ETHICS & DATA PROTECTION

Michèle Barbier
Ethics Expert for the European Commission
Institute for Science & Ethics
Data protection

Let’s face... we are not Superman... or Super Woman!

Let’s try an ethical approach
3 Digital phenomena

- Artificial intelligence progresses exponentially,
- Advances of the machine learning in everyday life: connected objects: Smartphones, televisions, speakers, cars or watches, that exchange between them, which will soon offer them a great Contextual knowledge
- Human/Machine Interfaces are made every day more natural
3 Digital phenomena that are developing

- Natural Human/machine interfaces
- Use of sophisticated voice recognition, heat, motion, micro-expression sensors
- "Classic" interfaces, based on screens and buttons do not disappear => More and more Discreet by integrating into all everyday objects or taking new forms,
- Example: Glasses of mixed reality.
Spectacular success of Virtual assistants: Alexa, Siri or Google assistant:

- Invisible interfaces that are addressed in a simple and natural language.
- Thanks to AI, these programs learn to understand us better and to know each new request.
- The list of their functions lengthens as they interconnect with each other.
Example: Amazon and Microsoft have just signed a partnership to allow Alexa and Cortana to communicate or with other services like Uber, Shazan or Kayak
These three phenomena are linked and mutually reinforcing.

Because connected objects are packed with sensors and communicate, they gain in contextual intelligence.

This technology is more and more intelligent, we can interact with it in an ever more intuitive way and it makes us ever more important services.

Because it is more and more intuitive and useful, it is always more deeply integrated into every aspect of our everyday life.

And because it is always more deeply integrated, we interact with it without even realizing it — until it simply anticipates our needs.
**Few examples**

- Your car will give the order to your parking garage door to open and will automatically turn on the lamps of your living room if it is dark;

- Your mattress will calculate your body temperature and automatically adjust the room's air conditioning to optimize your sleep cycles;

- Your digital diary will program your alarm clock, prepare coffee and automatically order a taxi if it finds that you are flying abnormally early for a business trip.
The future: Permanent exchange between these interfaces emerged, and submerged, by linking various platforms to meet consumer needs.

1. I receive every month a face cream tailored L'Oréal concocted by algorithms and experts taking into account my lifestyle, my age, my type of skin, etc. If my L'Oréal account is watching an explosion of business trips in recent times, it will automatically adapt the cocktail to combat fatigue and propose me to book at a preferential price a treatment in a SPA near my home or directly on Place on my next trip.

2. I watch on my television a short film of a prestigious director for the new perfume Guerlain. Automatically, the advertisement directs my connected lights to stoop and take a deep blue color in order to create an immersive experience. If I look at the video to the end, I am offered to drop a sample in my mailbox within two hours or, if I am recognized as a loyal customer of the house, to go to the launch party to chat with a master perfumer.
Innovation

Artificial Intelligence

Serviciels ecosystems

consumers/brand

Real World

FREE WILL

DIGITAL

DATA PROTECTION

Human/machine

agreements

Technological platforms
What is data protection?

- Data protection is not about protecting data (contrary to Data security), it is about protecting Humans (data subjects).

- Data: Article 2 (a)… „any information relating to an identified or identifiable natural person ("data subject")”;

- Data Controller: Article 2 (d) … “"controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data..”
The protection of personal data in Europe

The protection of personal data is a fundamental right in the European Union. “Everyone has the right to the protection of personal data concerning him or her” – Charter of Fundamental Rights of the European Union

The personal information and data of individuals are processed in many aspects of everyday life –
What are personal data?

‘Personal data’ relate to any personal information which can be used to identify you, directly or indirectly, such as your name, your telephone number, your email address, your place and date of birth, etc.
Personal data collection

When?
- opening a bank account,
- signing up for membership of a gym,
- booking a flight,
- registering for loyalty cards in shops,
- Renting a car
Data protection law is based on the assumption that every processing of personal data is prohibited unless it is permitted.

- A permission can be granted by law, due to the informed consent of the data subject or based on an assessment and balancing of interests of data subjects.

- As a consequence, that implies that by default processing is forbidden and any data processing must be “justified” by the applicants.
What are your rights?

When your personal data are processed, you have enforceable rights, such as:

- be informed that your personal data is being processed in a clear and understandable language;
- have access to your own data;
- rectify any wrong or incomplete information;
- object to the processing on legitimate grounds;
- not to be subjected to an automated decision intended to evaluate certain personal aspects relating to you, such as your performance at work, creditworthiness, reliability, and conduct;
- receive compensation from the data controller for any damage you suffer, etc.
What are a data controller’s obligations?

A data controller = an entity (public or private sector) responsible for processing personal data. The obligations are:

- ensure that your rights are observed
- ensure that data are collected only for specified, explicit and legitimate purposes, that they are kept accurate and up to date and for no longer than is necessary;
- ensure that the criteria for making data-processing legitimate are observed, for example, when you give your consent, sign a contract, or have legal obligations;
- confidentiality of the processing;
- security of the processing;
- notification to the data protection authority, in some cases;
- ensure that, when a transfer of data occurs to countries outside the EU, these countries guarantee an adequate level of protection.
What can you do if your rights are violated?

• You can file an application with the Data Protection Authorities (DPAs) established in all Member States.
  • France: CNIL
• responsible for ensuring that your rights and obligations are respected.
• competent to hear your complaints and may prohibit the processing.
• You have at your disposal a judicial remedy for any breach of the rights and obligations guaranteed by the national law.
What can you do if your rights are violated?

https://www.cnil.fr/en/home
FACEBOOK proceeded to a massive compilation of personal data of Internet users in order to display targeted advertising. .../

FACEBOOK collected data on browsing activity of internet users on third-party websites, via the “datr” cookie, without their knowledge.../...
The concept of anonymity

- anonymous data
- With anonymous data you are not subject to data protection law and no requirements are necessary
- The terminology in the different countries/languages is highly confusing => wrong impression that data are anonymous if identifiers such as names and addresses are deleted.
- Data are often re-identifiable and ICT technologies such as big data amplify these risks
- Data are only anonymous if they cannot be re-identified with „reasonable efforts“
The European Legislation in Data Protection

Full harmonisation

  - harmonises national laws which require high-quality data management practices on the part of the "data controllers" and the guarantees of a series of rights for individuals.

  - guarantees the processing of personal data and the protection of privacy in the electronic communications sector.

- Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data of 18 December 2000
  - regulates the processing of individuals' personal data when the processing is taking place by Community institutions and bodies.

  - on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
core principles of CoE Convention 108, 1981

- Notice—data subjects should be given notice when their data is being collected;
- Purpose—data should only be used for the purpose stated and not for any other purposes;
- Consent—data should not be disclosed without the data subject’s consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—data subjects should be informed as to who is collecting their data;
- Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles
Michele Barbier, PhD
Scientific officer, Mediterranean Science Commission
Ethics Expert H2020, European Commission
Executive Director, Institut de Science et Ethique

Independent Ethics Advisor
Tel: +336 3307 9899
mbarbier@scinceethics.org