Introduction to Privacy, 5G and Economics Minitrack

Samant Khajuria
Aalborg University, CMI
skh@cmi.aau.dk

Lene Sørensen
Aalborg University, CMI
ls@cmi.aau.dk

Knud Erik Skouby
Aalborg University
skouby@cmi.aau.dk

Abstract

The mini-track on Privacy, 5G and Economics focus on discussion of different aspects of security and privacy in the data rich environment including user right to privacy with regards to collection, retention, analysis and transfer of personal data. Differences between the regulation in the EU and the USA are debated in different examples. The mini-track also insists on the economic value of end users' data to innovatively redefine the relationships between end users' concerns on their personal data handling and the legal businesses on data analytics, in order to make that relationship ethically correct, compliant with regulation and also profitable for all.

1. Introduction

Privacy is a foundational issue of the digital world. This complex, multidisciplinary issue is commonly understood and valued differently by different individuals, data holders, courts and legislations. Privacy is a human-made concept that evolves with users and the environment they live in. One of the most used definitions from Westin [1] defines privacy, as "the right of the individual to decide what information about himself should be communicated to others and under what condition". This definition was further developed by Smith et al. [2] focusing specifically on perspectives in online privacy concerns – unauthorized secondary use of personal information, improper access of personal information and errors in collected personal information.

The growing quantity and quality of personal data is the driver for the global economy. This data today is generated everyday by people in a form of tens of billion text messages, posts and/or micro-posts. Castells refers to this phenomenon as "mass self-communication" [3]. With the rise in time spend online has inspired businesses, marketers and other interested parties like data brokers to become a part of the process, and to explore new business models.

Service providers have already for a long time been assigning value to the personal data for advertisement purposes. Only thing that is changes from the past is the quantity and quality of the data generated by user devices in a form of their location, searches, posts, emails, messages etc. Today service providers can build more accurate customer profiles, do better targeted advertising and sell the information to 3rd party providers without users' consent. Most economic value may come from reusing data for purposes other than the one data has been collected for. Users may or may not be aware of what is going on: today, it is not clear to what extent the current privacy preserving methods (such as the informed consent and other forms of permission) are effectively understood by users. Research by Futuresight [4] has shown that 50% of mobile users regularly provide consent without effectively reading agreements, due to excessive language complexity (but also because of lack of time). In addition to that, todays' user – service provider relationship model, when users wish to access a service from a service provider, it is often a matter of choice between either accepting all service terms and conditions or not using the service at all ie., "take it or leave it" approach. Users are asked to present a set of specific personal attributes to the service provider, often without seeing the relevance or justification of disclosing them.

This mismatch of information exchange and lack in the transparency related to the collection of users' personal data and its use, have made users reluctant to share information with their service providers. This results in lack of trust in the users with respect to activities around the services used. A survey conducted by Pew research clearly shows that 86% of the internet users have tried to use the internet in ways that would minimize the visibility of their digital footprints [5]. However, fifth generation (5G) technology is user centric and data centric [6]. It is very importation that the users of the technology to trust services provided by the network and share accurate information with the services. The new 5G technology is expected to serve not only the new function for people and society but

URI: http://hdl.handle.net/10125/50360
ISBN: 978-0-9981331-1-9
(CC BY-NC-ND 4.0)

also enable verticals like smart cities, V2X (vehicle to everything), smart grids, e-health etc.

"From the smallest personal items to the largest continents, everything, everywhere will be digitally connected, and responsive to our wants and likes" [7, p.17], comprises today's vision for the communication network of the future ie.,5G. This vision is strongly supported by recent market studies conducted by global organizations, telecom companies, and operators [ibid]. According to the 5G Infrastructure Public Private Partnership (5GPPP) [8], the 5G network will natively meet the requirements of three groups of use cases ie., Massive broadband (xMBB) that delivers gigabytes of bandwidth on demand, Massive machine-type communication (mMTC) that connects billions of sensors and machines and critical machine-type communication (uMTC) that allows immediate feedback with high reliability and enables for example remote control over robots and autonomous driving. To meet the requirements, technical goals are set to provide a system concept that supports; 1000 times higher mobile data volume per area, 10 times to 100 times higher typical user data rate, 10 times to 100 times higher number of connected devices, 10 times longer battery life for low power devices and 5 times reduced end-to-end (E2E) latency.

Based on the use cases and verticals in 5G defined by the organizations and industries, it seems like almost everything will become a service in the 5G environment. Traditional classification of online services and business models will not be applicable and flexibility and personalization attributes (PAT) will become predominant features and as a consequence of this the data expressing PAT will become increasingly valuable assets [9]. This raises concerns about user data privacy and security.

The digital world has introduced the need for a more definitive meaning of privacy especially information privacy. After two decades, the Data Protection Directive 95/46/EC (DPD) is finally phased out and replaced by General Data Protection Regulation (GDPR) [10]. A step towards the ongoing recognition of the value and importance of personal information. The regulation was formally adopted by 28 member states of the EU in 2016 and given two years for implementation. Even though the regulation is only applicable to the member states of the EU it will affect any organization in the world that provides services to any member state and/or is involved in processing EU citizen data. The main aim of the GDPR is to build or increase trust in EU citizens in using digital services [10]. The regulation was carefully designed in coherence with the EU Digital Market Strategy [11], where the ambition is to produce right incentives for the services to flourish by providing trustworthy infrastructure supported by the right regulation. GDPR is seen as a modernization of the protection of the processing of personal data to cover the legislative gaps created by the rise of social media, big data and increasingly digital world. The regulation extends the definition of personal data to any information relating to an individual, such as name, photo, an email address, bank details, postings on social networking websites, medical information or a computer's IP address [10]. Most of the legal practices in the new regulation are based on existing legislation. However, a number of new initiatives are also introduced ex., new rights for data subjects and new obligations for the data controllers and processors, partial harmonization of rules across the European countries, One-stop-shop where the main establishment of the company interacts with only one European supervisory authority [10]. Additionally, failing to comply with the Regulations, the new initiative introduces significant penalties including administrative fines – a fine up to 10 Million EUR or up to 2% of the annual worldwide turnover of the preceding financial year in the case of an enterprise, whichever is greater.

Following terms are used throughout the regulation and are applied with a very specific definition:

Personal Data: According to article 4 [10], "any information relating to an identified or identifiable natural person ('data subject')" – meaning that information is not personal data if there is no way to link it to a person. The regulation breaks down personal data into different categories. Some personal data are common data while others are sensitive and referred to as special categories of personal data. Ethnic origin, religious beliefs, political opinions etc. are considered as a special category of personal data. Organizations need to be very careful about how data is gathered and used, as by gathering sufficient amount of data and remove the anonymity about the user.

Controller: Article 4 defines controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data" [10]. The controller is usually a service provider to which the user provides their information. The controller decides which data will be collected from the user, from whom the data to be collected from and how the data can be stored. In addition to data, it is controller's duty to make sure that the 3rd party data

processors follow the regulation and ensure the protection of the rights of the user.

Processor: The entity is defined in article 4 as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" [10]. These entities are contracted by the controllers to process personal data information. An organization can be a controller as well as a processor.

Processing: According to article 4 "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;" [10]. The term itself is very broad, this essentially means, anything that is done to, or with, personal data.

The goal of this mini-track is to provide a platform for the academia, industry and government organizations to discuss ties and differences between the EU and USA from a privacy as well as an economic angle in future technologies (5G). his may include discussions on economic perspectives on the regulation in Europe and across the US and as well as on user' right to privacy with regards to collection, retention, analysis and transfer of personal data. The papers selected for the presentation for the mini-track fall under the following research areas [12]:

- **Security/privacy** – Design and implementation of novel Privacy Enhancing Tools (PET) to provide users with the functionality they require without exposing any more information than necessary, and without losing control over their data, to any third parties. In order to realize that, security mechanisms like attribute based encryption, and authentication mechanisms are also part of the research.
- **Usable Privacy /Interaction Design** – The research area of Usable Privacy develops methods and techniques to analyzing and visualizing privacy policies for creating user interfaces and awareness around privacy for users as well as options for managing privacy. The Usable Privacy research areas is founded in Interaction Design principles and insights in user behavior, interface design etc.
- **Economics/ privacy** – Realizing user centric and data centric 5G technologies based on user trust in data privacy further requires viable business models. Today personal data has become an economic asset belonging to the service providers whose business case often includes and is dependent on the use and selling of such data to third parties. This type of business case is increasingly disputed both from a privacy and from an economic ownership perspective.

Following topics will be presented:

- In *Putting a Price Tag on Personal Information - A Literature Review*, Amina Wagner et al. [13] provide an overview of the literature on the value people assign to their personal information and how to deal with possible direct compensation or protection.
- Jari Porras et al provide in *Security In The Internet Of Things – A Systematic Mapping Study* a survey of current research trends in security concerns of the IoT concept and understanding of the topic [14]. The mapping study identifies nine main concerns and 11 solutions. The findings also reveal challenges, such as secure privacy management and cloud integration that still require efficient solutions.
- Xiaobai Li and Jialun Qin discuss in *Protecting Privacy When Releasing Search Results from Medical Document Data* the privacy-preserving extraction, summary, and release of information from these documents in a US setting [15]. A novel approach to enable privacy-preserving extract, summarize, query and report patients' demographic, health and medical information from medical documents is proposed.
- Garlach and Suthers introduce in *'I'm supposed to see that?' AdChoices Usability in the Mobile Environment* the issue of alerting consumers to the presence of behaviorally-targeted advertising on the mobile web [16]. AdChoices, an app from the Digital Advertising Alliance (DAA) is presented as the primary tool for this. The paper presents findings from the first empirical usability test of AdChoices.

12. References

[1] Westin, A.F. "Privacy and Freedom", Ateneum, 1967

[2] Smith H.J., Milberg, S.J., and Burke, S.J. "Information Privacy. Measuring individuals' concerns about organizational practices". MIS Quarterly, 1996, Vol. 20, no.2, pp. 167-196

[3] Castells, M., "Communication Power", 2013, Oxford University Press

[4] Futuresight, “User Perspectives on Mobile Privacy, Summary of Research, www.gsma.com/.../futuresightuser perspectivesonuserprivacy.pdf

[5] PewResearch, “Digital Footprints”, www.pewinternet.org/2007/12/16/digital-footprints

[6] Monserrat, J.F., Alepuz, I, Cabrejas, J., Osa, V., López, J., Roberto, G., Domenech, M.J., and Soler, V. “Towards User-Centric Operation in 5G Networks”, EURASIP Journal on Wireless Communications and Networking, December, 2016, 2016:6.

[7] Prasad, R. and Dixit, S., “Wireless World in 2050 and Beyond – A Window to the Future, 2016, Springer Series in Wireless Technology.

[8] 5G-PPP EU, “5G Vision”, https://5g-ppp.eu/wp-content/.../02/5G-Vision-Brochure-v1.pdf

[9] 5G-PPP EU, “Automotive Vision” https://5g-ppp.eu/.../5G-PPP-White-Paper-on-Automotive-Vertical...

[10] European Commission, “The General Data Protection Regulation”, 2016, ec.europa.eu/justice/data-protection/reform/.../regulation_oj_en.pd..

[11] European Commission, “Digital Single Market”, 2015,. https://ec.europa.eu/digital...market/.../shaping-digital-single-mark.

[12] HICSS Call for Papers, http://hicss.hawaii.edu

[13] Wagner, A. Wessels, N. Buxmann, P. Krasnova, H. , “Putting a Price Tag on Personal Information - A Literature Review”, 2018, Presented at the HICSS Conference, “The Privacy, 5G and Economics” mini-track, January 3-6, 2018.

[14] Porras, J. Pänkäläinen, J. Knutas, A. Khakurel, J. , “*Security In The Internet Of Things – A Systematic Mapping Study,* ”, 2018, Presented at the HICSS Conference, “The Privacy, 5G and Economics” mini-track, January 3-6, 2018.

[15] Li, X. and Qin, J., “*Protecting Privacy When Releasing Search Results from Medical Document Data*”, 2018, Presented at the HICSS Conference, “The Privacy, 5G and Economics” mini-track, January 3-6, 2018.

[16] Garlach, S. and Suthers, D. “*‘I’m supposed to see that?’ AdChoices Usability in the Mobile Environment*”, 2018, Presented at the HICSS Conference, “The Privacy, 5G and Economics” mini-track, January 3-6, 2018.