Data Protection, Privacy & Freedom of Information

Chapter 14

Course Instructor: Engr. Saeeda Kanwal

Chapter Outcome

After studying this chapter, you should:

- *understand the concerns that led to the passing of legislation regarding data protection, freedom of information and privacy of communications;*
- *be familiar with the data protection principles enshrined in UK law;*
- *understand the main obligations that legislation in these areas imposes on the information systems professional.*

Why is privacy an important issue?

In recent years there has been a growing fear about the large amount of information about individuals held on computer files.

In particular it was felt that an individual could easily be harmed by the existence of computerised data about him/her which maybe inaccurate or misleading and which could be transferred to an unauthorised third party at high speed and very little cost.

The Data could be…

- **Healthcare** records
- **Criminal justice** investigations & proceedings
- Financial institutions & transactions
- **Biological** traits, such as genetic material
- **Residence** and geographical records
- **Ethnicity**
- Privacy breach
- Location-based service and geolocation

Criticism of Facebook (Privacy concerns)

Electronic Frontier Foundation (You create a "Connection" to most of the things that you click a "Like button" for, and Facebook will treat those relationships as public information.)

Facebook Beacon 2007

> “Beacon was a part of Facebook's advertisement system that sent data from external websites to Facebook, for the purpose of allowing targeted advertisements and allowing users to share their activities with their friends.”

Publish user activity from other websites without explicit permission from the user.

Cooperation with government

Data mining : "We may use information about you that we collect from other Facebook users to supplement your profile”

Inability to voluntarily terminate accounts (previously)

Photo recognition and face tagging 2011

Timeline

Psychological effects

The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Women

Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video Games

HOME » TECHNOLOGY » GOOGLE

Google must delete your data if you ask, EU rules

Europe's top court has backed the controversial 'right to be forgotten' but experts doubt it will work in practice

By Matt Warman, and David Barrett
11:06AM BST 13 May 2014

Comments

The European Union's top court has ruled that data about individuals held by Google must be deleted on request.

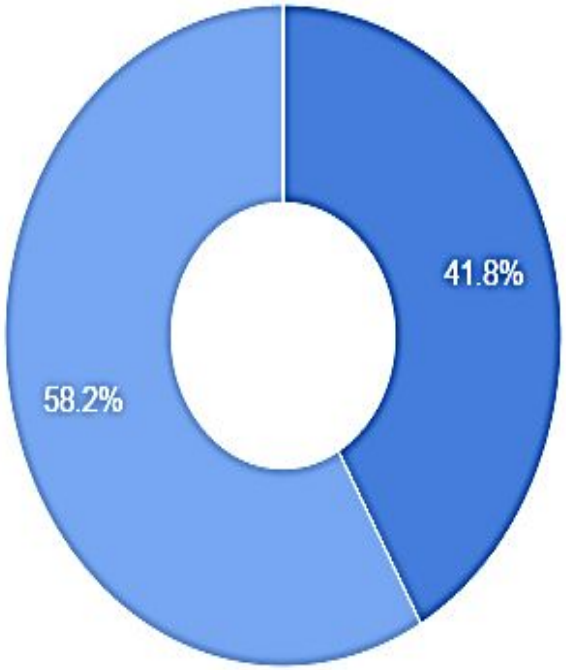
The statistics here reflect the number of law enforcement agency requests for information we receive at Google and YouTube, the percentage of requests that we comply with (in whole or in part) and the number of users or accounts specified in the requests. We review each request to make sure that it complies with both the spirit and the letter of the law, and we may refuse to produce information or try to narrow the request in some cases.

January to June 2014

Country	User Data Requests	Percentage of requests where some data produced	Users/Accounts Specified
Finland	17	94%	31
United States	12,539	84%	21,576
Lithuania	6	83%	7
Netherlands	72	82%	95
New Zealand	24	79%	45
Japan	121	77%	164
Belgium	213	73%	513
United Kingdom	1,535	72%	1,991

URL removal request totals

The graph below shows data on the percentages of URLs we have reviewed and processed. The figures on the right are based on the total number of requests received. These data date back to the launch of our official request process on May 29, 2014.



URLs Removed URLs Not Removed

All | FR | DE | GB | ES | IT | Other Countries

Total URLs that Google has evaluated for removal: **554,487 URLs**

Total requests Google has received: **165,395 requests**

The graph reflects URLs that have been fully processed, while the figures above reflect the total evaluated. URLs that require more information or are pending review are not included in the graph.

What is the Data Protection Act?

Freedom to process data vs. privacy of individuals.

1984 act was repealed by the 1998 act.

Anyone who processes personal information must comply with the eight principles

It provides individuals with important rights, including the right to find out what personal information is held about them

Data protection act 1998

Main objective of Data Protection Act was designed to protect individuals from:

the use of inaccurate personal information or information that is incomplete or irrelevant;

the use of personal information by unauthorized persons;

Use of personal information other than the intended purpose

Terms of the data protection Act

Technical terms used in the act:

Personal data: Its an information about a living individual

Data users: are organisations or individuals who control the contents of files of personal data – i.e. who use personal data which is covered by the terms of the act

A Data subject: is an individual who is the subject of personal data

Data controller: means a person who determines why or how personal data is processed. This may be a legal person or a natural person.

Rules of Data Processing

The rules regarding the processing of sensitive personal data are stricter than for other personal data.

Processing means obtaining, recording or holding the information or data or carrying out any operations on it, including:

(a) organization, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the info or data,

Rules of Data Processing…..

(c) disclosure of the info or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

This is an extremely comprehensive list and it is difficult to imagine anything that one might do to personal data that is not included within it.

The Act provides for the appointment of a Data Protection Commissioner and the establishment of a Data Protection Tribunal.

How can the Data Protection Act help us?

- It gives us the right to see our files
- It says those who record and use personal information must be open about how the information is used.
- It must follow the 8 principles of '*good information handling'*

Main principles of the 1998 Act

Personal data must be:

- *fairly and lawfully processed*
- *processed for limited purposes*
- *adequate, relevant and not excessive*
- *accurate not kept for longer than is necessary*
- *processed in line with your rights*
- *held securely*
- *measures shall be taken against unauthorized or unlawful processing of personal data & against accidental loss or damage*
- *transferred to countries with adequate data protection*

First data protection principle

Personal data shall be processed fairly and lawfully and in particular shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met and

(b) in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The most significant condition in Schedule 2 of the Act is that the data subject has given their consent.

If this is not the case, then the data can only be processed if the data controller is under a legal or statutory obligation for which the processing is necessary.

Second data protection principle

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 that purpose or those purposes.

Data controllers must notify the Information Commissioner of the personal data they are collecting and the purposes for which it is being collected.

Third data protection principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Many violations of this principle are due to ignorance rather than to intent to behave in a way contrary to the Act.

Local government has a bad record of compliance with this principle, for example shops that demand to know customers' addresses when goods are not being delivered are also likely to be in breach of this principle.

Fourth data protection principle

Personal data shall be accurate and, where necessary, kept up to date.

While this principle is admirable, it can be extremely difficult to comply with.

In the UK, doctors have great difficulty in maintaining up-to-date data about their patients' addresses.

Particularly patients who are students, because students change their addresses frequently and rarely remember to tell their doctor.

Fifth data protection principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This principle raises more difficulties than might be expected:

- It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time.

Sixth data protection principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

The rights of data subjects are discussed in the next subsection.

Seventh data protection principle

Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Of the eight principles this is the one that has the most substantial operational impact.

It implies the need for access control (through passwords or other means), backup procedures, integrity checks on the data, vetting of personnel who have access to the data, and so on.

Eighth data protection principle

Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This principle can be viewed in two ways. It can be seen as protecting data subjects from having their personal data transferred to countries where there are no limitations on how it might be used.

Eighth data protection principle…..

It can also be seen as specifically allowing businesses to transmit personal data across national borders provided there is adequate legislation in the destination country.

In practice, of course, if a website is physically located in a country that does not have adequate data protection legislation, a visitor to that website from a country that does have such legislation has no protection.

Rights of Data Subjects

The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

The 1998 Act extends this right of access so that 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 organizations to which it may be disclosed;
- an intelligible statement of the specific data held about them;
- a description of the source of the data.

Data protection Act in Pakistan

The following Data Protection acts Exists in Pakistan:

The electronic data protection and safety act 2005

Prevention of Electronic Crimes Ordinance, 2007, 2008, 2009, 2012.

Prevention of Electronic Crimes Act, 2014

Data protection Act in Pakistan….

Due to the increasing threat of security, a number of acts and regulations have been implemented in most countries.

These Acts allow government security services and law enforcement authorities to intercept, monitor and investigate electronic data only in certain specified situations such as when preventing and detecting crime.

Powers include being able to demand the disclosure of data encryption keys.

Data protection Act in Pakistan….

Organizations that provide computer and telephone services (this includes not only ISPs & other telecom service providers but also most employers) can monitor and record communications without the consent of the users of the service, provided this is done for one of the following purposes:

To establish facts, for example, on what date a specific order was placed;

To ensure that the organization's regulations and procedures are being complied with;

To ascertain or demonstrate standards which are or ought be to be achieved;

Data protection Act in Pakistan….

To prevent or detect crime (whether computer-related or not);

To investigate or detect unauthorized use of telecom systems;

To ensure the effective operation of the system, for example, by detecting viruses or denial of service attacks;

To find out whether a communication is a business communication or a private one (e.g. monitoring the emails of employees who are on holiday, in order to deal with any that relate to the business);

To monitor (but not record) calls to confidential, counselling helplines run free of charge by the business, provided that users are able to remain anonymous if they so choose.

Freedom of Information

The primary purpose of the Freedom of Information Act is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information.

The Act also provides an enforcement mechanism if the information is not made available.

The legislation applies to Parliament, government departments, local authorities, health trusts, doctors' surgeries, universities, schools and many other organizations.

Freedom of Information Ordinance 2002

Under the Freedom of Information law, any citizen can seek any information or record from any public body, except for information categorized by law as exempt from disclosure.

The Right to Information Act (RTI) is an Act of the Parliament of India "to provide for setting out the practical regime of right to information for citizens" and replaces the erstwhile Freedom of information Act, 2002.

In Pakistan, KPK and Punjab assemblies have also passed RTI acts in 2013.

Freedom of Information

Unlike the other legislation discussed here, the Freedom of Information Act creates a requirement for new information systems and for packages that can be used to develop them.

Such systems are commonly known as record management systems and document management systems.

References:

http://www.google.com/transparencyreport/removals/?hl=en