Title:

# Privacy in the 5G World: The GDPR in a Datafied Society

Sebastiao Teatini

Marja Matinmikko-Blue

University of Oulu - FINLAND

July 2019

## 1. Introduction

We may be embarking upon a societal journey that will lead us toward a techno-surveillance dystopian future and the technological revolution that will allow for this scenario to come to fruition is 5G, or 5th Generation Wireless Technology. As we march towards a globalized world where digital data fuels the economy, cities will become hyper-connected and the necessity for data collection will proliferate. As a consequence, regulators around the world will be confronted with the reality that privacy may be on its death bed and 5G will deliver the final blow. With the increase of data transfer speed and reliability comes the risk of privacy deterioration as 5G interlaces with ubiquitous computing creating a socio-technical all-encompassing global web of personal digital data extraction, storage and transfer that will directly impact the way society organizes itself.

The focus of this article is on identifying and understanding the possible threats to privacy protection that may be encountered in the deployment of 5G. The datafication of society is likely to increase in the upcoming 5G world and legal safeguards are necessary to ensure our privacy rights are protected. The purpose of this chapter is to analyze some of the unique characteristics of 5G and how the EU General Data Privacy Regulation (GDPR) stands as the last legal guardian against unwanted personal data violations.

Sweeping aside the hyperbole, it can be stated with some degree of confidence that we are in the midst of a technological revolution in the field of wireless communication that will transform the way society organizes itself. The coming hyper fast wireless communication infrastructure, 5G, will enable future business ecosystems to flourish in the fields of augmented reality, virtual reality and artificial intelligence, autonomous driving, health care, among others (Habib, 2019; Frias, 2018). Due to its low latency, reliability, high capacity, energy efficiency and speedy data transmissions, 5G will directly impact the way we interact, communicate, work and participate in society (Jacobson, 2019; Lemstra, 2018). For this breakthrough to take place a new generation of communication infrastructure is being designed, created and implemented in many urban areas in Europe, North East Asia, North America and other regions of the world. In addition, more intangible elements, such as software, protocols and standards are being put in place that combined with form the 5G technical ecosystem. Not only the volume, velocity and variety of digital data will increase in the 5G world, but

also the value. However, in the fast approaching datafied world, privacy is rapidly becoming a cherished commodity rather than an inherited human right (Cave, 2018).

The main concern for regulators and developers of this infrastructure is how to better protect individual data privacy in the coming ubiquitous computing connected world (Liyanage et al., 2018). With increased connectivity comes increased fear that our personal data may fall in the hands of unscrupulous or uninvited actors, such as hackers, unwanted advertisers or overzealous security agencies. Complete data security is impossible and the protection of personal data remains especially challenging in a world where our personal data is being extracted, organized, classified, manipulated and commercialized (Zuboff, 2019). Over the past decade we have observed an overflow of digital devices and sensors in our cities, work, homes and increasingly in our bodies. Our entire surrounding functions in a constant data production mode. The thirst for the optimization of data extraction, analysis and manipulation is justified by the logic of surveillance capitalism, where all personal digital data that can be monetized will be (Silverman, 2017).

Today, more than half of the world population is connected to the internet, producing searches, posting videos, playing games, paying bills, sending messages, making calls, and the number of users who consume and produce digital data is likely to increase. The scope, speed and depth of data collection will dramatically accelerate as 5G will allow for billions of sensors (Internet of Things, IoTs) to be connected to the Internet. From our home appliances to automobiles, factories, machines, clothes, power grids and smart cities, ‘everything’ will be connected to Internet and constantly producing digital data (Cave, 2018).

The structure of this chapter is as follows: in the first part we discuss what distinguishes 5G from its predecessors and some regulatory challenges for the coming technology. In the next section we analyze in detail the appropriateness of the current data privacy legal infrastructure (GDPR) in Europe and how some individual nation states may be coping with its implementation. We then identify some potential obstacles to ensuring data privacy in the 5G world. A synthesis of our analysis will be presented in the conclusion.

## 2. The 5G World. What sets it apart from previous communication technologies?

Most mobile data users are not yet familiar with 5G because the technology will not be commercially available on a large scale until 2020. According to the EU 5G Action Plan, which delineated the strategies and goals for the building and deployment of the 5G infrastructure in member states, a roadmap was established to facilitate the implementation of 5G by via spectrum allocation by national governments and to facilitate the coordination between industry and the public sector via the EU Public-Private Partnership (5G-PPP). Until 5G is available to consumers, for the most part, users will rely on 4G (LTE) and its evolutions, or even 3G, to access the internet, send messages and place phone calls from their gadgets. So what distinguishes 5G from its predecessors?

5G is expected to change the traditional mobile communication business ecosystem by connecting billions of devices and ultimately digitizing the entire society which can have a big impact on productivity and competitiveness. Policy makers have globally recognized the importance of widespread deployment and timely take-up of very high capacity networks for realizing the full economic and social benefits of the digital transformation. The development of 5G networks will be based on dense deployments of small cell networks in specific high demand locations.

Traditionally, a small number of Mobile Network Operators (MNO) has dominated the mobile connectivity market with high infrastructure investments and long-term spectrum licenses granted by the national regulators (Al-Debei et al., 2013). The mobile communication sector has recently gone through a transition where the MNO market dominance has been shaken with the appearance of over the top (OTT) services that have substituted MNOs' voice and text services (Weber & Scuka, 2016). These internet services can operate independently of the infrastructure, leaving the MNOs to act as bit pipes providing mobile broadband connectivity to deliver the services. Regulations on the other hand have not evolved along with the complex technical and market developments resulting in different regulatory requirements for the mobile connectivity domain and the internet domain. National regulators are currently in the process of adapting their regulatory mechanisms for the adoption of next generation networks and

implementing the European Electronic Communications Code (EECC 2018; Briglauer et al. 2017).

5G networks aim at providing new high-quality wireless services to meet stringent and case-specific needs of various vertical sectors beyond traditional mobile broadband offerings. 5G networks are expected disrupt the traditional mobile communication market by lowering the entry barrier to new entrants by sharing of required resources (Agiwal et al., 2016; Samdanis et al., 2016). This development has the potential to open the mobile market for a large number of local 5G networks (Matinmikko et al. 2018).

A key regulation aspect shaping the 5G market is spectrum. Globally, new spectrum is made available for the deployment of 5G networks through World Radiocommunication Conferences (WRCs) and existing bands for cellular networks are being transformed to allow the deployment of 5G networks. New 5G spectrum awards by the national regulators are showing a divergence in the approaches taken in different countries either strengthening the existing MNO market dominance or allowing new entry for different stakeholders to locally deployed 5G networks (Matinmikko-Blue et al. 2019).

## 3. Data Privacy and the GDPR

In the coming 5G world, privacy concerns are likely to increase as the speed and quantity of personal data being transmitted over the network will increase significantly (Lemstra, 2018; Cave 2018). The legal system, specifically the laws and regulation related to privacy rights and privacy protection, is the most effective safeguard individuals have to protect them from unscrupulous actors that may attempt to extract, manipulate, commercialize, classify or misuse personal data without the users' explicit consent.

Just as authorities were slow to react to the growth of the internet in the 1990s and social media in 2010s, 5G will again pose a challenge to regulators trying to get a grasp of the direction this technology will take society from its inception (Wu, 2011). Data is the fuel of the digital economy. Data privacy laws address the way in which data is collected, stored, classified and disseminated (Bygrave, 2014). In Europe, the current law that covers personal data protection was

approved by Parliament in April 2016 and after a 2 year grace period, to allow national governments and regulators to get ready, was finally put into practice on May 25 2018. The General Data Protection Regulation (GDPR) was enacted in order to enable EU citizens and institutions to get better control of their personal data.

This legislation, which attempts to address the increasing concerns of EU residents about the use of the data, may also have some adverse effects. Due to its broad reach, many business operators are struggling to adjust to the new legal playing field (Reuters, 2018). One of the focus of the law is to ensure transparency and accountability in order to minimize risks of individuals' data from being misused. Organizations, whether European or from abroad, operating in the EU are now required to abide by this legislation and this presents a challenge as some global institutions, such as NGOs and multinational corporations, will have to comply with several regulatory bodies (Bygrave).

There are some important cultural differences that impact the way privacy laws are interpreted in the US and Europe. In the US, privacy protection concerns are mostly addressed by directives, whereas in Europe, the strong concern for personal self-determination and privacy calls are addressed by laws and regulations (Table 1). As we demonstrate in the next section, even inside the EU national governments have chosen different approaches in adopting the GDPR as regulators have intentionally left room for member states to interpret the law.

The 5G roll-out is likely to impact privacy in many realms. In real-time interactions, anything that can be connected to the Internet will be. From transportation, power grid management, home appliances and even wearables (Jacobson, 2019) the coming digital hyper connected ecosystem implies that everything that can be connected, will be. Thanks in great part to 5G, in the next 5 years there will be hundreds of billions of sensors connected and an enormous amount of digital data will be produced. In 2016 alone, there was as much digital data produced as the entire history of the universe going back to the big bang (table 2).

The datafication of society is operating at full throttle. Every day, 5 billion searches are made, 65 billion messages are sent on WhatsApp, 4 terabytes of data are created from connected automobiles, 294 billion emails are sent and 4 petabytes of data are produced on Facebook. It is estimated that by 2025 463 exabytes of digital data will be created daily around the hyper connected world,

and the 5G infrastructure will be an integral part of the coming digital society (VisualCapitalist 2018).

The GDPR is becoming the global standard for how privacy and privacy protection laws should be molded. In essence, it sets the rules by which companies treat our personal data. Legislators who wrote this legislation cherished the idea of consent, which means companies often have to ask users for permission to use their data. The law also stipulates that third party data sharing will be more restricted since they will have to offer a reasonable explanation for why and how long they need the data and EU residents now have the right to request their personal data from companies.

When it comes to the protection of data of EU residents, the law (GDPR) guarantee that not only organizations established in the EU, but also abroad, such as Amazon, Facebook and Weibo, are required to comply with the terms of the law. The scope of the law is broad to the extent that it covers not only digital data but also paper or other form, so long as the type of data can be used, directly or indirectly, to identify an individual.

Within the jurisdiction of the law an enterprise (private of public), an organization or individuals can collect private data for these purposes

- To execute a contract, such as a purchase of service or an employment agreement.
- To fulfill a legal obligation, as in the case of the place of employment providing personal data to welfare agencies.
- To protect vital interests, for example, to collect personal information to protect one's life.
- To perform bureaucratic duties, such as schools and hospitals.
- To carry out legitimate interests, as in the case of a bank using personal data of clients to benefit them, such as offering lower rates.

Any other form of personal data extraction and use without the consent of the individual is strictly forbidden. When an institution requires the consent of citizens to access their personal data, this consent has to be explicitly given. According to the law, for example, it would not be enough to simply click on an icon to indicate interest to be excluded from receiving emails. A clear and explicit agreement has to be made in order to authorize the other party to access and use the data. Before the decision is made, individuals have the right to receive

detailed information of who is requesting the data and for what purpose. Individuals also have the right to know how long the information will be used and stored and if the data will be shared with third parties. The law also states that this information should be clear and easy to understand.

In the case when a specific consent has been given to an organization to access the person's data, an individual can at any moment contact the institution and revoke the consent, at which point the organization will no longer be legally allowed to extract or use this data for any purpose. In a few rare specific cases, such as in a critical scientific study, or if the data extraction and manipulation is performed by public officials for the purpose of national security, the public interest may prevail over individual rights.

It has taken the European Commission almost 5 years to get the law in the books. There have been a few cases that served to illustrate the importance of having a law that would address the pertinent issue of data protection. The case of Google and Facebook in privacy by design (Rubinstein, 2012) fell under the EU laws that were written and adopted more than 20 years ago, when both companies didn't even exist and the technologies that today power the Internet were in its infancy and most people didn't use online banking, reserved trips online, or talked to their friends on the Internet.

In the current law the idea of Fair Information Practice was to be incorporated in the design and build-in of software, hardware and services, in order to guarantee that privacy would be addressed from the inception of new technological systems. The most efficient way to ensure the implementation of this legal specification was to establish specific and concrete measurable. In addition to the development of software interfaces that complied with privacy regulation. In his research, Rubinstein found that the main obstacle to implementing Privacy by Design was not the technical barriers or cumbersome regulatory infrastructure, but the competing interests between business and individuals. He concluded that "business interests overshadow privacy concerns".

The current GDPR is exactly what it states, a regulation and not a directive. There are some significant differences between them. The directive is a piece of legislation that has been brought out by the EU but it needs to be implemented into member states legislation before it effectively becomes law. A regulation is also approved on the EU level but automatically becomes law without the necessary national ratification process. The law however was written in a way

that intentionally leaves some room for national interpretation on specific items, either due to cultural awareness or legal practice. With this in mind, it is important to remember that the GDPR is legally binding and should be observed and respected by all member states.

The type data that concerns the law is personal data, otherwise it falls outside the scope of the law. What would be the legal interpretation of what is personal and what is not? This law has attempted to settle this debate by offering its own understanding of the concept. Personal data, under the new regulation, can be considered to be personal any information that may identify individuals, such as audio, address, video, texts, but also online identifies, such as IP addresses.

The new EU law also introduces and discusses the idea of pseudonymous data, which is data in which attempts have been made to identify the subject. Profiling is also covered under the law. So if genuine efforts have been made to pseudonymize personal data, the law looks favorably at these efforts in court cases. Effectively, GDPR will apply to all types of data collected, whether it is directly identifiable or quantitative and technical data from or about any EU resident.

One of the new aspects of GDPR is the scope and reach of this law that extends to other countries and territories under the concept of extra-territoriality. For that matter, institutions, whether private or public, with or without a presence in the EU, will fall under this legislation, so long as these organization offer goods or services to EU residents or monitor the behavior of EU residents.

The GDPR legislation supersedes all nation states privacy laws. However, EU regulators were conscious about the necessity for nation states to interpret some part of the law in accordance with national culture and practice so for that purpose EU countries have adopted their own strategy in implementing GDPR at home.

Table 1. Summary of Data Protection Regulation in Europe

| **Data Protection Regulation in Europe** |
| --- |

| | |
|---|---|
| **Finland** | New privacy regulation approved by the Finnish government in 2018 goes a step further than the GDPR protecting. The new legislation also increases the power of regulators to administer steep fines on individuals and institutions that breach the law. Based on the new law, children's date and age of consent states that public and private institutions, including individuals, will no longer be able to retrieve data of minors younger than 13 years old. |
| **Germany** | Germany has historically had some of the most comprehensive data protection laws in Europe. The German Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted in 1970. In the following decade Constitutional Court drew a distinction between the right to information self-determination from the right to respect for personality. In 2001 the parliament amended the Federal Data Protection Act by creating a provision which incorporated the recommendations of EU Directive 94/46/EC Since 2009 Germany has had some of the strictest data protection laws in Europe. However, as the GDPR supersedes national law, German regulators are required to apply GDPR standards when necessary. |
| **France** | The French Data Protection Bill was introduced by the Ministry of Justice in December of 2017. The new proposed legislation revises the previous 1978 French Date Protection Act. The new bill attempts to balance the increased need for access to personal data with the necessity to protect the privacy of some critical data, such as medical records, criminal records, data of under-age citizens, genetic data, etc In 2017 France passed a data protection law which called for the lowering of the age of consent from 16 to 15 years old. In addition, in 2018 France adopted a law that imposes hefty fines, up to 125,000 euros, on operators that fail to provide adequate data protection to users. |
| **Italy** | Rather than passing new a legislation, a decree was signed in 2018 that requires data operators to comply with the GDPR by introducing new code of conducts and guidelines. The decree maintained GARANTE as the national data protection agency in charge of guaranteeing compliance with the new EU legislation. The decree also stipulates that the age of consent was reduced to 14 years old and data controllers are required to design simple, clear, concise and objective consent forms for children. |
| **Spain** | The privacy and data protection law was enacted in December of 2018. The Protection of Personal Data and the Guarantee of Digital Rights targets five specific issues: political parties and personal data processing, digital rights at work, object of the law, data subject rights and data protection officers. The Spanish legislation goes a step beyond the EU law by offering increased personal data protection. The expansion of data rights is stipulated in the law by addressing the right of parents to access, modify, suppress and oppose on behalf of their children. |

| | |
|---|---|
| **Portugal** | In June of 2018 Portugal passed the Execution Law of the General Data Protection Regulation. A regulation approved by the Portuguese Data Protection National Commission lists the types of activities to be covered by the Data Protection Impact Assessment (DPIA). The purpose is to mitigate the threats posed by unnecessary exposing of personal data during the implementation of projects, systems, protocols, strategies and policies. The types of data included are: health data electronic devices, large scale profiling data, locators and trackers of individual subjects by organizations, biometric data for identification and genetic data. |
| **The Netherlands** | In the case of the Netherlands, the GDPR replaced the Dutch Data Protection Act. The Dutch Data Protection Authority (DPA) proactively instituted rules and compliance obligations to GDPR ahead of its EU counterparts. The new rules determine that failure to comply may result in the incurrence of fines up to 1 million euros, depending on the type and severity of the infraction. Dutch authorities also streamlined the process for individuals or companies to report data breach or misuse of data by contacting the DPA website and reporting the violation. |
| **Poland** | The Polish Data Protection Act (PDPA) was passed in order to facilitate the implementation of the EU's GDPR. However, the PDPA lacks enforcement mechanisms as authorities are not allowed to institute fines when an infraction has been detected. In addition, Poland is in the process of adjusting other laws, such as telecommunications, commerce and copyright in order to comply with GDPR. This work falls under the jurisdiction of the Ministry of Digitization. One of the concerns brought forth is the low fines instituted for public agencies, which is capped at 25,000 euros. |
| **Denmark** | In 2000 the Danish government enacted the Danish Act on Process of Personal Information in which it stated that personal data should be collected only for specific, legal and explicit reasons. It also stated that it should be accurate and not be excessive. The Danish Data Protection Act was passed in 2018 and it adopts and amends the GDPR by including in the regulation sections that were specifically designed to be interpreted by nation states. |

## 4.The risks and threats to privacy in 5G

There is still a significant amount of confusion about personal data protection in 5G. Are enhanced security features available in 5G going to assure the protection of my data? Engineers recognize that there are no infallible or invulnerable networks and the maintenance, improvements and protection of the technical infrastructure is an ongoing process. One of the main features of 5G is the ability users will have to download and upload vast quantities of data at hyper speeds with very low latency. However, the underlying internet infrastructure will remain the same. The same mechanisms that data companies, hackers and intelligence agencies exploit today to access our personal data will continue to exist. In addition, there will be a slow transition from 3G, 4G, or 4.5G to the new 5G protocols and engineers designed the infrastructure with the purpose to accommodate the previous protocols (Cave, 2018, Jacobson, 2019). Vulnerabilities and risks to the networks will continue to exist and will likely be exploited as nations transition to 5G. Due to structure of millimeter waves, one of the requirements of 5G is that antennas must be located much closer to one another which will allow for a precise geographic location of individuals and devices. This could pose a significant risk to privacy and security of users, especially those who are more vulnerable.

As 5G and IoTs interlace, billions of devices will be producing and transmitting data without any interference from users. From automated cars, to cellphones, to wearables, many personal devices are now being designed by default to be constantly connected to the internet. As ubiquitous computing becomes the norm, some of these personal devices will have different levels of security and any design flaw, such as hardcoded and embedded credentials or unpatched vulnerabilities can be exploited (Miller, 2019).

Researchers from the University of Oulu in Finland have identified several privacy issues related to 5G (Liyanage et al, 2018). Based on their analysis, we shed light and discuss some of the more significant matters that could represent a threat to privacy in 5G. Moreover, we discuss the threat presented by overzealous security agencies which pose a danger to civil liberty and privacy by operating on the outskirts of the legal system in order to extricate intelligence from digital data.

*Data Confidentiality:* It is related to the protection of data and its access without authorization. For confidentiality to be absolute only those who were granted access should be able to reach the data. In 5G, many organizations in vertical industries will be involved in the process and manipulation of user's data and it is

critical that privacy agreements are established between all parties involved, including network operators.

*Data Ownership:* In 5G and cloud computing, the idea of who owns the data is as important as where is the data. The EU data economy is on its infancy but it is vital that legal parameters are established to determine who owns the digital data. Clearly defined legal arrangements should be undertaken between operators and users.

*Shared Environment and Trust:* Not unlike other networks, the 5G infrastructure will be shared between several operators and users. In some cases, even competitors will be sharing network resources. In this scenario where multiple actors with different intents and purpose operate, unauthorized exploitation and breach of personal data, such as Distributed Denial of Service (DDoS) may occur. In this scenario, where several actors operate with distinctive goals, there is a risk that the level of engagement in network security and data privacy will be uneven or cumbersome.

*Loss of Visibility:* Communication Service Providers (CSPs) determine the level of security to their systems but may be reluctant to share the security strategy and measures with the mobile operator. As a consequence, privacy concerns may falter as operators lose full visibility to the network.

*The Globalization of Data Flow:* As we live in a globalized digital world, many networks and computer systems are interconnected around the planet. In 5G, data will move between countries at a hyper speed and the necessity to protect this data will be imperative. Operators and regulators have to clearly define what constitutes private data, how it will be transferred, stored and organized. What may a controversial privacy concern in a country, such as sexual orientation or political affiliation, may be a completely normal issue in another. This is a challenge the GDPR has attempted to address but its efforts may fall short as some nations have distinctive legislation that does not address privacy concerns in similar ways as GDPR.

*Hacking:* It usually occurs when an unauthorized intrusion to a computer or network takes place. 5G will be susceptible to hacking as cloud computing, IP and web-based attacks will exploit the vulnerabilities of the technology. Technical networks are never completely bullet-proof to prevent attacks and hackers will use their software and hardware expertise to extract data for nefarious purpose

that could compromise individuals' privacy. Hacking may be carried out by individuals, criminal organizations or government agencies under the banner of national security.

*Security Agencies:* Although this could be included in hacking, we decided to distinguish this threat from the others presented by the researchers based on its geopolitical significance. Over the past few years, some former security agencts turned whistleblowers, such as former NSA contractor Edward Snowden and William Binney, have shed light into the unscrupulous and overzealous methods utilized by the NSA, CIA and other intelligence agencies around the world on how and to what extent they are willing to bend the law in order to achieve their goals. US government programs such as PRISM, where private enterprises, among others Microsoft, Facebook, Google, Apple and Yahoo, as well as national governments, such as Israel, New Zealand, Australia, UK, Canada and others cooperated with the US intelligence community to collect data of individuals without their consent (Connor, 2019). At the moment the politics of 5G is on overdrive as the US and China attempt to position their technological advancements as a catalyst to global hegemonic power (Watts, 2019).

## 5. Concluding thoughts

EU Government officials and technology developers are eagerly promoting the benefits of the 5G with negligible regards for the public's concern about privacy. However, 5G is not a panacea, and it comes with a price tag society may not be fully informed about or ready to accept. Issues related to the continued and accelerated corrosion of privacy are likely to become 5G's biggest challenges to a successful implementation and deployment. The General Data Privacy Regulation (GDPR) in Europe is the current safeguard most EU consumers have to ensure their personal data is not being unintentionally used by uninvited parties. As it is often the case, laws tend to address recognizable issues. In the case of 5G and the unknown vertical industries it may foster, the GDPR will likely be inadequate to address yet undetected potential threats to privacy that will arise in the near future as we move steam ahead into a surveillance society driven by the logic of monetization of personal data (Zuboff, Silverman).

The coming 5G infrastructure will connect billions of data producing devices and sensors worldwide and this datafication of society may significantly alter the way we live. In addition to lighting speeds to communication technologies, countries are investing heavily on the deployment of 5G and the deployment of the infrastructure. The US, China, the EU, Japan, South Korea and others are engaged in a fierce global competition to be the first to take full advantage of this technology. In order to accomplish these lofty goals, countries must ensure the development and maintenance of this technology will not present significant threats to the public and society in general.

5G will be more than just a disruptive technology (Cave, 2018, Jacobson, 2019). 5G networks will facilitate the development of advanced robotics, Artificial Intelligence, Big Data, IoTs, and the possibilities for new verticals in the sectors of automobile, energy, industry and health care demonstrate the reach and significance 5G will have for society. Consequently, the amount of digital data produced will dramatically increase in the near future.

China is pressing ahead in development of this technology and the US and others are concerned with the speed, structure and pace of China's recent technological advancements. The issue of 5G technology plays into the scenario of global geopolitics and countries national security interests. One way where this has transpired in the global scene has been in the US and its allies pursue of banning Chinese products (Villas Boas, 2019).

The argument presented in this chapter is that the coming 5G technology and the infrastructure required for its deployment and operation, should be considered as an integral and indispensable part of a functioning society and as such, measures to protect its integrity and its users' privacy must be a priority not only for national governments, but also the private sector and civil society.

Table 2

**Daily Digital Data Production in 2020 (Estimation)**

- 500 million tweets
- 294 billion emails
- 4 billion email users around the globe
- 350 million photos
- 100 million hours of video
- 95 million photos and videos shared on Instagram
- 28 Petabyte of data extracted from wearables
- 5 billion searches
- 200 billion connected devices (IoTs)

## References:


**Ahmad, I, Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A. (2017)**. 5G security: Analysis of Threats and Solutions. *IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, 2017, pp. 193-199.

**Bräutigam, T., Miettinen, S. (Eds). (2016**). Data Protection, Privacy and European Regulation in the Digital Age. Faculty of Law University of Helsinki.

**Bygrave, L. (2014).** Data Privacy Laws: An International Perspective. Oxford University Press, UK.

**Cave, M. (2018).** How Disruptive is 5G?. *Telecommunications Policy*. 42. 653-658.

**Connor, B.T. (2019).** Government and Corporate Surveillance: Moral Discourse on Privacy in the Civil Sphere. Information, Communications & Society. Retrieved in July from https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1629693

**Council of Europe. (2008).** On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union*. Dec. 23. Council Directive 2008/114/EC, December 8. Retrieved on 25 June 2019 from https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

**Desjardins, J. (2019).** How Much Data is Generated Each Day. *Visual Capitalist*. Retrieved on July 2019 from https://www.visualcapitalist.com/how-much-data-is-generated-each-day/

**European Commission. (2019)**. Security of 5G Networks. Commission Recommendation, Strasbourg 26.3.2019. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks.

**Frias, Z., Martinez J.P. (2018).** 5G Networks: Will Technology and Policy Collide?. *Telecommunications Policy*. 42. 612-621.

**Habib, M.A., Ahmad, A., Jabbar, S., Khalid, S., Chaudhry, J., Saleem, K., … Khalil, M.S. (2019)**. Security and Privacy Based Access Control Model for Internet of Connected Vehicles. *Future Generation Computer Systems.* Volume 97. 687-696.

**Jacobson, A. (2019).** The 5G Future will be Powered by AI. *Network Computing*. Retrieved on 26 June 2019 from https://www.networkcomputing.com/wireless-infrastructure/5g-future-will-be-powered-ai

**Lemstra, W. (2018).** Leadership with 5G in Europe: Two Contrasting Images of the Future, with Policy and Regulatory Implications. *Telecommunications Policy*. 42. 587-611.

**Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., Ylianttila, M. (2018)**. 5G Privacy: Scenarios and Solutions. 10.1109/5GWF.2018.8516981.

**Klitou, D. (2014).** Privacy-invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st century. T.M.C. Asser Press, The Hague.

**Marr, B. (2018).** How Much Data Do We Create Everyday? The Mind-blowing Stats Everyone Should Read. *Forbes*. May 18. Retrieved on July 17 2019 from https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#4e5483d360ba

**Miller, M. (2019).** Hardcoded and Embedded Credentials are an IT Security Hazard. *Beyond Trust*. February 26. Retrieved on 19 July 2019 from https://www.beyondtrust.com/blog/entry/hardcoded-and-embedded-credentials-are-an-it-security-hazard-heres-what-you-need-to-know

**Reuters. (2018).** Top 5 Concerns with DGPR Compliance. Retrieved on June 28 2019 from https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

**Rubinstein, I.W., Good, N. (2012).** Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *New York University Public and Legal Theory Working Paper* 347.

**Sgora, A. (2018)**. 5G Spectrum and Regulatory Policy in Europe: An Overview. *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, Thessaloniki, Greece, 2018, pp. 1-5.

**Silverman, J. (2017).** Privacy under Surveillance Capitalism. *Social Research*. 84(1). 147-164.

**Smith, O. A. (2018)**. Finland's beefed-up Data Protection Act to Take Effect on January 1st. Helsinki Times, December 28. Retrieved on July 6 from http://www.helsinkitimes.fi/finland/finland-news/politics/16070-finland-s-beefed-up-data-protection-act-to-take-effect-on-january-1st.html

**Tikkinen-Piri, C. Rohunen, A, Markkula, J. (2018).** EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review*. 34(1). pp. 134-153.

**Villas Boas, A. (2019)**. Wuawei has been Blacklisted by the US Government. *Business Insider*. March 20. Retrieved on Feb. 8 from https://www.businessinsider.com/huawei-us-ban-similar-to-zte-us-ban-2019-5?r=US&IR=T

**Watts, G. (2019).** US is losing the 5G war to China. *Asia Times*. Retrieved in July from https://www.asiatimes.com/2019/07/article/us-is-losing-the-5g-war-to-china/

**Wu, T. (2011).** The Master Switch: The Rise and Fall of Information Empires. Random House, NY.

**Zuboff, S. (2019).** The Age of Surveillance Capitalism: The Fight for a Human Nature in the New Frontier of Power. Hachette Book Group, NY, USA.