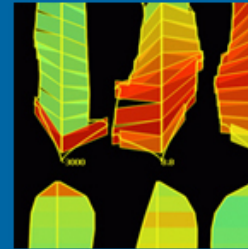
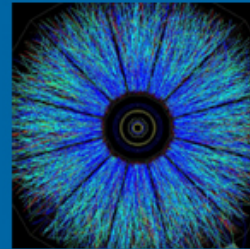
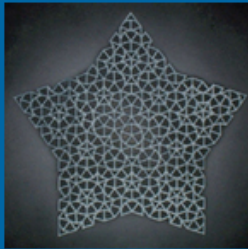




Swansea University
Prifysgol Abertawe

Legal Issues in Computing: Understanding Civil Law and the UK GDPR



Learning Goals

What are the differences between civil and criminal law?

Why do we need Data Protection

What is the core idea of the GDPR?

English (and Welsh) Law

English and Welsh Law is a huge, old, unique system of law with key elements being:

- Judicial precedent – judges are bound to follow decisions of superior courts
- Civil and Criminal distinction – crimes against society and disputes between parties are separate
- English Law has multiple sources
 - Statutes: Made by Parliament
 - Common law: Precedent as established by judges
 - EU Law: Made by the EU (for now....)

English law isn't just English USA, Canada, Australia and NZ all have similar underpinnings

Core Concepts in English Law

The Rule of Law: every person must obey the law no matter who they are and has essential components such as Equality, Fairness, Retrospective, Fairness and Due Process

Right to Trial By Jury: Anyone accused of a crime has the right to be tried in front of their peers.... but you don't always have to be

- Civil Law does not always require a jury because you are not being found guilty of a crime but are being found liable for some damages

So why is this?

*What are some of the
differences between
criminal and civil law?*

Criminal vs Civil Law

Criminal Law

Aim: is to regulate the punishment for crimes against society and the individual

Commencement: the Police and Crown Prosecution Service investigations

Burden of proof: the State to prove beyond reasonable doubt

Venue: Magistrates or Crown Court

Civil Law

Aim: to regulate relationships between individuals and other individuals and organisations

Commencement: Individuals/organisations suing other individuals/organisations

Burden of Proof: The Individual proves on the balance of probability

Venue: County Court or High Court

Criminal vs Civil Law

Criminal Law

Outcome: Conviction or acquittal

Remedy: Sentence to a punishment imposed by the state

Civil Law

Outcome: Defendants or is not liable to claimant

Remedy: Damages or other remedy such as **injunction**

Crown Prosecution Service – the people who decide whether to and then prosecute crimes brought to them by the police

Acquittal – different to being found innocent, you are not guilty

Liability – being found responsible for a harm caused

*Context out of the way – lets
focus on Data Protection*

*How much do you think your
personal data is worth?*

*\$1.70**

** For my information sold to a company buying information legally at random*

*\$240-\$300**

** Average revenue per person per year in Digital Advertising*

*\$2.97-\$50**

** Per google ad-words click through*

*\$2,733 per month**

** Amount one man sold his personal data for including
all calls, texts, location, pc usage*

\$2.80*

** Your Spotify password*

\$3.00*

** Your Netflix password*

*\$25.00**

** Credit card, address and email combined*

*5% of the balance in it**

** Online bank account*

*\$1,000**

** Full, leaked medical records*

Understanding Data Security

By now we should know that there are various possible attacks on computer systems and that there are ways to defend against those attacks

Now we look into the legal obligations that come with this issue and problems from the international nature of modern computing

A key point to understand and accept as you look at this – **you WILL handle other peoples data** in computer science based jobs and even in your degree itself

An important reminder – ignorance of the law is not an excuse for breaking the law!

A Case Study to think about

A customer ordering lingerie online notices that “customer id” appears in her URL and random ID’s give corresponding users names and shopping history

- The company’s response when contacted: *“ Well, there's no credit card numbers being displayed, so what's the big deal?”*
- Customer tells reporter *“I don't think Tammy so-and-so from Ridgefield, Connecticut, would want me to know that she ordered this or that”*
- The company's privacy policy assures discretion...

Were data protection laws violated?

In the US – ?

- ??
- ??

In the EU and UK – ?

- ??
- ??

Were data protection laws violated?

In the US – Sort of....

- US philosophy is market driven
- Each data holder must publish a policy, and can be sued if this is violated but this is a contract violation and nuanced

In the EU and UK – Yes

- If customers are identifiable from visible details, though it's not clear otherwise
- EUDPD gives strict guidance, ratified in law by member states like The GDPR

For organisations

Find out about your obligations and how to comply, including protecting personal information and providing access to official information.



Guide to data protection

Find out what your obligations are under the Data Protection Act.

Take action

[Register your organisation](#)



[Report a breach](#)



[Improve your practices](#)



Guides to the legislation

Find out about your obligations and how to comply under the Acts.



[Data protection](#)

If you handle personal information about

In your sector

Find out how to comply with the obligations in your sector.



[Education](#)

[Police, justice and borders](#)

The UK General Data Protection Regulations

ALL data in “accessible format” is covered, not just data on a computer

Failure to store data correctly can lead to fines of €20 million, or 4% of a companies annual global turnover (whichever is higher)

The GDPR describes three types of data:

- *Personal data* – name, address, NI number, passport number, any personally identifiable information must be protected
- *Sensitive data* – racial origins, sexual orientation, religion, politics, things you might be discriminated against because of
- *Credit information* – in a category of it's own



Prifysgol Abertawe
Swansea University

Legal Services and Compliance

Cymraeg



The General Protection Regulation (GDPR)

- Are You Ready?

The Data Protection Act 1998 will be replaced by the General Data Protection Regulation (GDPR) on the **25th May 2018**.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), however, there are some new elements and significant enhancements, so some things will be new and other things will need to be done differently. The major shift with the implementation of the GDPR will be in giving people greater control over their data.

Key Changes Include:

- new rules around **consent**
- more informative **privacy notices**
- **mandatory data breach notification**
- **increased fines**, **new** or **expanded rights** for data subjects
- **wider territorial scope**
- the **introduction of an accountability principle** making some measures that were previously recommended as being good practice now legally required in certain circumstances e.g. conducting **privacy impact assessments** and incorporating **data protection by design** into projects
- maintaining detailed internal **records of processing activities**
- ensuring that any third party data processing is done under **contract** in line with the

UK General Data Protection Regulation

Outlines 5 principles to follow when gathering personal data and covers any data about a living and identifiable individual

To hold or process data an individual must notify the Information Commissioners Office (ICO) of the companies status as a **Data Controller**

- While not expected to oversee each worker in them, a Data Controller must ensure sensible secure principles are applied, and that suitable training is given

Failure to comply with the Data Protection Act can result in civil claims for damages or even criminal prosecution by the ICO and CPS

GDPR Controllers and Processors

Data Controller - determines the purposes for which, duration of and the manner in which personal data is used

- Ultimately holds the responsibility for the data and meeting the DPA

Data Processor- often a sub contracted company that handles data without making key decisions about the data

- Might control how data is stored
- How data is transferred
- Specifics of the security of the data

However, just because one company contracts another it doesn't automatically make them a processor

What makes someone an “Identifiable Individual”?

Misuses of Data Protection Laws

2003 – a utility company cut power to elderly couple

- One of the couple died, cold contributed to death
- Local Social Services criticised the company for not informing them
- Utility company used DPA (GDPR equivalent) as defence

The ICO dismissed this defence saying the DPA (previous version of GDPR) doesn't override protection of life

- There is an element of 'common sense' written in to these laws



TIEDEMANN

Wider Reading

Book: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power

by Professor Shoshana Zuboff

- A heavyweight read on the problems that the current incentive structure of online transactions causes for everyday people

Receode Decode Podcast: Pete Buttigieg

- Democratic presidential nomination candidate talks about his ideas on the right to be forgotten

Freakonomics Podcast: How Spotify Saved the Music Industry (But Not Necessarily Musicians) (Ep. 374)

- Includes discussion of how Spotify was affected by the GDPR rules

Learning Goals

What are the differences between civil and criminal law

Why do we need Data Protection

What is the core idea of the UKGDPR?

Learning Goals

What are the differences between civil and criminal law

Civil law is about liability and balance of probability, criminal law is about guilt and being beyond a reasonable doubt

Why do we need Data Protection

Companies behaviour without it can be unethical and threaten our privacy or worse!

What is the core of the UKGDPR?

A set of rights and principles to protect us from intrusive, dangerous or unfair use of our personal data by making it illegal