Beyond anonymization: need for a cautious risk based accountability approach
Abstract

Gergely Acs, Claude Castelluccia, Daniel Le Métayer
Inria, France

In this paper, we will question the central role of notions of identifiability and deidentification in privacy regulations. It is now well established that deidentification is never perfect and generally comes into conflict with the objective of preserving the utility of the datasets. In addition, the fact that a piece of data is anonymous is by essence a relative notion because it depends on many factors, such as the available auxiliary knowledge, which may vary over time. Considering that data cannot be easily classified as personal or non-personal, or as sensitive or non-sensitive, we will argue that it is counterproductive to adopt a binary approach because it can lead both to inadequate protection of data subjects and inacceptable burden for industry. We will argue that the only way forward is to follow a more progressive, nuanced approach based on a rigorous analysis of the potential risks and benefits associated with the processing supplemented by strong legal, organizational and accountability measures.

However, further research work, reflections and debates need to be conducted to make this approach effective. Among the questions that need to be addressed, we would like to emphasize:

- The definition of the frontier between, on one hand the rights and obligations that should be respected regardless of the level of risk and, on the other hand, measures that could depend on the outcome of a privacy risk analysis.
- The notion of privacy harms and their severity, whose assessment form the ultimate objective of a privacy risk analysis.
- The trade off between potential privacy harms and the potential utility of the processing (especially for society), which should result from a collective deliberation.
- The implementation of the necessary accountability measures to address the residual risks and to create strong incentives for data recipients to respect privacy.

We will also discuss the evolution between the Directive and the GDPR to this respect. The GDPR represents a fundamental shift from an administrative process based on a priori controls to a risk based accountability approach. As such, it makes one step in the direction advocated here. However it also creates some ambiguities and leaves a lot of room for interpretation.