CE29x Team-Project Challenge

CSEE and the Law:

2. Privacy and Security Laws

Professor Anthony Vickers

Room: 1NW.3.17 e-mail: vicka

with acknowledgements to Keith Primrose, Michael Fairbank and Dr Audrey Guinchard of University of Essex Law Department

Lecture outline

- Last lecture
  - British Legal system
  - IP laws
- This lecture: look at other laws that affect CSEE, e.g.
  - Privacy Laws
  - Security Laws
  - Plus, some other relevant laws

Privacy Laws

Privacy Laws

These are described in the following slides:

1. Data Protection Act 1998
2. EU General Data Protection Regulation 2016
3. Freedom of Information Act (2000)
4. Privacy and Electronic Communications Regulations (2003)

1. Data Protection Act 1998

Data Protection Acts 1984 & 1998

- Applies to electronic and (since 1998) manually stored personal data (data allowing a person to be identifiable).
- DPA gives living, identifiable, individuals the right to know what information is on record and to challenge it if appropriate.
- Each organisation is a **Data Controller**, i.e. is responsible for compliance.
- The people who's data is stored and used are called "**data subjects**"
- See https://www.gov.uk/data-protection

Data Protection Act

- Everyone responsible for using data has to follow strict rules called ‘data protection principles’.
- Eight Principles - Personal data must be:

1. Obtained and processed ‘fairly and lawfully’
   - Must be with consent of the **data subject**
   - E.g. now have to be notified to accept cookies
2. Used for limited, specifically stated purposes
   - Data controllers must notify the Information Commissioner (a government body) of the personal data they are collecting and the purposes for which it is being collected

Data Protection Act

3. Used in a way that is adequate, relevant and not excessive
   - E.g. don't ask for customer's address or martial status etc, if that's not explicitly needed
4. Accurate
   - Kept up to date
   - But this can be impractical

Data Protection Act

5. Kept for **no longer** than is absolutely necessary

- It is necessary to establish how long each item of personal data needs to be kept.
  - E.g. Financial data is kept for seven years for auditing
  - It is appropriate to keep some personal data indefinitely (e.g. university records of graduating students).
- In all cases, the purpose for which the data is kept must be included in the purposes for which it was collected;
- Procedures to ensure that all data is erased at the appropriate time are needed, and this must include erasure from backup copies.

Data Protection Act

6. Handled according to people's data protection rights
   - E.g. data subjects have the right to receive:
     - a description of the personal data being held;
     - an explanation of the purpose for which it is being held and processed;
     - a description of the people or organisations to which it may be disclosed;
     - an intelligible statement of the specific data held about them;
     - a description of the source of the data.
   - The 1998 Act also gives data subjects the right:
     - to prevent processing likely to cause damage and distress;
     - to prevent processing for the purposes of direct marketing;
     - to compensation in the case of damage caused by processing of personal data in violation of the principles of the Act.

Data Protection Act

7. Kept safe and secure
   - Need access control
     - (through passwords or other means)
   - backup procedures
   - integrity checks on the data
   - vetting of personnel who have access to the data
   - Keep laptops secure from theft

Data Protection Act

8. Not transferred outside the UK without adequate protection
   - Data cannot be sent outside the European Economic Area, unless there is a guarantee that the data will receive adequate levels of protection.
   - Think before you upload clients' data to "the cloud"
   - US does not count as safe, however:
     - Certain US companies are certified under the "**Safe Harbour Privacy Principles"**
       - allows individual American companies to register their compliance with the EU requirements.

Data Protection Acts 1984 & 1998

- There is stronger legal protection for more sensitive information, such as:
  - ethnic background
  - political opinions
  - religious beliefs
  - health
  - sexual health
  - criminal records

Data Protection Acts 1984 & 1998

- The Data Protection Act gives you the right to find out what information the government and other organisations stores about you.
- Write to the organisation and ask for a copy of the information they hold about you.
  - If you don't know who to write to, address your letter to the company secretary.
- The organisation is legally required to give you a copy of the information they hold about you if you request it.
  - But they can charge you for the admin costs

DPA Exceptions

- There are general exceptions covering
  - Data related to national security
  - Data used for domestic or household purposes
- There are also explicit exceptions both for the data controller and the data subject
  - Controller must reveal data relevant to criminal investigations to the relevant authority
  - Subject has no right to see data:
    - that might result in infringing someone else's right
    - that consists of a reference regarding the subject
    - that is recorded by candidates during an academic, professional or other examination

Data Protection Acts 1984 & 1998

- DPA is administered by the Information Commissioner's Office (formerly known as the Data Protection Registrar)
  - which reports to Parliament.
  - Regulates compliance with the Act (and the FOIA, but for Scotland, FOIA is the Scottish Commissioner)
  - Imposes fines on organisations that fail to comply with the Act*
- In the news this week:
  - Uber fined £385,000 for losing UK customer data

* See p 152 F.Bott, Professional Issues in IT, 2nd ed. for examples of fines

Data Protection Acts 1984 & 1998

* DPA 1998 replaced DPA 1984
* GDPR (next slide) and DPA 2018 replace the above

2. EU General Data Protection Regulation 2016 (GDPR 2016)

EU General Data Protection Regulation 2016

- In force in UK from 25 May 2018
  - UK pledged to apply it after BREXIT
- Will AUTOMATICALLY repeal (nullify) the DPA 1998
- Unchanged:
  - The core definitions and principles for processing personal data
  - 8 Principles of DPA remain
- BIG Changes:
  - Making compliance visible: certification schemes with technical standards; data protection officer within organisations
  - sanctions: BIG FINES

EU General Data Protection Regulation 2016

* See https://gdpr-info.eu/

Processing as defined by DPA

- Obviously, the DPA (and GDPR) will likely affect you in your CSEE career
- The definition of processing data about individuals is very broad. It includes:
  - Obtaining, recording, or holding the data
  - Carrying out any operations on the data including:
    - Organisation, adaptation or alteration
    - Retrieval, consultation, or use
    - Disclosure by transmission, dissemination, or otherwise making available
    - Alignment, combination, blocking, erasure, or destruction

Data subjects' Rights under GDPR

- DPA gave 8 principles
- GDPR strengthens these further:

Data subjects' Rights under GDPR

- Right to be forgotten/erasure: confirmed
  - see Google Spain case:
    - It held that an Internet search engine operator is responsible for the processing that it carries out of personal information which appears on web pages published by third parties
    - It enforces "right to be forgotten"
- Right to have transparent and clear privacy policies

Data subjects' Rights under GDPR

- Right to ask for human intervention in automatic decision-making process with legal consequences
  - E.g. HMRC website has a questionnaire that decides if you are self-employed or employed-
    - And its decision is legally binding!
    - GDPR will mean individuals have right to object if information chatbots present is wrong – and to insist that a human to reviews the case
  - Machines could otherwise make decisions that affect us (credit scores, legal decisions…)

Data subjects' Rights under GDPR

- Right to data portability (Article 20 GDPR):
  - individuals can ask for the details of their data to be transferred (E.g. in CSV format) to prevent lock-in to one vendor
    - allows social media data or energy data to be transferred to a different platform
    - or to be sold by individual
    - so you can access your Facebook data and remove it

Data subjects' Rights under GDPR

- Websites etc must clearly separate "Right to consent to processing" and "right to consent to contract":
  - Prohibition of "click-wrap mechanisms"
    - Prevents bundling of a click "I agree" with right to access a website with at the same time forcing you to forfeit your privacy rights
- Effective right to withdraw consent to processing

Obligations of data controllers

- Data controllers = the organisation processing the data
  - in effect, you will be involved in the decisions to fulfil the organisation's obligations
- Obligation to inform:
  - Use of privacy policies. ATTENTION: the GDPR changes the game played. Transparency and clarity
- Obligation to secure BY DESIGN:
  - Think: cybersecurity special skills – worth paying a specialist if you don't have the skills as a software developer

Obligations of data controllers

- Obligation: PRIVACY BY DESIGN (Article 25 GDPR)
- Obligation to provide a trail of decisions made
- Auditing mandatory
- Certification schemes with data seals to guarantee privacy and security
- Obligation to have a data protection officer independent and impartial within organisation

Obligations of data controllers

- YOU will have to
  - keep track of any discussion and of any decision made,
  - so you can PROVE you created software and systems that
  - implement privacy and security by design
- Failure to meet any of those obligations
  - See https://gdpr-info.eu, https://gdpr.eu
  - BIG Fines (GDPR) for your organisation
- Cloud servers will not be exempt from GDPR enforcement

Obligations of data controllers

- BIG Fines (GDPR) for your organisation:
  - 4% of worldwide turnover, or €20m (whichever is greater) for not having sufficient customer consent to process data or violating the core of Privacy by Design concepts
  - Or 2% of worldwide turnover, or €10m (whichever is greater), for
    - for not having their records in order (article 28),
    - not notifying the supervising authority and data subject about a breach
      - Uber says 2.7m Brits hit by breach that was covered up
      - But only fined £385,000 under old DPA laws

Obligations of data controllers

- What matters for compliance is that:
  - You instigated privacy and security by design from the outset
  - That you assessed the risks to privacy, equality (avoid discrimination, direct or indirect), political rights etc…
  - That you were reasonable in your approach, including asking for advice to the Information Commissioner Office
- you can get the decision wrong, but you need the trail of paperwork to show you were not negligent

Personal data - anonymisation

To keep clients' data safe, you may try to "anonymise" it.

Definitions:

- Anonymisation:
  - only if re-identification is impossible (risk = zero), is data said to be anonymised.
  - DPA and GDPR would not apply
- Pseudonymisation: defined in Article 4(5) GDPR. Any data which can be re-identified with additional information.
  - DPA and GDPR apply – Article 25 GDPR
  - Even if the risk is of one per cent.
  - = pseudonymisation is no escape to data protection compliance

Difficulties with the DPA

- Difficulty in trading across international boundaries:
  - EU regulations place strict controls on the transfer of personal data to organisations based outside of the EU.
  - SAFE HARBOUR has been cancelled in GDPR
  - Privacy shield tries to provide better safeguards between EU and US; but it's criticised
  - Think regional: can I store data in the EU, or Canada, not the US?

Difficulties with the DPA

- Lack of clear guidance:
  - Many organisations have found it difficult to incorporate new data protection legislation into existing company policies and procedures.
  - Consult website of INFORMATION COMMISSIONER AND ARTICLE 29 Working party
    - they have detailed guidance with specific, practical examples
    - This working party makes recommendations that effectively become law

3. Freedom of Information Act

Freedom of Information Act 2000

- The Act gives members of the public the right to access information held by public authorities.
  - For example these include:
    - Government departments and local authorities;
    - Schools, colleges and universities;
    - Local Education Authorities; health trusts, publicly funded museums
    - And thousands of other organisations.
- From 1 January 2005, public authorities must reply in writing within 20 working days to specific requests for information, declaring whether they hold information of the kind requested. If so, they must then respond appropriately.

Scenario

- A prominent journalist writes to a University:

  "Dear Sirs

  I am making an application under the Freedom of Information Act for information on all your courses in the 'Department of David Beckham Studies'. Please supply me with the following:

  1. A list of all courses and all modules taught within each course
  2. Details of the fees charged for each course
  3. The number of students enrolled on each module
  4. The contact details of all the students enrolled on each of the courses

  Yours A. Nosey-Parker"

- How should the university reply?

4. Privacy and Electronic Communications Regulations (2003)

Privacy and Electronic Communications Regulations (2003)

- Came into force in December 2003
- Brought the UK into compliance with the rest of the European Union regarding issues such as e-mail marketing and telesales.
- Regulates the use of publicly available electronic communications services for direct marketing purposes.

Privacy and Electronic Communications Regulations (2003)

- Also covers unsolicited direct marketing activity by telephone, fax, e-mail and automated calling systems and even text messages.
  - Now requires consent (opt-in) and opt-out:
  - Organisations cannot merely add people's details to their marketing database and offer an opt out after they have started sending direct marketing.
- Includes requirement to accept or decline cookies
  - Must still be able to access the site if you decline cookies
    - …although maybe with reduced features

Security Laws

Security Laws:

These are described in the following slides:

1. Computer Misuse Act (1990) – updated 2006 and 2015
    1. Police and Justice Act (2006)
    2. Serious Crime Act 2015
2. Electronic Communications Act (2000)
3. Regulation of Investigatory Powers Act (2000)
4. Investigatory Powers Act 2016 (dubbed the snooper charter)

1. Computer Misuse Act (1990)

Computer Misuse Act (1990)

* Abbreviated CMA 1990
* Three offences were originally recognized:

  Section 1: “Unauthorized Access”

  Section 2: “Unauthorized Access with Intent”

  Section 3: “Unauthorized modification”

Computer Misuse Act (1990)

- Since CMA 1990 creation, it was modified by:
  - The Police and Justice Act 2006:
    - Modified s1 CMA: sanction increased to one year
    - Modified s3 CMA: the definition of the offence and the penalties increased
    - Added new s3A CMA: misuse of tools
  - The Serious Crime Act 2015:
    - Modification of s3A CMA
    - Added new offence of s3ZA CMA: it's s3A but for critical infrastructures.

S1 of CMA: "Unauthorised access"

- Any conduct or action which would enable access without authorisation.
- Up to 12 months imprisonment.
- Extradition is possible.
  - See Lauri Love case
    - Computer activist alleged to have stolen huge amounts of data from US agencies
  - or Gary McKinnon case
    - Alleged to have broken in to US military; he claimed to be looking for UFO cover-ups
  - Both threatened with extradition to USA for trial

S1 of CMA: "Unauthorised access"

- Authorisation:
  - Express: you've been permitted to access
  - Implied: you've been permitted to access BUT implicitly only for a specific purpose.
    - E.g.: you're a police officer; you have access to the Police National database; implicitly, you don't have access to the database to check personal matters

S1 of CMA: "Unauthorised access"

- Even guessing a password *wrongly* is an offence!
  - You do not need to obtain access
  - You type a password to gain access, knowing you have no authorisation
  - = you commit the offence

- The only exclusion is roughly, reading something on a screen that is left open.
- But as soon as you move the mouse or use the keyboard, you commit the offence.

S1 of CMA: "Unauthorised access"

- Scanning for vulnerabilities:
  - You are in tricky territory if you have not expressly discussed the matter with the target
- Technically, port-scanning, fuzzing, etc.. can fall within the scope of criminal law as soon as your target has not authorised you.
  - Recently some CSEE students reported a network vulnerability, and although our admins and university were grateful, the students technically broke the law!
- Read A Cormack, Can CSIRTs lawfully Scan for vulnerabilities? Scripted 2014, vol 11(3), 308 at https://script-ed.org/wp-content/uploads/2014/12/cormack.pdf (open access)

S2 of CMA: "Unauthorised access with Intent"

- There must be intent to gain access to make a more serious crime
  - E.g. to gather data to blackmail, to steal confidential data, to cause disruption
- S2 of CMA has same rules as S1 of CMA
  - but penalties higher if intent is proven:
    - £ unlimited
    - and/or 5 years imprisonment

S3: "Unauthorised act with intention to impair or damage"

1. Any action which can result in:
   - ⁎ Impairment (= damage)
   - ⁎ Prevent or hinder access (= denial of service attack)
   - ⁎ Impair reliability of data (= data is modified, deleted, added…)
2. No need of result (no need of damage for example)
3. Any above action with:
   - ⁎ Intention
   - ⁎ Recklessness (= a form of negligence)

⁕ = committing an offence under s3 CMA

⁕ £ unlimited fine

- ⁎ and/or 10 years imprisonment

s3A CMA: "Misuse of Tools"

- The Police and Justice Act 2006 added new s3A CMA: "misuse of tools" offence
  - (see http://www.legislation.gov.uk/ukpga/1990/18/contents)
- Covers three types of actions:
  - Creating or adapting tools to commit the previous offences
  - Supplying or offering for sale the tools
  - Obtaining for use or for supply the tools
- Tools = any software or data!
  - VERY BROAD

s3A CMA: "Misuse of Tools" What does it mean?

- if you use Nmap, Metasploit, Burp Suite, SQL injection etc..,
  - And you have not sought authorisation from target,
  - You may be guilty of 'obtaining' the tool, in addition to being liable for s1 CMA.
- Even the use of a VPN to cover one's track can fall within the scope of the offence, if you commit s1 or s3 CMA!!!
- The Serious Crime Act 2015:
  - Introduces modification of s3A CMA
  - Added new offence of s3ZA CMA: same as s3A, but for critical infrastructures.
    - See http://www.legislation.gov.uk/ukpga/1990/18/contents

CMA and theft

- Theft Act 1968 not applicable, but:
- "Computing theft" can mean the *theft of services*,
  - such as the *unauthorised use* of a company's information systems.
    - s1 CMA offence
- Software theft (software piracy), involves making unauthorised copies of software applications
  - copyright offence

CMA and theft

- Data theft:
  - Stealing sensitive information:
    - could be a s55 DPA 1998, or bring penalties under the GDPR;
    - Would breach civil law: confidentiality, trade secrets…
  - making unauthorised changes to computer records = section 3 CMA (even if you have good 'intentions' – a motive at law is not accepted)
- Theft can also involve altering computer records to disguise the theft of money or data = s3 CMA

NO PUBLIC INTEREST DEFENCE

- You cannot claim a public interest defence under the CMA
- See R v Cuthbert 2005:
  - Cuthbert was a founding member of Open Web Application Security Project (OWASP)
  - He checked the security of a charity website he donated to
    - His check tripped some intrusion detection software
    - When interviewed by police, he panicked, and said the intrusion was caused by "the action of a proxy server"
    - This lack of initial clarity motivated the CPA to prosecute him
  - He was found guilty of s1CMA,
    - to the great regret of the judge.

- Always seek clarification if you're in doubt
  - The law does not care

2. Electronic Communications Act (2000)

Electronic Communications Act (2000)

- The Act creates a legal framework for electronic commerce, both in the private and public sectors, It:
  - Clarifies legal status of e-signatures
  - Allows government to update legislation
  - Ensures quality of e-signatures

3. Regulation of Investigatory Powers Act (2000)

Regulation of Investigatory Powers Act (2000)

- The Act introduced measures that allow electronic communications to be monitored by government agencies.
- Many people felt that the Regulation of Investigatory Powers Act (2000) – known as the RIP Act, or RIPA – would have a profound effect on business organisations
- Its impact has not been as serious as predicted.
- The government's monitoring of electronic communications is not something new . . .

Project Echelon

- Computer monitoring: The use of computer and communications technology to monitor the activities of individuals.
- In existence, in various forms for over 60 years, Echelon is a global surveillance system that monitors communications around the world.
- The project is operated by the USA, UK, Canada, Australia and New Zealand.
- Each day, millions of telephone calls, faxes and e-mail messages are intercepted and scanned for key words and phrases.
- Messages matching the search criteria used are collected and sent to the United States for further analysis.
- The EU Parliament asked in July 2001 the UK to explain its mass surveillance programme. Meeting was scheduled in September 2001. With 9/11, it never took place.

4. Investigatory Powers Act (2016)

Investigatory Powers Act 2016

- In November 2016, the UK parliament passed the new Investigatory Powers Act.
- This is the infamous "Snooper's charter"

Investigatory Powers Act 2016

- Requires ISPs to keep a record of all websites numbers you've visited
- Pros:
  - Designed to protect us against terrorism
- Cons:
  - Privacy concerns.
  - If a malicious government took power, then they could identify and oppress opposition supporters
- Any more pros/cons?

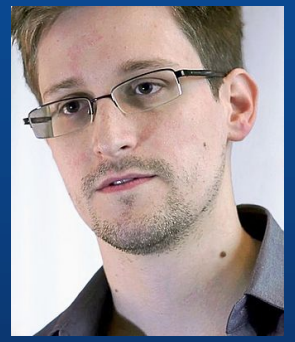
Investigatory Powers Act 2016

* Gives the government wide-ranging surveillance powers
  * including the ability to intercept and hack into millions of ordinary citizens' communications.
  * They were doing this already, with questionable legality, before this law was passed.

Investigatory Powers Act 2016

* Snowden revelations of PRISM surveillance program showed what techniques were already being used, e.g. unencrypted emails were being intercepted and searched.
* More damaging claims included
  * EU offices bugged to give US advantage in trade negotiations
  * Merkel phone calls 'intercepted‘

Source: BBC News article



Edward Snowden
1983-

Other Relevant UK Laws:

Other Relevant UK Laws

- The Health & Safety (Display Screen Equipment) Regulations 1992
- Health & Safety at Work Act (1974)
- The Consumer Protection Act 1987 (Product Liability)
- The Trades Description Act (1968)
- Trade Marks Act (1994)
- Sale of Goods Act (1979)
  - See lecture on Contracts
- Companies Consolidation Legislation (1987)
  - See lecture on Financial Accounts
- The Anti-terrorism, Crime and Security Act (2001) was introduced after the 9/11 terrorist attacks in the US
  - To strengthen existing legislation.
  - It requires companies:
    - to retain data on consumers' Internet and telephone activities
    - to make sure the data is searchable.
    - e.g.: guidelines suggest that Telcos / ISPs should keep telephone & call information for 12 months, e-mail data for 6 months, and web activity information for 4 days.

Lecture summary

- To be an effective CSEE worker, there is a lot of legislation you must be aware of
- Most important is probably data-protection act and its replacement GDPR
- Privacy and Security needs building in by design

- Quiz on Privacy and Security Laws

Further reading

- Charities fined by Information Commissioner
  - RSPCA fined £25000
  - British Heart Foundation fined £18000
  - Information Commissioner said fine was greatly reduced because these were charities.

Further reading

- Course textbook, F. Bott, *Professional Issues in Information Technology*, 2nd edition:
  - Chapter 13: "Data Protection, Privacy and Freedom of Information"
  - Chapter 14: "Internet Issues"
  - Chapter 15: "Computer Misuse"
- Careers at GCHQ: https://www.gchq-careers.co.uk

- Next lecture: Financial Accounting