

IEEE Symposium on Privacy and Security 2018, San Francisco.

Short Talk application

**Processing Publicly disclosed personal data according to the GDPR  
- a hole in the privacy regulation framework –**

Abstract:

How many personal data do we publicly disclose (spread) daily? How we do it? And, above all, which kind of data? GDPR Article 9.2 e) regulates the process of data manifestly publicly disclosed as an exception to the general provisions about the processing of sensitive data. No other clues are given about the concepts of “public”, “manifestly” and “disclosed”, as well as disclosure by who. These gaps can drive to a wide applicative grey area that exposes data subjects to a broad range of “shadow”-processing. Indeed, questions may raise in crossing this provision with concepts such as pluri-subjective data, meta and semantic data. Thanks to a technical interpretation, we can find a temperament within the notion of legitimate interest and the general prohibition of direct marketing with public data, but these are weak principles, not easy to apply in practice without a specific norm. So, this talk will give a brief overview of the relevant conflicts and issues, and show the threats to new kinds of data, such as biometric data, in a IoT environment. Finally, it proposes some options to better protect public data and to help players processing them in a compliant, legitimate and ethical way.