COM6655 Professional Issues
Autumn 2021-22

Data protection, privacy and freedom of information (part 3)

Dr Maria-Cruz Villa-Uriol
Department of Computer Science, University of Sheffield
m.villa-uriol@sheffield.ac.uk

Overview

- Privacy in the computer age
- Three aspects of privacy
- GDPR (General Data Protection Regulation)
- UK GDPR (UK General Data Protection Regulation)
- DPA 2018 (Data Protection Act)
- Investigatory powers
- Summary

Automated decision making and profiling

- The UK GDPR has provisions on:
  - Automated individual decision-making (making a decision solely by automated means without any human involvement)
  - Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

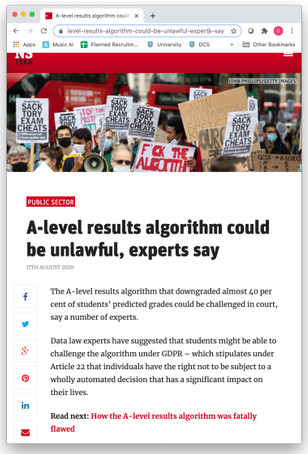
Automated decision making and profiling

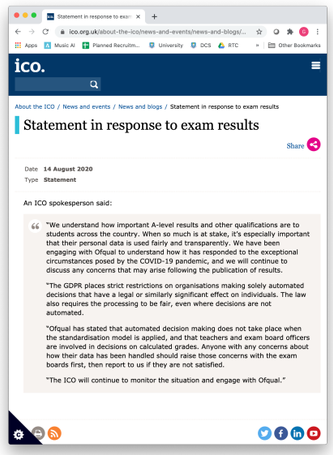
- Article 22 has additional rules to protect individuals if you are carrying out solely automated decision making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is:
  - Necessary for the entry into or performance of a contract; or
  - Authorised by domestic law applicable to the controller; or
  - Based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
  - Give individuals information about the processing;
  - Introduce simple ways for them to request human intervention or challenge a decision;
  - Carry out regular checks to make sure that your systems are working as intended.

What are significant effects?

- Automated decisions with legal or similar significant effects include, e.g.
  - Automatic refusal of an online credit application
  - E-recruitment not involving human intervention
  - Loan decisions
  - Access to health services
  - Access to education
  - Online advertising / differential pricing

Example: A-level exams (2020)





https://tech.newstatesman.com/public-sector/a-level-results-algorithm-could-be-unlawful-experts-say

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/statement-in-response-to-exam-results/

Other relevant legislation

- PECR - Privacy and Electronic Communications Regulations (EC Directive 2003) was latest updated on 29 March 2019
- PECR are derived from European law, and it is commonly know as the e-privacy directive
- The EU is currently updating its current directive, which will not automatically form part of UK law
- PECR regulates:
  - Marketing by electronic means, including marketing calls, emails, texts and faxes,
  - Use of cookies (or similar) that track information about people accessing a website or other electronic service
  - Security of public electronic communications services
  - Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID) ,and directory listings.

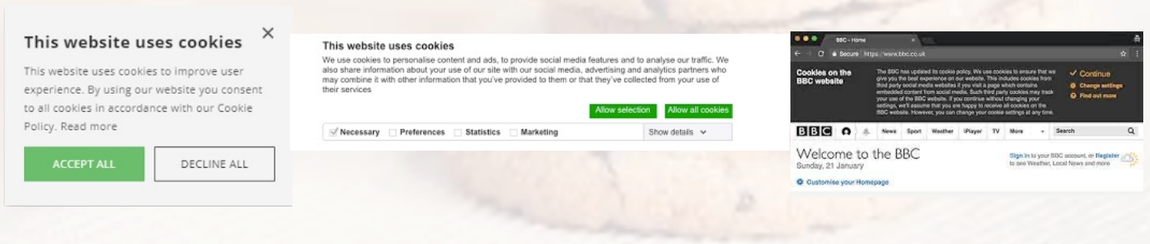
https://ico.org.uk/for-organisations/guide-to-pecr/

Other relevant legislation

- **For example, email marketing:**
  - sender must not conceal their identity, and must provide a valid opt-out address
  - senders cannot send messages unless they have the recipient's prior consent
  - some exemptions if addresses collected in the course of a sale, or negotiations for a sale

Other relevant legislation

- **Another example, cookies.**
  Basic rule is that you must:
  - tell people the cookies are there;
  - explain what the cookies are doing and why; and
  - get the person's consent to store a cookie on their device.



Information Commissioner's Office - ICO

ICO: The Information Commissioner's Office

- The responsibilities of the Information Commissioner include:
  - Compiling and maintaining a register of persons who hold personal data;
  - Serving notices to those who contravene the Act;
  - Ensuring that requests for information from individuals to persons that hold data about them are honoured.
- The Information Commissioner has a web site: https://ico.org.uk
- Enforcement
- The Information commissioner can enforce the Act by
  - Enforcement notices
  - Prosecution under the act

DPA violations

- There are various legal cases related to the earlier Data Protection Act. For example:
  - **Second Principle of Data Protection Act 1998**
    - 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 those purposes.

British Gas Trading Ltd vs. DPR (1998)

- The company wished to send marketing material to customers of previous bodies that supplied gas. Customers were informed by a statement sent with their bills and were told to write to the company in order not to receive marketing materials.
- **Decision: this breached DP principles**
  - Some of the marketing material related to services and products not connected to the supply of gas (e.g. credit card offers)
  - Customers should be able to object without having to write in – i.e. they should be asked to signify consent at the time their data was first collected
  - New customers should be able to tick an opt-out box at the time of signing their contract

DPA violations (continued)

- **Third Principle of 1998 Data Protection Act**
  - Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed. Local authorities were found to be collecting excessive information relating to Community Charge ("poll tax"):
  - **Runneymede Council v. DP Registrar (1990)**
    - Tribunal found that asking for information relating to types of property was excessive.
  - **Rhondda BC v DP Registrar (1991)**
    - Tribunal confirmed that asking for individuals' dates of birth was excessive.

More recent examples

https://ico.org.uk/action-weve-taken/

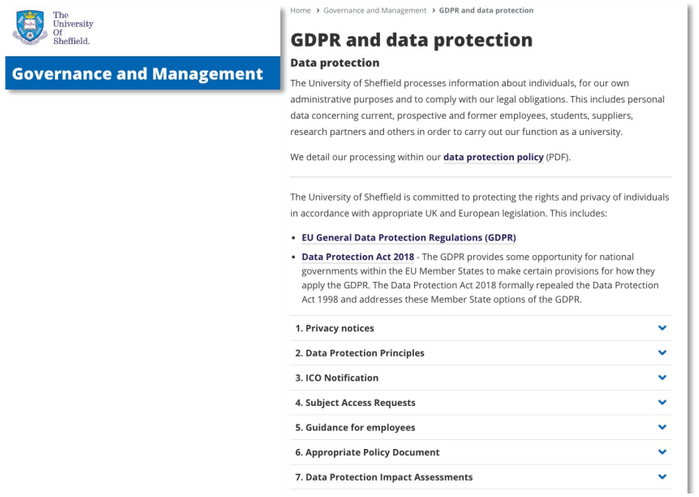
Freedom of Information Act 2000

- Drive for more transparency and 'open government'. Gives people access to information held by public authorities.
- Right to request public authorities to confirm or deny whether they hold information described in the request
- Similar rights of access to Data Protection Act.
- Also the responsibility of the Information Commissioner.
- Act popular with journalists, but many exemptions, especially for information about government
- In some cases, these requests might have some associated charges (e.g. to cover communication costs)

*Full text available: https://www.legislation.gov.uk/ukpga/2000/36/contents
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

Data protection and the University

https://www.sheffield.ac.uk/govern/data-protection



Investigatory powers

Investigatory Powers

- The Regulation of Investigatory Powers Act 2000 (RIPA) came into force in October 2000.
- Investigatory powers are the powers by which an authorised organisation can covertly gather information for investigative or intelligence purposes.
  - Part I: Interception of communications data
  - Part II: Surveillance
  - Part III: Encryption
- Amended by the Investigatory Powers Act (IPA) 2016*

*Full text available here: https://www.legislation.gov.uk/ukpga/2016/25/section/1

RIPA 2000

- *There are two distinct sets of powers under the Regulation of Investigatory Powers Act 2000 (RIPA) relating to communications.*
- *First, RIPA provides powers to intercept the content of communications, for example, by listening to telephone conversations or voicemail messages (Chapter 1 of Part 1 of the Act). The warrant is signed by the Home Secretary, Foreign Secretary, Northern Ireland Secretary or Scottish Ministers and oversight is provided by Interception of Communications Commissioner.*
- *Second is the power to acquire communications data, such as records of who contacted whom, when, from where and for how long (Chapter 2 of Part 1 of the Act). Authorisations for the acquisition and disclosure of communications data are issued by 'designated persons' within the organisations seeking the data, for instance a Superintendent in a police force …*
- https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/711.pdf

RIPA: What it means

- Certain public bodies may conduct surveillance and access a person's electronic communications in bulk:
  - Demand that an Internet Service Provider (ISP) provide access to a customer's communications in secret;
  - Mass surveillance of communications in transit;
  - Demand ISPs fit equipment to facilitate surveillance;
  - Demand that someone hand over keys to protected information;
  - Monitor people's Internet activities;
  - Prevents the existence of interception warrants and any data collected with them from being revealed in court.

Differing opinions

- “In updating law enforcement powers, we have been careful to see that individuals' rights are properly protected. This is all about a balance. We believe that RIPA strikes the right one.”
  - Jack Straw, UK Home Secretary, 2000

- "Jack Straw has reversed the usual burden of guilt: all encrypted files on your computer are presumed to be incriminating unless you can prove otherwise. Oh, and if you make any public complaint about your treatment, another five years will be added to the sentence. Only a home secretary as ingenious as Straw could invent a new crime of forgetting one's password..."
  - The Guardian (Francis Wheen, May 2000)

https://www.fipr.org/rip/

Investigatory Powers Act 2016

- *A Bill to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.*

- https://services.parliament.uk/bills/2015-16/investigatorypowers.html

Investigatory Powers Act (2016)

- “It legalises a whole range of tools for snooping and hacking by the security services unmatched by any other country in western Europe or even the US.” (Guardian, November 19th 2016)
- The legislation sets out clearly for the first time the surveillance powers available to the intelligence services and the police.
- It legalises hacking by the security agencies into computers and mobile phones and allows them access to masses of stored personal data, even if the person under scrutiny is not suspected of any wrongdoing.

A snoopers' charter?

- Civil rights and privacy campaigners called the 2016 Act a "snoopers charter"
- These Acts may be overused: is this a threat to civil liberty?
  - In 2008 RIPA was used to justify putting three children and parents under surveillance in Dorset to check whether they lived in the school catchment area.
  - Other councils have used surveillance to catch dog fouling, or fly tipping.

Objections

- Author and journalist Heather Brooke wrote in The Guardian:
  - "The spies have gone further than [George Orwell] could have imagined, creating in secret and without democratic authorisation the ultimate panopticon. Now they hope the British public will make it legitimate." (Guardian, 2015)
- Edward Snowden tweeted:
  - "By my read, #SnoopersCharter [The Draft Investigatory Powers Bill] legitimises mass surveillance. It is the most intrusive and least accountable surveillance regime in the West."

  - Source: ComputerWorldUK November 11 2015, Scott Carey

Legal challenges

- The organization Liberty has led legal challenges to the Investigatory Powers Act
- Most recently, challenged whether the Act is compatible with the European Convention on Human Rights
  - Article VI: Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
  - Article VIII: Everyone has the right to respect for his private and family life, his home and his correspondence.
- Legal challenge was unsuccessful: deemed that sufficient safeguards are in place in the Act.
- https://homeofficemedia.blog.gov.uk/2019/07/29/judgment-in-investigatory-powers-legal-challenge/

Summary

- Governments must find a fair balance between respecting privacy and the freedom of information.
- Data Protection Act 1998 enforced the principle that every individual should have the right to know what information is stored about him or her on computer, and the purpose for which it is used.
  - Replaced by GDPR and UK Data Protection Act 2018
  - After the Brexit transition period, personal data processing is regulated by the UK GPDR and DPA 2018
  - UK GDPR maintains the GPDR principles, and mostly affects transborder data transfers
  - The DPA 2018 imposes obligations on data users, and provides access rights to individuals.
  - Differences to earlier DPA - greater emphasis on transparency
- Freedom of Information Act 2000: access to information held by public authorities.
- Investigatory Powers Act 2016 provides a statutory framework for surveillance, including 'interception' of data communications via an ISP. It is highly controversial.