DIGITAL PRIVACY

KNOW

The dramatic expansion of the internet over the past twenty years has presented us with new challenges regarding human rights, specifically the balancing of the rights to freedom of the media and freedom of expression on the one hand, and the rights to privacy and data protection on the other.

Typing one's name into a search engine, however unknown we may consider ourselves to be, can wield a range of results about ourselves, from social media pages to news and other forms of information. Most of us have a digital identity made up of fragments of the past and present, which persist over time. This digital identity is knowingly or unknowingly used by other actors on the internet for purposes we may not be aware of.

Edward Snowdon's revelations in 2013 about the surveillance programmes operated by the US' National Security Agency and the UK's GCHQ[1] have heightened concern about the protection of our right to privacy and data protection in Europe.

Both the right to a private life and the right to data protection are protected under EU law and the European Convention on Human Rights. Neither are absolute though – your right to privacy and data protection may be limited in certain circumstances. Making use of these exceptions, government surveillance programmes have relied on national security to justify intrusions into privacy. These restrictions have been made all the more difficult to question as information on these limitations is kept secret. The development of the right to be forgotten also raises serious questions over the role of private companies in deciding when a right has been violated.

UNDERSTAND

The right to privacy and the right to data protection are protected under the EU's Charter of Fundamental Rights in Articles 7 and 8 respectively. The right to a private life is also protected in the European space and in all EU countries under Article 8 of the European Convention on Human Rights. Data protection is regulated throughout the EU under the Data Protection directive, passed in 1995, which required EU member states to pass national laws on data protection.

The 1995 Data Protection Directive ensures that individuals have strong rights over the processing and controlling of data concerning them, including the right to object to the processing of data and the right to access data. The "controller" of the data must ensure that information is collected for "specific, explicit and legitimate purposes," and must make every

---

[1] http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

effort to ensure that the data is accurate, and rectify or erase it if it is not. The Data Protection Directive does however impose the obligation of Member States to provide a number of exceptions in cases of public interest, for example the same data protection standards do not apply in instances of journalistic or artistic or literary expression.

Recent rulings by the European Court of Justice have stated that, "the right to data protection is not … an absolute right but must be considered in relation to its function in society," and should be measured using the principle of proportionality. Freedom of expression in particular often comes into conflict with the right to data protection, given its nature as another fundamental right which, in contrast to the prohibition of torture or slavery say, is not absolute and instead has to be "viewed in relation to its social purpose."

The EU's data protection regime It is also going through a process of revision. In 2012 the European Commission proposed a new data protection regulation, which would seek to harmonise the way member states deal with data protection, explicitly include the right to be forgotten and obliging non-European firms offering services to Europeans to conform with EU data privacy rules.[2]

WHEN CAN MY DATA BE COLLECTED?

- Your data can only be processed if it is based on one of the following criteria: your consent, necessary for a contract, in your vital interests, in the legitimate interests of others (but only so long as your fundamental rights do not override this legitimate interest), or where it is in the public interest.
- Sensitive data has a stricter requirement for consent to be explicit and does not allow collection of data solely for a contract. Sensitive data includes information on your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex life.
- It must be lawfully collected, which means not only that a specific law exists which allows the governmental body or company to collect your data, but that the law must be for the one of the purposes listed in the Directive or for the rights and freedoms of others. It must also be necessary in a democratic society, which means that the data collection corresponds to a pressing social need and the way is proportionate to the purpose.
- The purpose of collecting the data must be specifically and visibly defined before data is collected. Collecting data for an unspecified purpose is unlawful. Transferring data to a third party requires a legal basis.

---

[2] http://ec.europa.eu/justice/data-protection/

- Only data that is adequate, relevant and not-excessive for its purpose should be collected and data must be chosen based on the declared aim. The person collecting the data must also check that it is accurate and up-to-date. Importantly, data must not be kept in a way that allows persons to be identified for longer than is necessary for the purposes of the data collection. It can however be kept for longer if anonymised.
- People holding your data must keep you informed about how your data is being used and as far as possible, must act in a way which promptly complies with your wishes towards your data.
- Persons holding your data have an obligation to protect the security and confidentiality of that data. Telecommunications providers are obliged to tell you if your data security has been breached.

WHAT RIGHTS DO I HAVE UNDER THE DATA PROTECTION DIRECTIVE?

You have the right to:

- be informed if any person or company is holding your personal data in their files (websites, databases, service providers, etc.)
- correct or delete your data if it is incomplete or inaccurate
- be fully informed and give your agreement if a website wishes to store and retrieve information from your computer or to track you when you're online
- confidential online communication (e.g. e mails)
- be notified if your personal data held by a service provider has been lost, stolen or otherwise disclosed, and your privacy is likely to be adversely affected
- not be sent unsolicited advertising (spam)

EUROPEAN ALTERNATIVES

This project is funded by the Fundamental Rights and Citizenship programme of the European Union

CITIZENRIGHTS
A project by European Alternatives