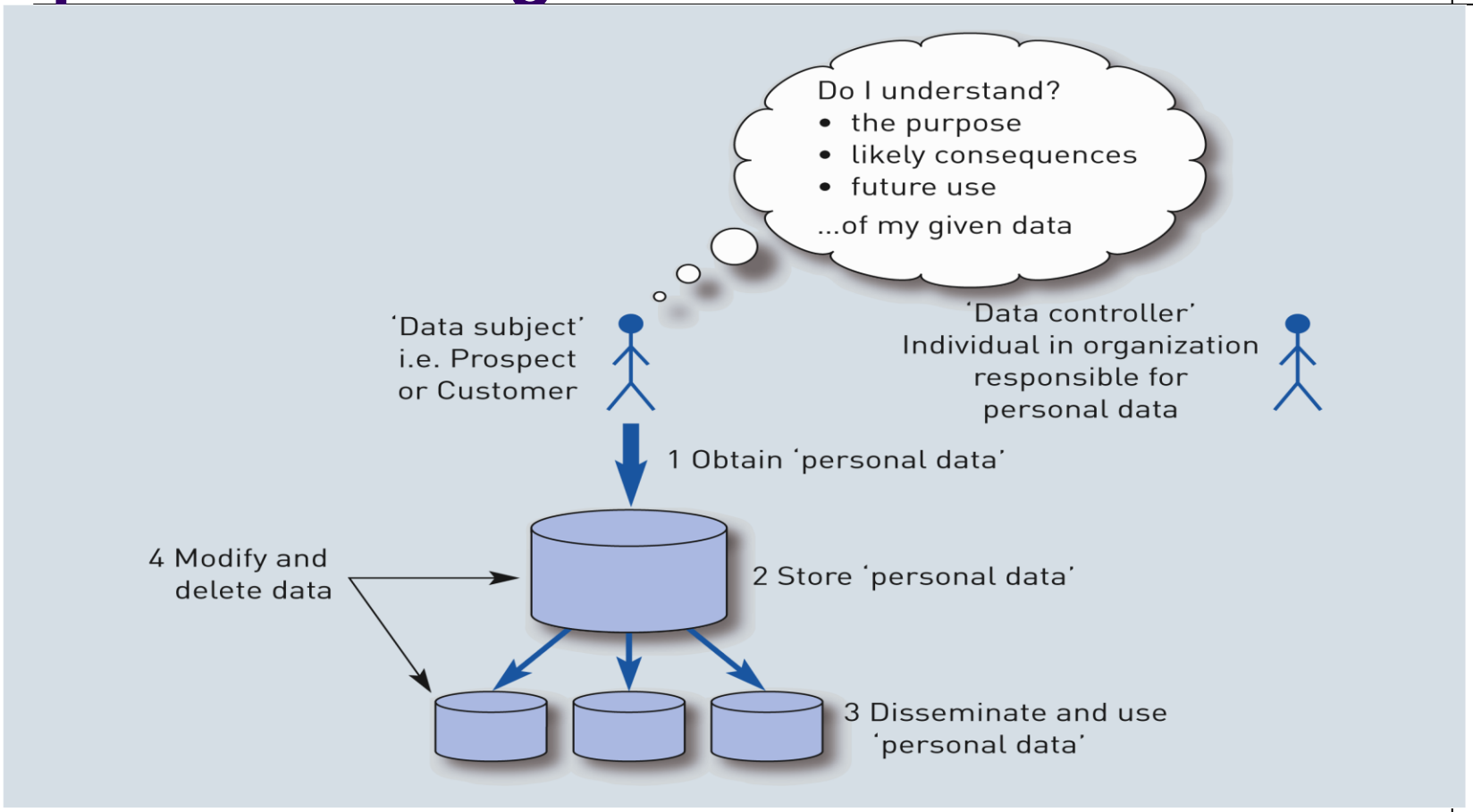
Computers and the law

- The law affects a number of areas where the computer professional will work
- These include:
  - Issues of developing systems
  - Storing and using information
  - Using and misusing computer technology

Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously impossible
- The number of statutes addressing an individual’s right to privacy has grown

Information flows that need to be understood for compliance with data protection legislation



Information flows that need to be understood for compliance with data protection legislation

Source: BIM

Reasons for Data Protection Act, 1984

- To protect individuals from abuses and inaccuracies stemming from computer-held data (but not manual)
- Set up the Data Protection Registrar who has the power to require changes in an information system, make the use of such a system illegal and prohibit transfer of data abroad.

  Data Protection Registrar is now the Information Commissioner (ico.org.uk)

Data Protection Act (1984, 1998, 2018)

The act that states that data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

DPA and GDPR

- The **Data Protection Act 2018** achieved Royal Assent on 23 May **2018**.
- It applies the EU's GDPR (General Data Protection Regulation) standards.

  Whereas the GDPR gives member states limited opportunities to make provisions for how it applies in their country, one element of the DPA **2018** is the details of these, applying as the national **law**.

DP Principles 1. *Fairly and lawfully processed*.

- This requires appointment of a **data controller** who is a person with defined responsibility for data protection within a company.
- Clear details in communications such as on a web site or direct mail of how a '**data subject**' can contact the data controller or a representative.
- Before data processing 'the data subject has given his consent' or the processing must be *necessary* either for a 'contract to which the data subject is a party' (for example as part of a sale of a product) or because it is required by other laws.
- Sensitive personal data requires particular care, this includes
  - the racial or ethnic origin of the data subject;
  - political opinions;
  - religious beliefs or other beliefs of a similar nature;
  - membership of a trade union
  - physical or mental health or condition

DP Principles 2. *Processed for limited purposes*

- This implies that the organization must make it clear why and how the data will be processed at the point of collection. For example, an organisation must explain how your data will be used if you provide your details on a web site when entering a prize draw. You would also have to agree (give *consent*) for further communications from the company.
- Only processed as far as necessary.

DP Principles 3. *Adequate, relevant and not excessive*

- This specifies that the minimum necessary amount of data is requested for processing. For example, it would not be applicable a prize draw for the company to ask about your credit history.
- There is difficulty in reconciling this provision between the needs of the individual and the needs of the company.
- The more details that an organization has about a customer, then the better they can understand that customer and so develop products and marketing communications specific to that customer which they are more likely to respond to.

DP Principles 4. Accuracy

- It is clearly also in the interest of an organization in an ongoing relationship with a partner that the data is kept accurate and up to date.
- The guidelines on the Act suggests that additional steps should be taken to check data is accurate, in case they are in error, for example due to mis-keying by the data subject, organization or some other reason.
- Inaccurate data is defined in the guidelines as: ‘incorrect or misleading as to any matter of fact.’
- Steps must be in place to keep data up-to-date.

DP Principles 5. *Not kept longer than necessary*

- The guidelines state: '*To comply with this Principle, data controllers will need to review their personal data regularly and to delete the information which is no longer required for their purposes*.'

DP Principles 6. *Processed in accordance with the data subject's rights*

- One aspect of the data subject's rights is the option to request a copy of their personal data from an organization, this is known as a 'subject access request.'
- For payment of a small fee such as £10 or £30, an individual can request information which must be supplied by the organization within 40 days.
- This includes all information on paper files and on computer. If you requested this information from your bank there may be several boxes of all transactions!

Principle 6 continued

Other aspects of a data subject's rights which the law upholds are designed to prevent or control processing which:

- causes damage or distress (for example repeatedly sending mailshots to someone who has died);
- is used for direct marketing (for example, in the UK consumers can subscribe to the mail, e-mail or telephone preference service or telephone preference services to avoid unsolicited mailings, e-mails or phone calls); (FCC)
- is used for automatic decision taking – automated credit checks, for example may result in unjust decisions on taking a loan – these can be investigated if you feel the decision is unfair.

DP Principles 7. Secure

- In full: '*Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*'

- Appropriate security is mandatory.

DP Principles 8. *Not transferred to countries without adequate protection*

- In full: '*Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.*'
- Transfer of data beyond Europe is likely for multi-national companies. This principle prevents export of data to countries that do not have sound data processing laws. If the transfer is required in concluding a sale or contract or if the data subject agrees to it with adequate safeguards, then transfer is legal.

DPA - Rights of the Data Subject

- To have data controller and purposes identified at time of data collection
- To object where damage/distress may be caused or data used for direct marketing
- To have data corrected, erased and blocked and previous recipients notified
- To have compensation for damage/distress by contravention by a data controller

DPA - Rights of the Data Subject

- To request right of access (in writing with fee) and receive data, purposes, logic used in automatic decision making and recipients – 21 days notification of intention to comply from data controller and data within 40 days.

Data Protection Act

- People (Data controllers) who use personal data relating to living individuals (Data Subjects) notify themselves to the Information Commissioner in writing with details of:
  - Data subject categories,
  - Data types,
  - Processing purposes
  - Other parties to whom data is to be disclosed

- Notification must **be renewed every three years.**
- **Compliance must be** “designed in”, not “bolted on”

Problems with DP Act interpretation 1

- In December 2003 an elderly couple in the UK died through hypothermia after their utility company had cut off their gas supply. Initially the press supported the company suggesting that the utility supplier had made every effort to assist the couple, but data protection laws prevented them passing sensitive personal data onto social welfare and charity organizations.

Problems with DP Act interpretation 2

- *Guardian* (2004) quoted the commissioner as saying that organizations used the act as a '*smokescreen for their own shortcomings*'. He suggested that common sense should be applied.
- Commenting on the utilities case he said: '*Where a gas company is disconnecting people they know to be vulnerable, I don't have a problem with telling social services. I would find it wholly unacceptable if they told a bank or credit card company*.'

Scenario 1

- You work for a local authority as an database manager and you receive two requests via e-mail for information from the database. One asks for the name of the chief executive of the local authority along with her home address and phone number. The second request is from a local resident who lives in rented council accommodation. The person asks for a copy for all information that relates to them. What are your legal obligations to answer these e-mails?

  What laws affect how you store your data?

Freedom of Information Act 2000 (FOIA)

The Information Commissioner web site states:

"The **Freedom of Information Act 2000** gives people a general right of access to information held by or on behalf of public authorities, promoting a culture of openness and accountability across the public sector.

This should lead to a better understanding about:

- how public authorities carry out their duties
- why they make the decisions they do
- how they spend public money"

(http://www.informationcommissioner.gov.uk/)

A fee is applicable and the request should usually be answered within 20 days

Freedom of Information Act

- The UK FOIA does not address personal data and privacy, rather it is to encourage openness amongst public authorities.
- It is intended to give citizens access to information held by public authorities, enabling them to participate ‘in the discussion of policy issues and so improve the quality of government decision making’ and ‘holding government and other bodies to account’.

FOIA

- By law public organizations must produce a **Publication Scheme** which consists of the classes of information that are made available.
- One implication of the FOIA may be that organizations selling services to governments may be able to access what would formerly be thought of a confidential details about competitive bids. This may contain commercially sensitive information which will affect the outcomes of future bids.
- However, the Act does exempt trade secrets. In fact, businesses need to consider all types of information given to public bodies since it may be disclosed at a later date, although there are exemptions.

Computer Misuse Act 1

1. *Unauthorised access to computer material*.

The law states:

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

Computer Misuse Act 2

2. *Unauthorised access with intent to commit or facilitate commission of further offences*.

In this case, it is found there is a specific intention to destroy data, cause damage or commit fraud. A fine and/or five year prison sentence can occur in this situation.

3. *Unauthorised modification of computer material*.

The law adjudges this to have occurred when there is an act committed

which:

'*causes an unauthorised modification of the contents of any computer*'

These specific examples of the purpose of modification are given:

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

Computer Misuse Act 1990 (2)

- Note: The offender must be aware at the time that their action is unauthorised; for this reason it is recommended that login and other banners be displayed wherever possible.

Scenario 3

You receive an e-mail from a friend which contains a url and the message “check this out. you’ll be surprised.” You type the url into your browser and find that you have access to people’s bank account details held by a major high street bank. What are the legal implications for you of doing this? What should you do next?

You notice that your boss is one of the names listed. You click on the her name to find out further information about her bank account. What are the legal implications of taking this action?

Regulation of Investigatory Powers Act 2000 (RIPA)

- service providers must maintain “intercept capability”
- statutory controls governing access to communications data
  - e.g billing data
- provides legal basis for covert surveillance activities
  - by law enforcement agencies
- power to require persons to disclose encrypted data in “plain text”
  - + extra powers to demand decryption keys

Data Retention and Investigatory Powers Act 2014

- the Act ensures that critical capabilities to fight crime and protect the public are maintained. It clarifies existing law without extending current powers
- interception and access to communications data are critical to the ability of our law enforcement and intelligence agencies to fight crime and protect the public
- the Act makes clear that anyone providing a communications service to customers in the UK – regardless of where that service is provided from – should comply with lawful requests made under the Regulation of Investigatory Powers Act 2000
- it also replaces the current regulations under which domestic companies can be required to retain certain types of communications data for up to 12 months, so this may later be acquired by law enforcement and used in evidence
- alongside the Act, the government is introducing a package of measures to provide reassurance that the rights of members of the public to security and privacy are equally protected

https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014

RIPA - potential

- UK Government could:
  - order telecoms providers (Inc. ISPs) to intercept individual's communications
  - force providers to install interception systems
  - monitor any user's activity on the net
  - order "mass surveillance" via interception warrants
  - demand handover of keys to encrypted data
- Government agencies
  - need not mention warrants & surveillance data in court
    - so individuals may not be aware of interceptions

Other laws applying to information

- **The Malicious Communications Act (1988)** makes it an offence to send any message that might be considered obscene or threatening.
- **The Defamation Act (1996)** is concerned with slander and libel. This legislation extends to comments made in e-mail messages and material displayed on web sites.
- **The Electronic Communications Act (2000)** is intended to support the growth of e-commerce in the UK. Amongst other things, the Act serves to make electronic signatures legally binding.

Other laws applying to information (continued)

- In the wake of the September 11 terrorist attack on the United States, the **Anti-terrorism, Crime and Security Act (2001)** was introduced in the UK as a means of strengthening existing anti-terrorism legislation. Of particular importance to the IS industry is a requirement to make sure that certain companies retain data on consumers' Internet and telephone activities and to make sure the data is searchable. As an example, guidelines from the Home Office suggest that ISPs should keep telephone subscriber and call information for 12 months, e-mail and ISP subscriber data for 6 months, and web activity information for four days.

What is intellectual property ?

- Having the right type of intellectual property protection helps you to stop people stealing or copying:
- the names of your products or brands
- your inventions
- the design or look of your products
- things you write, make or produce
- Copyright, patents, designs and trade marks are all types of intellectual property protection. You get some types of protection automatically, others you have to apply for.

https://www.gov.uk/intellectual-property-an-overview

What counts as intellectual property?

Intellectual property is something unique that you physically create. An idea alone is not intellectual property. For example, an idea for a book doesn't count, but the words you've written do.

Owning intellectual property

- You own intellectual property if you:
- created it (and it meets the requirements for copyright, a patent or a design)
- bought intellectual property rights from the creator or a previous owner
- have a brand that could be a trade mark, eg a well-known product name
- Intellectual property can:
- have more than one owner
- belong to people or businesses
- be sold or transferred

Copyright (1)

- Copyright law and copyright originated in the UK from a concept of common law, the Statute of Anne 1709. It became statutory with the passing of the Copyright Act 1911. The current act is the Copyright, Designs and Patents Act 1988.

- **Computer programs regulations in 1992 extended the copyright of literary works to include computer programs**.

Copyright (2)

- Copyright law gives the creators of literary, dramatic, musical, artistic works, sound recordings, broadcasts, films and typographical arrangement of published editions rights to control the ways in which their material may be used.
- International conventions give UK copyright protection in most countries, subject to national laws.

Copyright (3)

Aim –To protect the fruits of someone's work, labour, skill or taste. Allow creators to gain rewards and encourage further work.

Covers – Computer Programmes and Databases. Literary, Dramatic, Musical, Artistic work,

Does not cover – Craftsmanship. Merit or Quality is not a Factor.

Copyright (4)

Protects artistic work, not the Idea

Has to be recorded. The physical embodiment.

Example – A Photograph

A newspaper can not reproduce it, in whatever form.

An artist, can not copy the photograph in any form.

Television can not show the photograph.

However,

Another Photographer can go and take the same picture.

An Artist can go and paint the same scene, etc.

Copyright (5)

- Is free.
- It is automatic.
- Work only has to be fixed.
- Worldwide protection. Berne Convention
- Lodge a copy with a court respected form.

Who Owns The Copyright On A Piece Of Work (6)

- the individual or collective who authored the work
- if a work is produced as part of employment then normally the copyright belongs to the person/company who hired the individual.
- For freelance or commissioned work, copyright will usually belong to the author of the work, unless there is an agreement to the contrary, (i.e. in a contract for service).
- Anything which is copied from a previous work is copyright the original author

How Long does it last? (7)

70 years after the end of the year of the death of the author.

Exceptions

Sound recordings – 70 years from the year it was published.

Films – 70 years after the death of the last surviving creator.

Types of protection (8)

The type of protection you can get depends on what you've created. You get some types of protection automatically, others you have to apply for.

Type of protection	Examples of intellectual property
Copyright	Writing and literary works, art, photography, films, TV, music, web content, sound recordings
Design right	Shapes of objects

Protection you have to apply for (9)

Type of protection	Examples of intellectual property	Time to allow for application
Trade marks	Product names, logos, jingles	4 months
Registered designs	Appearance of a product including, shape, packaging, patterns, colours, decoration	1 month
Patents	Inventions and products, eg machines and machine parts, tools, medicines	Around 5 years

Scenario 4

- You are a student at university. Your tutor has asked you to complete a piece of coursework which requires you to use some proprietary software. You are unable to go into the university because you are looking after your sick cat. A friend offers you a copy of the software to help you out. You take the copy of the software and complete the coursework. You think the software is very good and decide to keep the software on your computer at home. What law (if any) have you broken?

Future development

- The new Data Protection Bill is designed to sign European privacy rules into British law, as well as update the existing Data Protection Act which has not changed since 1998.
- This measure is part of the European General Data Protection Regulations (GDPR)

What are the new measures?

- **Right to be forgotten**
  - Consumers will be able to ask businesses and organisations for access to their personal data and for it to be wiped, giving them more control over how their information is removed.
  - The UK law will extend this slightly by requiring social media companies to delete all of a person's posts from before they were under 18, if they ask for it.
  - The requirement will be subject to some exemptions.

What are the new measures? Cont.

- **Personal data**
  - The definition of personal data will be greatly expanded to reflect new types of data that were not covered by the 1998 regulations. They include IP addresses (used to identify a phone or computer visiting a website) and internet cookies (data about your web browsing habits). This follows concerns that internet browsing records are increasingly being used to target people.

What are the new measures? Cont.

- **Privacy**
  - The new laws will make consent explicit - people will have to opt in to being put on cold-calling lists and be aware that their information is being passed on to marketing companies.

What are the new measures? Cont.

- **Automated processing**
  - This is another law being taken over from GDPR, but its consequences are still yet to be seen. When individuals are “profiled” by an algorithm based on their personal data, such as an evaluation of their health, wealth or movements, individuals can demand this action is performed by a person, rather than a machine.

What are the new measures? Cont.

- **Data portability**
  - Consumers will be able to move data between companies should they wish to.
  - For example, they will be able to easily move photos between cloud storage companies.

New powers

- ICO will be able to levy fines of up to £17m, or 4 per cent of a company's global turnover, for breaching the rules, well up from the current £500,000 maximum for breaching the current Data Protection Act.

New criminal offences

- There will also be two new criminal offences, which could have unlimited fines:
- **Re-identifying people from anonymous data:** Data is often kept anonymous to respect people's privacy, but by piecing many of these bits together, it might be possible to identify an individual's browsing habits or credit card transactions. This will become a criminal offence.
- **Changing data:** Organisations could also face criminal charges if they are found tampering with data that has been requested by an individual.

Summary

- All information security professionals must understand the scope of an organization's legal and ethical responsibilities
- Understand the current legal environment
  - Keep apprised of new laws, regulations, and ethical issues as they emerge
  - To minimize the organization's liabilities
- Educate employees and management about their legal and ethical obligations
  - And proper use of information technology

References

- Davison, R.M., (2000), Professional Ethics in Information Systems: A Personal Perspective, Communications of the Association for Information Systems, Vol. 3, (8), April
- Johnson, D.G. (2001) *Computer Ethics – third edition,* Prentice Hall. (especially chapters 2 and 3)
- Legislation.gov.uk. National archives. Computer Misuse Act 2000. http://www.legislation.gov.uk/ukpga/1990/18/contents. [date accessed 14 Nov 2016].
- Titcomb.J. (2017) The Telegraph. http://www.telegraph.co.uk/technology/0/data-protection-bill-will-new-laws-affect/ [date accessed 27 Nov 2017]
- The Intellectual Property Office. https://www.gov.uk/intellectual-property-an-overview [date accessed 21 Nov 2016].