Data Protection – Responsible Entrepreneurship : the role of Blockchain and Privacy in the Digital Society

Iraklis Paraskakis
Professor, Computer Science Department,
CITY College, University of York, Europe Campus
Senior Research Officer, SEERC

The context and motivation of today's talk

- Data
- Use of data
- Industry 4.0
- Massive Individualisation
- Retail is Data Dependent
- Government is Data Dependent
- Everything is Data Dependent

Why we need privacy?

- Do we need privacy?
- How is privacy been understood?
- Can we use privacy to deter access for legitimate reasons?
- Are there legitimate reasons for collecting data and processing data?
- What could be such reasons?

- Look at work of Prof Shoshana Zuboff
  - In the Age of the Smart Machine 1988
  - The Age of Surveillance Capitalism 2018
  - See the video from YouTube: https://www.youtube.com/watch?v=hIXhnWUmMvw

So what is the solution to privacy from a practical perspective

- Two solutions so far:
- The USA solution
  - NO framework
  - up to individual

- The EU way:
  - Provide a framework for enabling fair play

- The result: A huge point of friction between the US and EU to the point of having a trade war because of such legislation

Contents for Privacy IPR & Bloackchain

- What is Privacy?
- What is Intellectual property?
- Blockchain Challenges and Opportunities in above areas

The world of Privacy

- Privacy is governed in Europe mainly by Data Protection Act 1995 (an EU directive) and latest update is General Data Protection Regulation (GDPR) (an EU regulation) introduced in 2016 and activated in May 2018.
- Data protection was raised as an issue in UK back in 1965 and they were granted an Act in 1984, which was replaced in 1998 by the Data Protection Act and ultimately surpassed in 2018 by GDPR.
- GDPR is a point of friction between Europe and USA – huge point of conflict.
- Reflects different philosophies – that of trying to regulate the use of Data in the Digital Economy and Digital Society.
    - Europe is favouring a regulated environment that combines the needs f business as well as offer protection to natural persons.
    - USA believes that each individual is free to choose and select whether data is collected or not, so it is up to individual.
    - Not true since data collection is not direct and active but rather passive – e.g., security cameras – use of credit cards etc.

Privacy in some details

- To understand the principles and philosophy of Privacy and Data Protection you are better to view the principles of Data Protection Regulation since its philosophy is encompassed in 8 principles which are easy to understand
- GDPR is described in 110 articles which make it difficult to convey and make it comprehensive in a seminar, hence the reference to Data Protection Act since GDPR with a few exceptions really builds on Data Protection and reflects and includes the experience of over 15 years of usage and testing of Data Protection Act with Data Protection Authorities as well as decisions from Courts.

Data Protection is now enforced across the universe through the demand for all companies that trade with EU customers to abide GDPR

DIGI GRENT

- Another clarification/stricter enforcement of Data Protection is that the emphasis is on the protection of the individual and not on companies whose seat is in the EU.
- This way any company on the world that does business with an EU citizen must now observe and apply GDPR of the EU citizens. An opportunity for Blockchain. The company is no longer required to have a physical presence in the EU. Overcomes cases such as Cayman Islands (lands of opportunities).
- Possible use of blockchain as a way to ensure that a certain webpage is visited by an EU citizen that does not use VPN facilities.

- What follows, in the following slides, is an analysis of the Data Protection Act (DPA) 1997, which is the same in spirit with the GDPR. I analyse the DPA since it is easier to be taught and the differences are not that great with the only exceptions being mainly the
- Right to be forgotten
- Right to have your data transferred to another Data Controller in interoperable format
- The establishment of a DPO – which is really a formalisation and a tightening of the organisational and operational obligation from DPA.
- Carry out of the Risk analysis – this was not provisioned in the DPA

Objectives of the Act

- From the EC Directive: the objective is

'.. to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data'.

- The Act gives legal rights to individuals (data subjects) in regard to personal data held about them by others, e.g. the right to have incorrect data erased or amended.

- The Act appoints a Data Protection Commissioner (formerly 'registrar'), whose responsibilities 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 Hellenic Data Protection Commissioner has a web site :

http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL

- The UK Office of the Commissioner has a web site:

http://www.ico.gov.uk/

Terms used in the Act

- Data
- Data Controller
- Data Processor
- Data Subject

Data

- Data means information which

(a) is being processed by means of equipment operating automatically;

(b) is recorded with the intention that it should be processed;

(c) is recorded as part of a relevant filing system;

(d) forms a record of the health or education of an individual or is kept by a Local Authority for housing or social security purposes.

- A relevant filing system is one which is not automatically processed, but in which the data is 'structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that information relating to a particular individual is readily accessible'.

Q. Which of the following are data?

- A library catalogue on microfiche.
- An account number on a cheque.
- Employee records stored on a card index system.

Data Controller

- A person who (alone or with others) determines the purposes for which and the manner in which the Personal Data is to be processed.

Data Processor

- A person (other than an employee of the Data Controller) who processes Personal Data on behalf of the Data Controller.

- Examples:
  - A self-employed market researcher;
  - ISPs that provide Internet access to clients who transfer Personal Data via the web or email.

Data Subject

- An individual who is the subject of Personal Data.

Q. Why does this definition refer to an ‘individual’ but the others refer to a ‘person’?

Personal Data

•Data about a living individual who can be identified from that data, or from that data and other information which is in the possession of the Data Controller.

•This includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Processing

• Processing means obtaining, recording or holding data, or carrying out any operations on data including:

organisation, adaptation, alteration retrieval, consultation or use disclosure by transmission or dissemination alignment, combination, grouping, erasure or destruction

Q. Can you think of any action, which might constitute processing and is missing from the above definition?

list is intended to be exhaustive

Registration and Offences

• Data Controllers and Data Processors (now under GDPR) both must register with the Commissioner.

The following must be given:

- a description of the Personal Data to be processed;
- details of the purposes for which the data is processed;
- details of any recipients to whom the Data Controller intends to disclose the data;
- the names of territories outside the EU to which the Data Controller intends to transfer the data.

• Failure to register is a strict liability offence, subject to a maximum £5000 fine in the Magistrates' Court or an unlimited fine in the Crown Court.

• Operating outside the terms of registration is also an offence. Same penalty as above, but a defence is available if due care has been taken.

Q. Your registration allows you to transfer data to France, but due to Internet problems it is routed via the USA. Is this an offence under the DPA?

This is even more of a problem now with Cloud Computing. Why?

• The Act defines other offences too, e.g. enforced subject access, unlawful selling of personal data.

The Data Protection Principles

- A breach of the following principles is not a criminal offence, but allows the Data Subject to seek damages.

- The Commissioner may issue an enforcement notice requiring that a Data Controller abide by the principles. It is a criminal offence to ignore such a notice.

- If a judge believes that the principles have been broken, a warrant allowing the Commissioner to search the Data Controller's premises may be issued.

First Principle

- Personal Data shall be processed fairly and lawfully, and shall not be processed unless at least one of the following is satisfied:

    - the Data Subject has consented;
    - the processing is necessary for the performance of a contract with the Data Subject;
    - the Controller has a legal obligation to process the data;
    - the processing is necessary for legitimate interests
    - pursued by the Data Controller.

- Consent need not be explicit - it may be implied, for example by failure to tick a box on a form.

- An exception concerns the processing of ‘sensitive’ data - this requires explicit consent of the Data Subject, unless the processing is required by law in connection with employment.

- Sensitive data is that which concerns racial origin, political opinions, sex life etc.

Second 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 those purposes.

- *British Gas Trading v. DP Registrar (1998)*

See Bainbridge p. 395

BGT acquired companies (including Goldfish credit card) and placed all customers on mailing list, telling them they could write in to have their names removed. Held to be unfair - customers should be able to object without a positive act such as writing in, and some products were not directly related to gas. New customers could opt out by ticking a box..

Third Principle

- Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.

- *Runneymede Council v. DP Registrar (1990)*

  See Bainbridge p. 369

  Runneymede collecting information on poll tax. Information about type of property held to be excessive.

- *Case with Alitalia in Athens Airport v. HDPA (2003)*

  See http://www.epractice.eu/en/news/283820

  Voluntary use or biometrics to establish identity of passengers

  Was deemed as excessive since there were other means to establish identity of passengers - passports

Fourth Principle

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

- The Data Controller must take 'reasonable steps to ensure the accuracy of the data' – it cannot be assumed that data originating from a Data Subject or third party are accurate.

Q. How might out-of-date data harm someone?

- Case in Greece (around 2004), and was decided by court in Larisa.

A person applied for a credit card, but was refused. He was told that his was listed in Tiresias with a default. He complained and was awarded compensation of 5000.00 €. The entry in Tiresias was not accurate and up to date. He had acted as a guarantor to a loan. Borrower had not paid installments and the Bank listed both the borrower and the guarantor in Tiresias, although guarantor had paid the installments after he was notified.

Fifth Principle

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

Sixth Principle

- Personal data shall be processed in accordance with the rights of Data Subjects under the Act.

- For example, this principle will be breached if the Data Controller fails to give the Data Subject access to a copy of his data when requested to do so.

Seventh Principle

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or damage.

- A Data Controller must choose a Data Processor who provides sufficient guarantees in respect of this principle (there must be a written contract ensuring this).

Eighth Principle

- Personal data shall not be transferred to a territory outside the EU unless that territory ensures an adequate level of protection for the rights and freedoms of Data

  Subjects in relation to the processing of Personal Data.

- There are exceptions to this; for example, if the Data Subject has consented to the transfer.

The Rights of Data Subjects

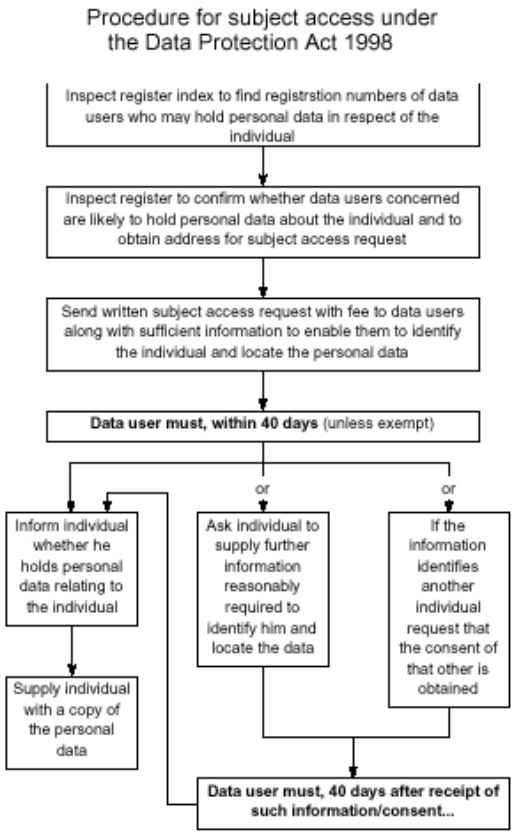
- When requested, and on payment of a fee to the Data Controller, a Data Subject is entitled to be told:
    - whether data is held about them;
    - if so, what data is held, the purposes for which it is being processed and who it is being disclosed to;
    - the logic involved in any process which makes a
    - decision about them using fully automated means;
        - **Q. When might such automated decisions be made?**

The Rights of Data Subjects (cont'd)

Rights to prevent processing

- An individual can serve a written notice on a Data Controller requiring them not to process data which is likely to cause them (or others) damage or distress.
- An individual can require that a Data Controller not use their data for purposes of direct marketing.
- An individual can require that their data is not used for making decisions that affect them purely by automatic means.

The procedure for Data subject access



The steps defined in this diagram could be stipulated in a central system that accepts all requests from data subjects logs them and ensures that Data Controllers receive them and apply the prescribed procedure and reply as required and expected and no dispute exists for lost emails etc.

Controversial provision with GDPR: The right to be forgotten or the right to erasure

- This rationale for this right has a noble motivation
- The rationale is to allow a citizen to press restart
- The rationale is to force erasure of past data, that characterises one's past to be wiped out
- Huge implications for Health records – anticipated to be decided at national level by member states define what is allowed and what is not.
- Very controversial – UK tried to exclude from GDPR all medical records – Working Group 29 was outraged. Even more with Germany that tried to exclude from GDPR all records held by civil service
- It is controversial as it is collides head on with the very desirable property of Blockchain – immutability - not able to change a record or its contents.
- A problem that is been looked up and some solutions are found – research ones not used in real life situations.

Thank you!