Essential notions on privacy and data protection

Clément Levallois

2017-11-01

Table of Contents

last modified: 2019-01-08

1. Privacy: just one aspect of data protection

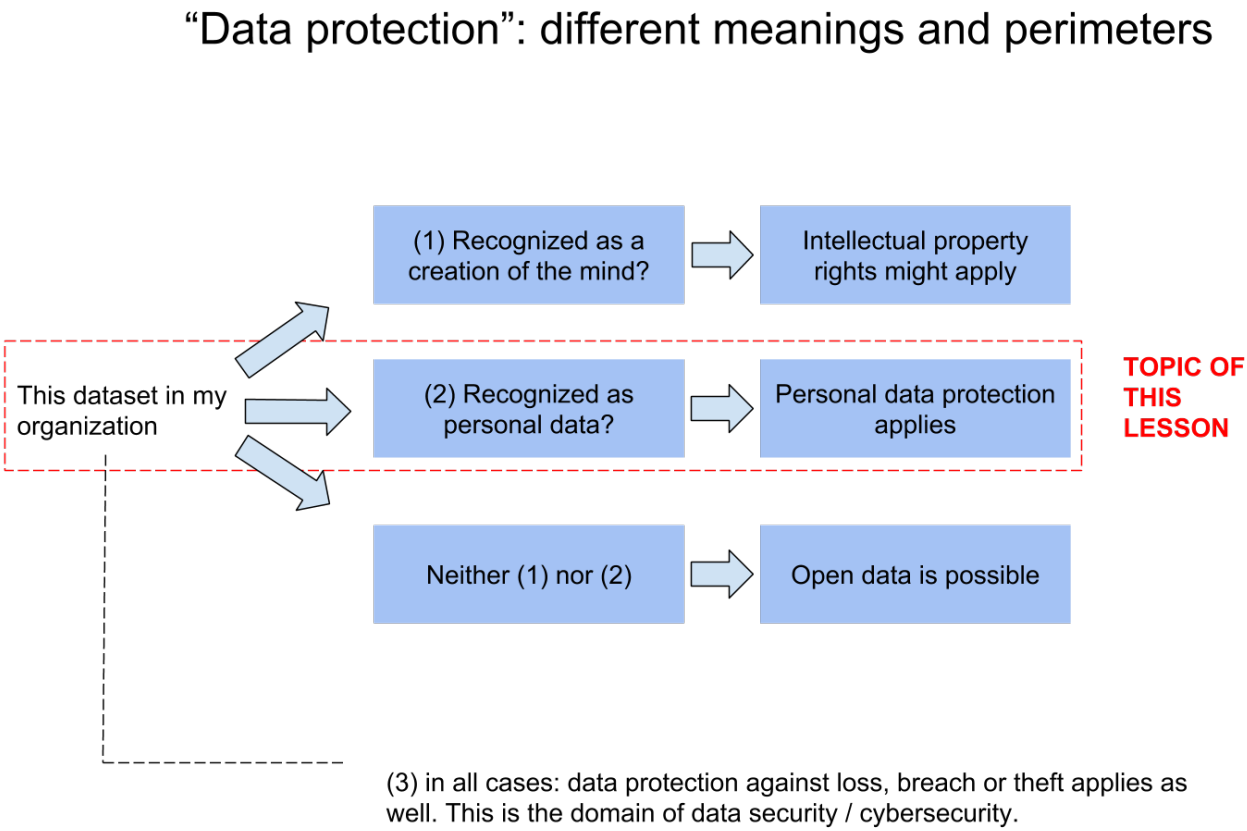

Figure 1. Defining data protection

2. When is personal information considered "data"?

At the most basic level, anything could count as "data" with possibly a personal character to it, including comments written about somebody in a personal notebook.

In practice, "data" starts to to be considered as such when it can be **processed automatically** or when it consists in **structured records** that can be used to facilitate the retrieval of specific information on specific individuals.

→ Hint: paper records, filing systems, databases

3. Personal data matters because of privacy

Definition of personal data:

> Personal data are any anonymous data that can be double checked to identify a specific individual (e.g. fingerprints, DNA, or information such as “the son of the doctor living at 11 Belleville St. in Montpellier does not perform well at school”).
>
> — CNIL (French Independent Administrative Authority)

Personal data is data that an individual has the right to keep private. **How and why is privacy an issue**?

Privacy is mentioned in the Article 12 of the 1948 Universal Declaration of Human Rights:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> — Universal Declaration of Human Rights

This article from the Declaration is found in similar forms in most of the conventions on human rights in the world.

This **right to privacy** enables individuals to define their identity in relation to the world, by giving each individual the power to control what to keep for themselves, and what to reveal / share with the world.

In 2005, a report on Privacy in the Digital Environment by the Haifa Center of Law & Technology develops:

> The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity.

> The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.

In addition to shaping an individual's own personal sphere and identity, privacy also underpins the development of a relation between the individual and the society she is part of:

→ when an individual's privacy is secured, they don't have to fear that their personal opinions and activities (as simple as reading a newspaper) will endanger them as citizens.

→ this gives liberty to individuals to develop political expressions which do not necessarily conform with the power structure in place. This would be much harder if everyone's political opinions could not be kept private.

4. Evolution of privacy

Privacy is a social norm which transforms as societies evolve. Since the 2000s, a couple of tendencies can be identified:

- increasing tracking of the digital traces left by individuals by companies which use these traces for ad targeting and data reselling.
- increasing state surveillance through digital means, against security threats and unspecified goals.
- broader public acceptance of new forms of violations to privacy.

For example, TV shows where participants are filmed 24/24 and where they reveal their (real or supposed) intimacy, dates back only from the late 1990s.

Figure 2. The Truman Show, 1998

5. Privacy of the consumer and privacy of citizens: the relations between the two

Thanks to whistleblowers like Edward Snowden, a former contractor for the National Security Agency - NSA, the extent of privacy breaches by governmental agencies is now better known.

This trailer for "CitizenFour" gives a sense of the dangers whistleblowers face when revealing how governmental agencies spy on their citizens:

▶ https://vimeo.com/108771171 *(Vimeo video)*

Journalists, academics, activists and NGOs such as the Electronic Frontier Foundation make the case that:

- consumers are insufficiently aware and sensitive of how much information is captured in the normal conduct of their lives, just by using mobile phones and apps, web browsing, and increasingly in public places.
- citizens are insufficiently aware and sensitive of the breach of their privacy by security agencies of their own country of residence, and by other countries.

Many citizens consider that if they don't break the law, then they have "nothing to hide".

Similarly, consumers might find that bargaining their private data against a free service and some targeted ads, is a good deal.

Sociologist of technology Zeynep Tufekci goes further:

Her argument is that besides "surveillance" and "lack of privacy", companies like Google and Facebook developing a business model based on ad targeting by analytics on personal data, design a **persuasion architecture** which can be used / highjacked for political purposes.

Tufekci does not argue that Google, Facebook or the likes inherently have anti-democratic purposes, but that:

- they develop of an information architecture which has the potential to shape opinions of crowds,
- they do so without transparency
- some past experiments on voting in the US, and current developments on electronic surveillance in China, show that the power of these technologies has already consequences in the real world:

▶ https://www.youtube.com/watch?v=iFTWM7HV2UI *(YouTube video)*

6. Conclusion: data protection in business, more than an regulatory obligation

The collection and treatment of personal data by businesses has far reaching implication, and should not be considered merely from a legal standpoint by firms.

The topic engages the Corporate social responsibility of the firm.

The nature of the **business model** itself - profiling consumers in the most specific way - has profound consequences on the design of the environment surrounding individuals.

What are the next steps? Several trends can be identified:

1. Some voices question the business model: are personalized ads based on personal data as effective as the market valuation of Facebook suggests? How much is just scam? Some voices warn against the extent of the fraud in digital ads, as the video below shows:

▶ https://www.youtube.com/watch?v=oVfHeWTKjag *(YouTube video)*

2. Legislation by political authorities to protect the public interest, especially via an obligation for transparency, in the face of more personal data being collected, for a larger variety of purposes.

3. A deepening of the current model with more personal data being collected, in private spaces (homes) and behavior in public places (crowd management in streets, stadiums, etc.):

Figure 3. Echo Alexa

Echo Alexa is a home assistant with a conversational interface, providing services personalized with the data provided by the user.

The end

Find references for this lesson, and other lessons, here.

This course is made by Clement Levallois.

Discover my other courses in data / tech for business: https://www.clementlevallois.net

Or get in touch via Twitter: @seinecle