CI465 An Introduction to IT Law

1

Lecture layout

Criminal or civil?

Criminal offences

Theft???

Computer Misuse Act 1990

Data Protection Act 1998

Intellectual Property law

- Primarily the Copyright, Designs and Patents Act

Civil offences

Breach of Confidence

- Proposed tort of 'misuse of private information'

Defamation Act 2013

Publication injunctions and super-injunctions

Mareva injunctions & Anton Piller orders

Other relevant laws

2

IT security law

- IF it is possible to identify the perpetrator of an information security breach…
- The breach might fall under criminal or civil law
  - So the victim may have a choice
- Criminal law
  - Police involvement
  - Jail sentences available
  - Beyond reasonable doubt
- Civil law
  - Solicitor involvement
  - Damages available
  - Balance of probabilities

3

Criminal law: theft

- The key damage in many breaches is unauthorised obtaining of information
- Is this theft?
  - Theft: Appropriating property belonging to another dishonestly with intent to permanently deprive
  - … so information theft is explicitly excluded from the Theft Act 1968
  - *Oxford v. Moss 1979*

4

Criminal Law – Fraud Act 2006

Updated various offences originally prosecuted under the Theft Acts

It is an offence to do the following with the intent of making gain for yourself or a loss for another:

Make a false representation

Fail to disclose information that you are legally required to

Abuse a position of safeguarding financial interests

Also an offence to possess or make articles for use in frauds

5

Criminal law - Computer Misuse Act 1990

The Act was designed to deter hackers

Unauthorised access to a computer

Summary offence – max sentence 6 months

Unauthorised modification of a computer

Either way offence – max sentence 2 years

Serious Crime Act 2015 – causing damage to economy or environment = max 14 yrs

- http://www.telegraph.co.uk/news/2017/04/09/hacker-sets-every-emergency-siren-dallas/?

Denial of service?

Yes, by case law – *DPP v. Lennon [2006]*

Making, supplying or obtaining articles for use in computer misuse offences?

Yes, under Police and Justice Act 2006 s37. Controversial.

Making information available with intent [e.g. other people's passwords]?

Not yet – under discussion since News International phone hacking scandal 2011

6

Criminal law – Data Protection Act 1998

Requires that certain data about identifiable living people is handled correctly and kept private

Such data must only be processed fairly and lawfully

Very wide definition of data 'processing' – *Campbell v. MGN [2002]*

Damages available if DPA breach causes pecuniary damage

So anyone who uses 'stolen' information might fall foul of this Act…

…but in practice, it's a bigger issue for the company who 'lost' the information to prove that they were handling it correctly

7

Criminal Law - GDPR

- The EU-wide General Data Protection Regulation took effect on 25 May 2018
- Updates the Data Protection Act 1998
- Biggest change: huge increase in fines
  - Talk Talk data breach 2015: fine of £400,000
  - Under GDPR, predicted fine would be £52 million

8

Other changes under GDPR

- Individuals must give 'clear and affirmative consent' to their data being processed. Ticking a box is adequate; staying silent on the subject is not.
- IP addresses and mobile device IDs are now unquestionably defined as personal data (their status was debatable under the Data Protection Directive).
- Genetic data and biometric data are classified as "sensitive personal data".
- There is a strong incentive to pseudonymise data sets; such data is still classed as personal data but is exempted from various requirements of the GDPR. Encryption is also encouraged.
- The "right to be forgotten" established by the European Court of Justice (Google Spain v. AEPD 2014) has been extended to become a "right of erasure"; it will no longer be sufficient to remove a person's data from search results when requested to do so, data controllers must now erase that data. However, if the data is encrypted, it may be sufficient to destroy the encryption keys rather than go through the prolonged process of ensuring that the data has been fully erased.

9

Complying with GDPR

Checklists

- Various organisations including the Information Commissioner's Office have published text-based checklists for organisations to use when preparing to comply with GDPR.
- E.g. GDPR Article 39: "Data Protection Officers are under a specific obligation to implement appropriate training. Although not an express obligation for organisations where DPOs are not required, we consider it to be almost impossible to demonstrate that an organisation is able to achieve compliance without policies setting out how to comply coupled with training to bring those policies to life."
- Checklist: "Organisations should implement a training programme covering data protection generally and the areas that are specifically relevant to their organisations, and implement a policy for determining when training should take place and when refresher training should be carried out and a process for recording when training has been completed"

10

GDPR: Unresolved issues

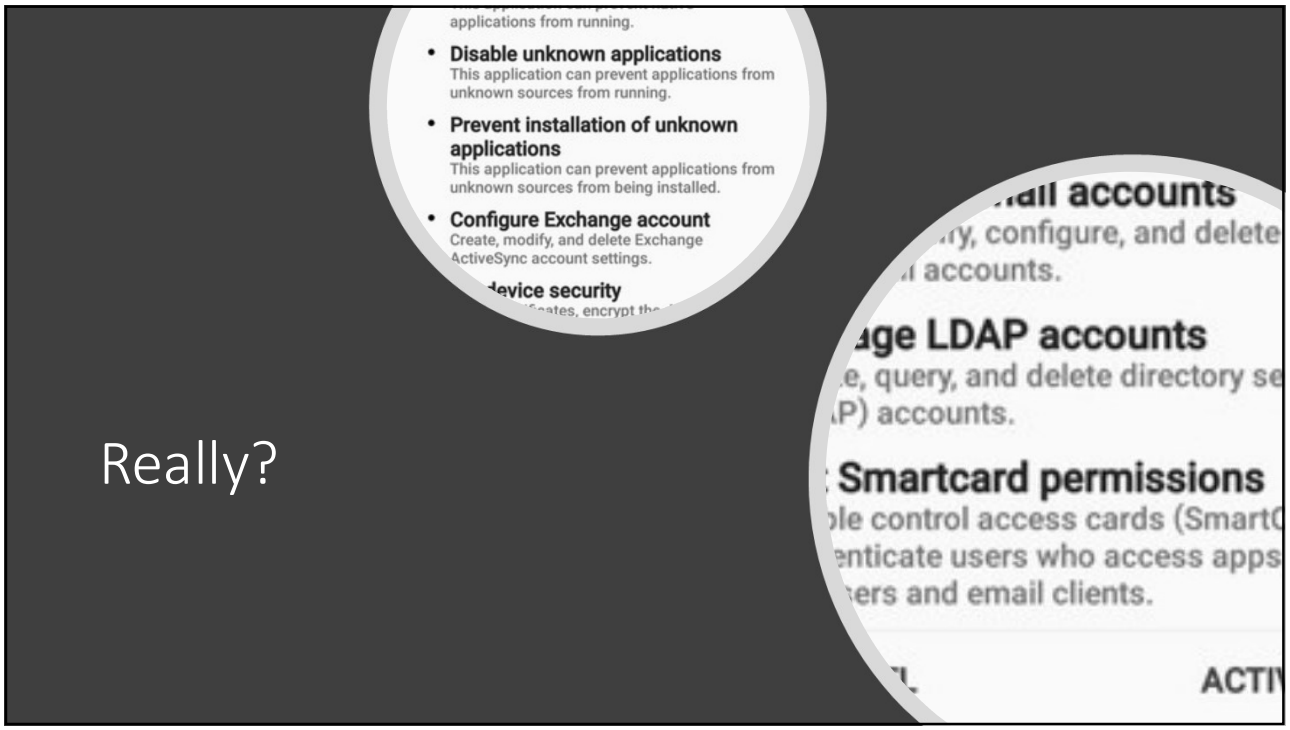
- DPOs are required to offer training, but do staff have to accept the offer?
- Which staff need to be trained?
- If multiple jurisdictions are involved, which supervisory authority/ies should take action?
- Who or what decides whether training is adequate or suitable?
- If an organisation does not require a DPO, does it truly have no requirement to train its staff in data processing issues? Might there be a requirement under contract or tort law?
- What do words such as “regular” and “large-scale” mean?
- ECJ decisions are expected…

11

GDPR: Who is the threat?

- Under GDPR are you a threat to cloud service providers? And the companies they support?

12



Really?

13

A particular issue for AI/ML systems: responding to requests for personal info

Articles 13-15 require that the data subject be given a variety of information about their rights regarding the storage and processing of their personal data, including "the purposes of the processing for which the personal data are intended."

If their personal data is being used for "automatic decision making including profiling" then they are also entitled to "meaningful information about the logic involved, as well as "the significance and the envisaged consequences of such processing for the data subject."

Article 22 spells out the purpose of these requirements: that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Impossible for machine learning systems?

14

Issues for machine learning systems

GDPR does explicitly state that data subjects have a right to "obtain an explanation of the decision reached after such assessment"

… but in Recital 71 (which is non-binding) rather than in the legally binding Articles

Is it possible to provide "meaningful information about the logic" and to explain "the significance of decision making" without giving a full explanation of an individual decision?

The current best advice is "yes"

Provide a document giving a technical description of the model.

- Burt (2017) suggests describing where the data comes from; the method used; and how many features are selected for.

And another giving an understanding of the decision(s) that the model is used to make and the consequences of a false positive or an omission. This will help to explain not only the logic of the decision but also its significance.

15

Criminal (and Civil) Law – Intellectual Property Law

IP law only applies if the 'thief' actually uses the 'stolen' information

So at least there is someone to prosecute…

Patent law

Infringement of patent after 'theft' of information

Rarely applies: the purpose of patents is to persuade inventors to publish their designs in return for a time-limited monopoly on use

- So theft is unnecessary!

Copyright law

Relatively easy to prove

- By similarity

Protects form, not function

- If the design for a market-leading chocolate bar was stolen and reproduced, copyright law would only protect the wrapper and the shape

16

Intellectual Property Law

- Copyright law includes the 'database right' (CDPA s16)
  - Covers any organised collection of independent works
    - *British Horseracing Board v William Hill (2004)*
  - Offences:
    - unauthorised extraction or re-utilisation of all or a substantial part of the contents of the database
    - repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of a database
  - So it protects the contents, not the form
- Trademark law
    - Applies if someone uses a similar trademark
    - … in your jurisdiction

17

Civil Law: Breach of Confidence

Originally designed to protect trade secrets

So anyone who learned a trade secret under a confidentiality agreement could not reveal it

Key factors

The information has "the necessary degree of confidence about it"

The information was provided in circumstances importing an obligation of confidence

There was an unauthorised use or disclosure of that information and, at least, the risk of damage

Progressively broadened by case law decisions

No contractual relationship is required

- *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948)*

Only a 'reasonable expectation of confidence' is required

- *Douglas v Hello! (2002)* – this concerned confidentiality of electronic information (photographs)

May create a tort of 'misuse of private information'

2014 case against Google for working around cookie blockers to obtain personal information for targeted ads (Vidal-Hall v. Google Inc.)

18

Civil Law: Defamation

Also called 'libel or 'slander'

Publication (or voicing) of statements that negatively affect the claimant's reputation

Rarely used in cases of information 'theft' because:

The statements have to be false; truth is a defence

Government pressure to reduce such cases

e.g. withdrawal of Legal Aid

Has been used to prevent 'kiss and tell' stories from former employees

19

Injunctions and Super-injunctions

Injunctions can be made to prevent publication

The only action that can be issued against 'persons unknown'

Hampshire Waste Service v Persons Unknown [2003]

Super-injunctions forbid both the public disclosure of information on a particular issue and also any disclosure of the existence of the directive itself.

However, both types of injunction only apply within UK jurisdiction

20

Mareva injunctions (Asset freezing orders)

If a person who has 'stolen' information is identified, rapid action is often required

Mareva injunction freezes assets at short notice

Intended to prevent dissipation of assets before court judgment

Named after the (second) case to grant them: *Mareva Compania Naviera SA v International Bulkcarriers SA [1975]*

Does not transfer ownership of assets, merely prevents their use or movement

21

Anton Piller orders (Search orders)

'Search warrant' without prior warning

An order where the defendant must give permission for searchers to enter

Generally used when search is required at very short notice e.g. to prevent destruction of computer data

Anton Piller KG v Manufacturing Processes Limited (1975), dealing with the theft of trade secrets

Very destructive to targeted businesses

Reveal important business information to others

Computers may be seized and kept for months

So very high threshold:

There must be an extremely strong *prima facie* case against the respondent,

The damage, potential or actual, must be very serious for the applicant, and

There must be clear evidence that the respondents have in their possession relevant documents or things and that there is a real possibility that they may destroy such material

22

Other relevant laws

- Accessibility of websites
  - Primarily an issue for disabled people
  - Equality Act 2010; EHRC Statutory Code of Practice
- Health and Safety (Display Screen Equipment) Regulations 1992
- E-commerce
  - Contracts law, especially Consumer Rights Act 2015
- Internet Law
  - Liability of social media / ISPs for what their users publish
  - Privacy and Electronic Communications (EC Directive) Regulations 2011
    - Anti spam law. Fines up to £5,000 + damages
  - Investigatory Powers Act 2016
    - Permitted collecting internet activity and phone records and letting public bodies grant themselves access to these personal details with no suspicion of serious crime and no independent sign-off.

23

Summary

IT security laws

Criminal

Civil

Internet laws

Including e-commerce

Equality laws

Health and Safety laws

Asset freezing and search orders

24