Aspetos Socio Profissionais da Informática

Privacy and the GDPR (General Data Protection Regulation)

José Legatheaux Martins

Departamento de Informática da

FCT/UNL

Lecture Outline

- What is privacy
- Privacy and the Law
- GDPR
- The Way Forward: is GDPR effective?

These slides are vey partially based on slides from the University of Glasgow and from Danny Palmer on ZDNet

Privacy Origins

- It is a very old, complex and fuzzy concept
- It was absent in old nomadic societies and also quite restrained in rural villages
- It was born with urban life, commerce and complex social relationships, at the same time as contracts, police and laws, to protect citizens from each other, specially from public "powers"
- Publilius Syrus (Roman writer of first century): "The one who reveals publicly your privacy, cannot be your friend"

Why Privacy?

- Our social life is a complex mix of cooperation and competition over resources
- If "society" knew everything on everyone, for example his intentions or her thoughts, society could protect itself from thiefs, burglars, terrorists, …
- Who could be the gatekeeper of that information, guaranteeing it would not be misused?
- What is law if evidence became superfluous?
- Some authors calls it the "the big brother society"

Privacy is Needed to Protect Persons and their Freedom

- Physical privacy: to protect your home from strangers
- To protect you from public powers abuses
- To protect you from discrimination (race, religion, opinions, ...)
- To refrain others of using their knowledge about you at their own advantage in contracts, negotiations, relationships, with rumours, …
- Lake of privacy can have serious consequences in the relationships with individuals that may want to take advantage of you
- **What is privacy? Is the right that a person has to control the disclosing of his or her personal information**

Your Privacy Rights are Protected by …

- Article 12 of United Nations Declaration of Human Rights
- Article 8 of the European Convention on Human Rights
- Artigo 35° da Constituição da República Portuguesa
- Lei de proteção de dados – Lei n.° 67/98 de 26 de Outubro
- Regulation EU 2016/67 – General Data Protection Regulation (GDPR)

Data is a Valuable Asset

- For Good
  - Data on commuters can be used to optimize urban transports
  - Data on people genome, diseases, ancestors, is a key asset to study public medicine and prevent your future illness
- For Bad
  - Data on what you need and know, is key to sell you products
  - Data on how you feel, or on the people you trust, is key to influence your opinions
  - To influence people is key to win wars

GDPR is an European Union Regulation

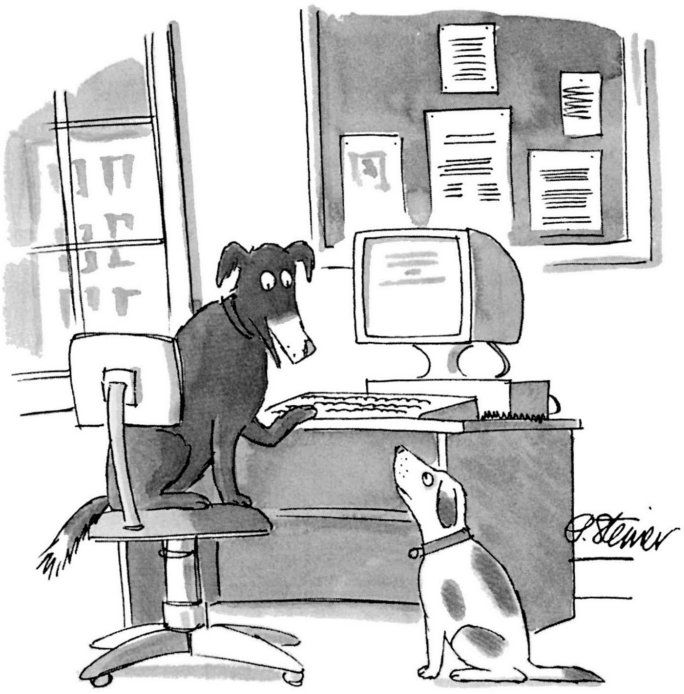
Image: iStock

General Data Protection Regulation

- At its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy

- The reforms are designed to reflect the world we're living in now, and brings laws and obligations - including those around personal data, privacy and consent - across Europe up to speed for the internet-connected age

Privacy in the Information Age



"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

- *On the Internet they know you're a dog*
- If you do a lot of posts in social networks, probably they know you better than your psychiatrist
- They also know:
  - The name of your owner
  - Your preferred can food
  - Where you go for a walk
  - In which trees you prefer to pee

What is Personal Information

- The types of data considered personal under the previous legislation included name, address, images and photos

- GDPR extends the definition of personal data. New additions:
  - Online identifiers, Device identifiers,
  - Cookie IDs, IP addresses,
  - Pseudonymised data,
  - Sensitive data includes genetic and biometric data

Data Controllers and Data Processors

- A controller is "a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data"

- A processor is "a person, public authority, agency or other body which processes personal data on behalf of the controller"

- A controller can also be the processor or outsource this processing to an external processor

New and Expanded Rights

- Right to be informed and need to informed consent (explicit opt-in)
- Right to erasure
- Right to data portability
- Right to rectification
- Right of access, including additional processing details
- Right to prevent automated processing, including profiling

Changes to Privacy Notices and Consent

Privacy Notices:

- More robust, concise, transparent, understandable and accessible
- Must explain personal data processed, purpose of processing, intended retention, subject rights, source of data, conditions of processing

Consent:

- Freely given, specific, informed, unambiguous,
- Demonstrable by a statement or clear affirmative action

Data Protection by Design

- Requirement for increased accountability and documentation of processing activities
- Data protection concerns reflected into design of all procedures, projects, systems
  - Good data protection compliance should be default
- Privacy Impact Assessments required for new activities and undertakings
  - Particularly for profiling, surveillance, and processing of special categories of personal data

GDPR Compliance

Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so

Data Controllers and Data Processors

- GDPR ultimately places legal obligations on a processor to maintain records of personal data and how it is processed, providing a much higher level of legal liability should the organisation be breached.

- Controllers will also be forced to ensure that all contracts with processors are in compliance with GDPR

- Even if the breach is caused by a processor, the controller is also liable

Breach Reporting and Sanctions

- Data breaches inevitably happen. Information gets lost, stolen or otherwise released into the hands of people who were never intended to see it - and those people often have malicious intent
- Mandatory breach notification
- Notify Information Commissioner (Comissão Nacional de Proteção de Dados - CNPD) within 72 hours
- Sanctions of up to €20,000,000 or 4% of annual worldwide turnover

GDPR Advantages for Business

- Instead of having to deal with 28 different laws

- GDPR establishes one law across the continent and a single set of rules which apply to companies doing business within EU member states

- The Commission claims GDPR will save €2.3 billion per year across Europe

- This means the reach of the legislation extends further than the borders of Europe itself, as international organisations based outside the region but with activity on 'European soil' will still need to comply

Image: iStock

GDPR took effect on 25 May 2018

GDPR One Year Later

- The Click to Accept Syndrome
- Are consumers more protected?
- Do they have alternatives to "one size fits all"?
- Three different scenarios
  - small traditional business
  - small and medium business or agencies dependent on the digital to deal with the public (e.g. banks, supermarkets, press, public services, …)
  - the giant GAFA companies (Google, Amazon, Facebook, Apple)

Barriers to Progress

- The business model: "free" service in exchange of your data
- How to price individual data?
  - Probably, all services providers should be obliged to also provide a paid version of their services at a reasonable price
  - Music and movies distribution, some news services, newspapers and Apple News are signs of new business models
- Major things missing
  - Real fight against monopolies
  - Sets of easily recognizable privacy signs (e.g. devices power consumption classification)
  - More public awareness on privacy concerns

Some Good Signs

- Technology
  - Solid (web decentralization project) Tim Berners-Lee project
  - Homomorphic cryptography
  - A cheaper way of making micro payments in an annonimous way
- Public awareness is rising
- In response, a new wave of companies is monetizing the new opportunity of offering paid-for services with heightened privacy
- Does privacy will become something only the rich can pay?

Conclusion

- Personal data became a commodity and a valuable asset for governments, public institutions and businesses
- Personal data mining is a promising tool for human progress in medicine, administration, urban management, …
- But is also a powerful weapon against individual rights
- Will privacy concepts change in the near future?