5G Privacy: Scenarios and Solutions

Madhusanka Liyanage*, Jukka Salo†, An Braeken‡, Tanesh Kumar§, Suranga Seneviratne¶, Mika Ylianttila‖
*§‖ Centre for Wireless Communications (CWC), University of Oulu, Finland,
†Nokia Networks, Finland, ‡Industrial Sciences Department, Vrije Universiteit Brussel, Belgium.
¶School of Information Technologies, The University of Sydney, Australia.
Email: *§‖[firstname.lastname]@oulu.fi, †jukka.salo@nokia.com, ‡an.braeken@vub.ac.be,
¶suranga.seneviratne@sydney.edu.au

***Abstract*—The next mobile generation, 5G, is expected to bring an enormous amount of new services and increased user experience. However adequate protection mechanisms for data and user privacy are required as this new technology will play a crucial role in society by connecting vertical industries, such as smart-grids, e-health, finance, transport and manufacturing. In this paper, we identify the most important privacy issues caused by the new technologies planned to use in 5G. Then, we discuss the objectives for privacy protection in 5G and correlate the identified issues with these objectives. Finally, we highlight how these objectives can be met by both a regulatory and technological approach. To this end, several privacy preserving technological solutions are presented for 5G networks.**

***Index Terms*—5G, Privacy, Network Security, SDN, NFV, Telecommunication, Cloud Computing**

I. Introduction

Due to the rapid increment of mobile users, popularity of Internet of Things (IoT) and bandwidth hungry digital services, telecommunication networks have to support over 1,000 times increased traffic volume by 2020. However, the existing telecommunication architectures are too rigid, static and inflexible to support booming traffic demand and new network services. Therefore 5G, which is the next generation of the mobile telecommunication networks, is expected to be deployed by 2020 [1]. 5G will offer greater capacity, higher-speed, more dynamicity and more cost-efficiency than any generation has provided before [2].

The 5G network architecture will be developed based on new technology concepts, such as Software-Defined networking (SDN), Network Function Virtualization (NFV) and cloud computing [2], [3] to achieve the above features. The SDN concept proposes to separate the control and data planes [4]. NFV allows to implement the control functions as virtualized functions in a mobile cloud [5] and share them among a pool of network hardware on-demand basis. Cloud computing enables on-demand network access for mobile networks to a shared pool of configurable hardware and storage resources [6].

As recognized by the United Nation and other governing organizations, privacy is a basic human right [7]. Privacy is the right of each person to choose or decide which personal information should be available to others. Moreover, each individual has the right to choose under what conditions his personal information can be accessible by others. In this manner, unapproved auxiliary utilization of individual data, unauthorized access of securely stored individual data, unauthorized gathering of individual data, and blunders in gathered individual data will lead to privacy violations. As humans are becoming a part of the "always connected" paradigm with more and more utilization of digital services in day to day life, it is challenging to ensure the privacy of users [8].

The rise of the new architecture, new technologies and new network services in 5G will open up new challenges to privacy protection and achieving privacy objectives. Most of the mobile users already have some experience with services providing security and privacy by earlier generations of telecommunication networks [1]. In order to provide continuity of perceived security, 5G networks should also offer at least an equal degree of security and privacy as current networks, even though 5G networks may implement different security mechanisms. However, the privacy awareness is significantly increasing among the users. In present day, most of the mobile phone users are concerned and informed about their privacy [9]. They are not downloading mobile applications which they do not trust. Nonetheless, many mobile users are still not hesitating to store their personal information on mobile phones due to easy accessibility. As a result, future mobile phones will have more personal information which must be protected [9]. Therefore, 5G networks need to provide an extra level of security compared to the earlier generation of networks.

This paper discusses the impact of new technologies such as SDN, NFV and cloud computing on the new 5G mobile network. We present a list of possible privacy protection approaches that can be used to ensure 5G privacy. To the best of the authors' knowledge, this is a first paper which provides a complete overview on 5G privacy, privacy challenges and possible solutions.

The rest of the paper is organized as follows. Sections II and III briefly introduce 5G privacy and its challenges respectively. Objectives of 5G privacy protection are discussed in Section IV. Possible privacy protection mechanisms for 5G are presented in Section V. Section VI contains the conclusion of the research.

II. 5G Privacy

Privacy in general deals with the protection of personal information which may reveal or may lead to hinting any details of personal information/activities regarding a specific user. If such information is not secured well enough, it might

be used by any intruder to notice their daily activities and eventually can be utilized to harm them through various means. Having privacy does not mean that the user needs to protect all the personal data in every case. For instance, in certain situations some piece of personal information can be shared with authorized entities under some criteria. Privacy also shows how much the users have the control over their own private data. However, according to James Moor, controlling whole the information in digital world is unfeasible or impractical, but preserving privacy may be referred to as the ability for a valid entity to access information at the right time under certain conditions [10].

Privacy in 5G networks will be crucial because it will bring huge transformation in terms of new daily life applications and access modes of digital services. Also, 5G will bring new enhancements in terms of architectural and service oriented requirements as compared to traditional mobile networks (3G, 4G), so it will require strong privacy polices and regulations. 5G privacy will be vital for whole eco-systems including users and various other stakeholders. Therefore, in order to have complete public acceptance and adoption of the 5G network, it is mandatory that privacy issues are well addressed. User privacy of 5G mobile network can be divided into three main categories; *data*, *location* and *identity privacy* [11]. In this section, we explain each privacy category under the 5G network framework.

Data Privacy: Data privacy represents the confidentiality and privacy of stored data. As the advancement towards future 5G mobile networks is rapid and concrete, consumers will be giving more preference to mobile networks as compared with traditional internet based services. Consequently, 5G mobile networks are expected to have high data speed and low latency, which eventually results into huge volume of data. For example, the critical applications such as healthcare and banking will generate sensitive user data and thus require data protections while storing and utilizing that data.

Location Privacy: With the advent of 5G technology, Location Based Services (LBS) are getting more important as users can access useful services based on knowing the location information [12]. Also, nowadays, several gadgets possess the capabilities of positioning and tracking, providing numerous location based services [13]. For example, online applications on mobile devices can suggest locations of various hospitals, restaurants, shopping malls etc, that are the nearest to the particular user. Recently various social networking websites such as Facebook introduce location aware features such as 'check-in'. These features are very helpful in socialization of the people by knowing the location of nearest friends/relatives. However, along with such kind of services, users would be continuously tracked by various actors through their personal gadgets or devices embedded in the environment and that could cause serious concerns to user's privacy.

Identity Privacy: Identity privacy refers to protecting the identity information of the subscriber and the device/User Equipment (UE). With 5G and IoT, it is expected that billions of devices will be connected to the internet. In such digitalization, every entity (user or device) would be categorized by some identity in order to access or deliver required services. Using identities, services and personal information can be accessed. For example, online applications such as healthcare require identity to access patient information and online shopping or banking requires payment modes through some cards, which include identity information. similarly, the device identity can also lead to leakage of the user personal information [14], [15]. Thus, it is important to have secure and efficient identity management mechanism in 5G networks.

III. 5G Privacy Issues

The integration of new technologies such as SDN, NFV and cloud computing concepts into future 5G networks will open up numerous new privacy challenges. Some of these issues listed below may originate from the threats identified in the context of cloud concepts [16]. They are, however, also relevant to other concepts (i.e. SDN and NFV) as the implementation of those concepts are to a great extent exploiting the cloud technologies.

A. End to end (E2E) data confidentiality: In 5G, various heterogeneous service providers and operators will store and use personal data of consumers with or without their permission. There will be different stakeholders involved in the whole 5G eco-system for providing different services. Hence, the consumer's personal data will go through the hands of multiple actors in a process, thus it requires secure mechanisms to ensure end to end data confidentiality [17].

B. Responsibility ambiguity/Loss of Data ownership: In 5G networks various players are involved such as mobile network operators, cloud service providers and third party application developers. However, the ambiguity of roles of different users and corresponding responsibilities may induce business or legal dissension [18]. Lost of data ownership has some similarities to responsibility ambiguity [19]. The ownership of user data should be properly defined between network operators and other players by using firmly established, privacy enabled service agreements.

C. Bylaw conflict / Location of legal disputes: User data projection is depending on the bylaw of the hosting country according to the different applicable jurisdictions. There are, at least, three possible locations to choose from: that of the victim, that of the offender, or that of the service provider [20].

D. Shared environment: The network resources are virtualized and the same infrastructure is shared between different network service users such as Mobile Virtual Network Operators (MVNOs) and possibly competitors [21]. In such shared environment, unauthorized user data access attacks can be possible and that will compromise the user privacy [16] [22]. Various intra host attacks are demonstrated over the years. These attacks range from the exploitation of bugs in the hypervisor to Distributed Denial of Service (DDoS) attacks, which execute influence over other virtual machines [23], [24].

E. Different objectives for trust: The participating entities, network infrastructure providers, MVNOs, Mobile Virtual

TABLE I: Summary of privacy objectives with privacy issues of high impact and relevance

	Promote digital market	Balance of interests	Privacy legislation in global context	Foster interop-erability and data portability	Applicable law must be easy to define	Right to erasure and rectify	Increased responsi-bility and account-ability
End to end data confidentiality	X	X	X	X			X
Responsibility ambiguity/Data ownership	X		X		X	X	X
Bylaw Conflict/Location of legal disputes	X	X	X		X	X	X
Shared environment		X	X	X	X		X
Different objectives for trust	X	X	X	X	X	X	X
Loss of governance/ Loss of control	X	X	X		X	X	
Service Provider lock-in	X			X			X
Visibility	X	X	X	X	X	X	X
Trans-border data flow	X	X	X				
Hacking			X		X		X
Providing Information for Third party	X					X	X
IoT Privacy				X		X	X

Network Enablers (MVNEs) and Communications Service Providers (CSPs), may work collaboratively but could have different objectives/priorities for security [2], [21]. Moreover, they might be competing each other in the business world. As a result, they might not cooperate to ensure all the aspects of security and privacy are relevant to all the entities [22] [25].

F. Loss of governance/ Loss of control: For mobile network operators, migrating a section of its network to a cloud, implies to partially handovering the control to the CSPs [26]. This transition is causing lost of direct control of all network management operations. The network operator has to cooperate with the CSP to carry out activities that span the responsibilities of both parties [16] [18]. Loss of control is quite similar to loss of governance. Transitioning to cloud architecture requires a transfer of some of the control and responsibility of the mobile operator's information and system components to CSPs. However, these system components were under the operator's direct control in previous generations of networks. Thus, operators now have to be dependent on the cooperation of the CSP [16].

G. Visibility: The mobile operator needs to know the security measures of the CSP to define its privacy management plans. In most cases, CSPs may not want to share their security and privacy measures with mobile operators. As a result, mobile operators lose the full visibility of their networks [16] [18].

H. Trans-border data flow: Due to the increasing global connectivity, it is important to define how data is being stored and processed as well as transmitted outside the borders of the nation. However, different countries have a different level in data protection mechanisms [27]. In some countries, law enforcement agencies can intercept data in ways which are beyond what is acceptable in another country. Moreover, the personal data privacy values can be very different between different legislations. For instance, sexual orientation or religious beliefs which are not sensitive issues in one country can be very sensitive in another. With the use of public clouds, network operators will lose the physical boundaries of data storage. The current Internet routing protocols are designed to achieve the maximum redundancy and flexibility. Once the destination IP is defined, there is no restriction on how to reach the destination. Therefore, data packets which are transmitted within the country (start and end points are in the same country) can also cross the border of the country.

I. Hacking: Since 4G Long Term Evolution (LTE), the telecommunication networks are converted to an IP-based open architecture. As a result, recent telecommunication networks (including 5G networks) are now vulnerable to the full range of IP and web-based attacks including hacking. Moreover, high dependency of cloud technologies in 5G networks would further increase the vulnerability to hacking attacks which eventually cause serious privacy concerns to the users.

J. Providing information for third party: 5G opens up a new interface for third party application developers to use the telecommunication network. These developers can share or sell personal information with other parties by using their privileges to access the 5G systems. As an example, the health insurance portability and accountability act does not prohibit the sharing of user health information by using mobile apps. Moreover, the data sharing principle in a cloud based system could raise a lot of privacy concerns. The potential use of data for unpredicted future applications could compromise privacy [22] [28].

Moreover, newly added features such as network programmability and the connectivity support of various vertical industries increase the dynamic nature of 5G networks. It is important to keep configurations and access lists up to date for dynamic third party applications. Thus, the regular verification of existing security configurations with privacy policies is required. Inconsistencies between access rights might form privacy threatening vulnerabilities [29].

K. IoT Privacy: The 5G technology will further consolidate and empower the success of IoT. However, there is a huge

security problem in the current generation of IoT devices as security is often not inherently included in their design. A latest study [30] concluded that 20% of the creators do not consider security at all in their design and more than 40% of the developers do not encrypt their communications, mostly because of cost constraints.

On the other hand, history has shown in the attack on Dyn (October 2016) that even small devices such as webcams, thermostats, baby monitors and refrigerators (i.e. typical IoT devices), can be used to launch a successful distributed denial of service attack.

Consequently, if control can taken over these devices, also information shared by these devices are at risk. This information involves personal data, which might be sensitive to derive useful information for criminals (e.g. presence at home, health status, etc).

So, industry should be aware of the importance and address the correct countermeasures to offer a decent level of security to its users, otherwise the problems might explode with the arrival of 5G.

IV. Objectives for Privacy Protection

In order to ensure the protection of privacy in 5G networks, a list of privacy protection objectives has been identified, based on generic regulatory objectives and the regulatory objectives in cloud computing [16] [18]. These objectives are defined to secure the privacy in the context of 5G mobile networks technologies [2] [28].

1) **Promote the digital single market:** It is required to harmonize the privacy of digital services at global level. All relevant directives and legislative instruments should be encouraged to enable cross border policies.
2) **Balance the interests** in protecting privacy and in fostering the global use of services. All the countries should fully realize the benefits of new technologies.
3) **Privacy legislation in a global context** is required to ensure their compatibility with new technologies. Different jurisdictions should cooperate together to develop interoperable privacy requirements and facilitate the flow of information with required level of privacy protection. For instance, the "Safe Harbor" agreement between US and EU, requires US companies to obey EU regulations so that EU companies can store and process data in US data centers [29].
4) **Foster interoperability and data portability** support technology neutrality by avoiding mandated standards or preferences which could prevent the interoperability. Moreover, it is needed to promote on-going interoperability efforts in the industry that will be useful to define uniform and global privacy policies.
5) **Define an easy applicable law:** It is required to define a single set of data protection laws which can be used across the border and they should be simple enough to be set up globally. Moreover, this framework should be based on the concept of accountability. These laws should also support self-regulatory codes and mechanisms.
6) **Include the right to erasure and rectify:** It is the right of each person to request the rectification of incorrect or incomplete personal data or to erase his/her personal information from the digital world. In particular, how the digital world handles the death of its users is also becoming increasingly important. Deceased individuals should have the right to privacy even after death and so their dignitary rights should extend posthumously [31].
7) **Increase the responsibility and accountability** of the entities who are processing the personal information and data. This also includes transparency towards the users in how personal data is processed and to which extent it is used.

Table I shows how the different objectives are influenced by the privacy issues of high relevance [32] [33] [34].

V. Privacy Protection Mechanisms for 5G

In this section, we discuss the possible mechanisms to protect the privacy of 5G networks by achieving the privacy objectives.

*1) **Regulatory Approach**:* Regulation is required to promote the objectives of privacy among different entities. Regulation can be mainly categorized into three types [35] [32] [33].

- **Government Regulation:** The governments are responsible bodies for writing and enforcing regulations which are relevant to each country. Government level representations in multi-nation organizations such as United Nations (UN) and European Union (EU) are useful to extend national level regulation to global level [36].
- **Industry Self-regulation:** At the industry level, different industries and industrial groups can develop principles and practices that reflect consensus on the best approach to protect the privacy [37]. Currently, there are several industry-level standardization bodies like 3GPP (3rd Generation Partnership Project), NGMN (Next Generation Mobile Networks), ONF (Open Networking Foundation) and ETSI (European Telecommunications Standards Institute). These groups can influence not only their business partners but also other government level regulation bodies to meet industry standards on security and privacy [33].
- **Consumer or Market Regulation:** Consumers are the real users of the systems and they are the ones who need privacy protection. They can enforce the terms to obtain the desired level of privacy. They can also influence the governments through voting and industries through the marketplace choices [34].

In Table II, we present how the three above described regulatory approaches would contribute to achieve the privacy objectives [32] [33] [34]. In the table, "Yes" means that the regulatory approach in question (column) supports the privacy objective in question (row) and "No" means otherwise.

As can be concluded from the different perspectives summarized in Table II, the Government regulation is able to promote many of those targets, at least at EU level. In particular the

TABLE II: Perspectives on the regulatory approaches for 5G Privacy [32] [33] [34]

Criteria (Privacy Objectives)	Government regulation	Industry self-regulation	Consumer or market regulation
Promote the Digital Single Market	Yes. The responsibilities need to be defined in the same way across countries Yes. Agreements between governments are needed to push the European-wide standards and practices.	Yes. The traditional telecom entities can define inter-operable standards. No. Market dominating service providers prefer to use their own standards for interconnection and portability	No. Service providers define the privacy standards and rules.
Balance of interests	Yes. Possible in in region-wise (e.g. EU level). No. It is challenging to balance the interests across different regions (Europe, America, Asia) due to cultural and political differences.	No. Industrial entities always try to obtain the benefits of the new technologies. No. Cultural and differences in income level impact balance in different countries.	Yes. Consumers will select the operators who can provide the expected level of privacy and operators who offer that will succeed. No. Different opinion on privacy due to cultural and education differences.
Privacy legislation in Global context	Yes. Privacy legislation approaches as well as their compatibility with new technologies can be agreed at regional level (e.g. EU level). No. The privacy legislation with the new technologies is difficult to synchronize across different regions.	No. Local players may have very different views and interests about security and privacy Yes. Big international players will have interests to agree on rules which are applied globally.	No. Some regions are allowing the market regulation approach.
Foster interoperability and data portability	Yes. Agreements between governments can be used to push the global level standards and practices.	No. A dominant player may want to push their own closed standards on interoperability.	No. Consumers or corporate users have no power to push interoperability and data portability.
Applicable law must be easy to define	Yes. Regional governments (e.g. EU Commission) can agree on the applicable law for the region. Yes. Responsibility and accountability of those storing and processing data can be defined. No. The common agreement across different regions would be challenging to establish due to cultural and political differences.	No. The Industrial players may not have to agree on the applicable law due to the lack of mandate.	No. Consumers may not have to agree on the applicable law due to the lack of mandate.
Right to erasure and rectify	Yes. The governments or regional bodies (e.g. EU) can enforce the rule.	Yes. The consensus on the right to be forgotten can be reached between the companies of good reputation. No. Rogue companies which do not want follow industry standards may act differently.	No. Consumers cannot enforce to be forgotten by the service provider.
Increased responsibility and accountability	Yes. Governments can define and enforce the responsibility and accountability for Service Providers.	No. It is challenging due to the lack of clear definition of responsibility among service providers and users may evoke conflicts.	No. Consumers have no power to define nor to enforce responsibility and accountability rules.

traditional telecom players can also contribute to many of the objectives. Moreover, the consumer or market regulation has least impact on achieving any of the objectives. Therefore, Government regulation would be the best option to promote the targets for 5G Privacy. In particular, the General Data Privacy Regulation (GDPR), applicable as of May 25th, 2018 in all member states of the EU already covers most of the identified objectives [38].

*2) **Privacy-aware Routing Mechanisms by using SDN**:* The use of SDNs in 5G networks and Internet will allow to design privacy-aware routing mechanisms [39], [40]. On an SDN network, user data packets containing privacy information that should not cross country borders could be identified. Then, the SDN controller could define flow rules so that these packets are routed only via the links and routers within the national borders. More sophisticated routing protocols can be designed by increasing the number of qualifiers. Thus, operators can define more flow rules on permitted and forbidden routes [41].

*3) **Hybrid Cloud Approach**:* A hybrid cloud approach allows the mobile operators to store critical data on the in-housed cloud and to process locally while less sensitive data is stored and processed on the public cloud [42]. In such an approach, operators can have full control of their data and can decide what to share to a public cloud [43]. Some use cases, such as enterprise IoT and health, motivate the use of hybrid cloud architectures consisting of private and public clouds. Moreover, the recent trends of using Multi-access Edge Computing (MEC) and Fog Computing concepts in 5G mobile networks will also increase the utilization of hybrid cloud approach [44].

*4) **Privacy by Design**:* Privacy by design is an approach in system engineering, which promotes the integration of privacy throughout the whole design process [45]. It has been defined in 1995 and recognized in 2010 by regulators from around the world as a fundamental component of fundamental privacy protection. The concept is based on 7 foundational principles, proactive and not reactive, privacy as default setting, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, respect for user privacy [46]. Consequently, the main idea of the privacy by design approach is

that it prevents privacy risks to occur. It is important to mention that it does not offer solutions, once privacy infractions have materialized [47].

Some guidelines to apply this methodology for the development of web applications are proposed by the OWASP Top 10 Privacy Risk Project[1]. Unfortunately, no concrete details are given on how to establish this approach in the design architecture of IoT or even 5G networks. In fact, in order to establish a privacy by design approach, the following steps should be realized.

- Definition of a general framework for addressing the requirements of the privacy by design policies.
- Development of highly efficient Privacy-Enhancing Technologies (PETs), able to cope with the scalability and interoperability issues within the framework.
- Implementation and evaluation of the solutions.

Existing privacy protection schemes require complex key agreements, using highly demanding cryptographic operations like elliptic curve pairing. Also solutions based on the existence of a trusted third party would cause too much delay in 5G low latency communications, due to the multiple required enquiries to this remote third party. A solution can be based on secret sharing principles, where the SDN controller is able to choose multiple paths in the network to transmit different parts of the data stream. Only the receiver, who is in possession of the secret shared key, is able to collect and reorganize all these pieces of information.

*5) **Software Defined Privacy Approach**:* In [29], authors demonstrate "Software Defined Privacy (SDP)" concepts which allow easy orchestration of existing tools to enforce privacy requirements of an Infrastructure as a Service (IaaS) cloud customer. This concept can be further extended to provide privacy protection for 5G networks. The SDP approach has also the same three layered model (application, control and infrastructure layers) as SDN.

The user defines the privacy protection level at the application layer by selecting the required privacy policies. Based on the user's selection, "Privacy Officers" define the set of rules which are transmitted to the control layer. This SDP methodology uses an agent-based approach at the control layer. These agents change the underlying infrastructure layer components such as hypervisors, virtual machines, storage systems, switches and other network components based on application layer privacy rules [29].

The SDP approach can be used to synchronize the network wide privacy policy management in 5G networks [48]. The centralized intelligence and controlling features in 5G networks enable the fast and efficient validation/synchronization of various privacy policies. The 5G network controller can also identify and remove redundant and overlapping privacy rules and even optimize the decision-making phase [49].

*6) **Service/Context Oriented Privacy Preserving Mechanism**:* Service oriented security and privacy preserving approaches will play a key role in 5G networks [17]. This is because, the privacy requirements in 5G networks may vary from one service to another one. For example, privacy needed healthcare related applications should be higher than the information searching based applications.

*7) **Security and Privacy Assessment**:* In order to address privacy issues as loss of visibility or protection inconsistency, a security and privacy assessment conducted by a trusted third party can provide a viable solution. However, such assessment requires in the first place the definition of a set of standardized and accepted measurable security metrics for the different network functions.

Table III summarizes which privacy issues (mentioned in Section III) can be solved by using the privacy protection mechanisms explored in this section.

TABLE III: Different Solutions to 5G Privacy Issues

Approach/Solution		Privacy Issue
Regulatory Approach	Government Regulation	A, B, C, F, H, I
	Industry Self-regulation	D, E, F, G, J
	Consumer/Market Regulation	A, D, E, J
Hybrid Cloud Approach		B, D, G, E, J, K
Privacy by Design		B, C, E, H, K
Software Defined Privacy		A, B, D, E, G, I, J, K
Service/Context Privacy Preserving Mechanism		A, D, J
Security and Privacy Assessment		A, B, F, G

VI. Conclusion

The deployment of Software Defined Networking (SDN), Network Function Virtualization (NFV) Cloud Computing concepts in 5G networks can trigger a number of privacy issues stemming mainly from the new interfaces, shared environments and new players with different views and objectives on privacy.

Privacy objectives are derived from the identified privacy issues. We discuss in this paper several technological solutions like, privacy-aware routing mechanisms by using SDN, hybrid cloud approach, privacy by design, and software defined privacy. However, the complete solution to achieve these privacy objectives goes beyond technology and involves a regulation and legal framework. In particular, it has been illustrated that government regulation is able to promote most of the objectives, at least at EU level. Moreover, the know-how and good practices from several communities (operators, cloud service providers, equipment vendors, government as well as users) are also required to solve the complete puzzle. We hope that this paper will trigger discussions in the telecommunication community around issues related to security and dependability, to serve as a catalyst of joint efforts in mitigating critical privacy issues.

Acknowledgment

This work has been performed under the framework of the SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems), 6Genesis Flagship (grant 318927) and

[1]https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

Towards Digital Paradise projects. This research is funded by Academy of Finland and TEKES, Finland. The authors would also like to acknowledge the contribution of the COST Action CA15127 (RECODIS) and CA16226 (SHELD-ON).

REFERENCES

[1] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[2] J. Rodriguez, *Fundamentals of 5G Mobile Networks*. John Wiley & Sons, 2015.

[3] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, 2015.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[5] N. M. K. Chowdhury and R. Boutaba, "A Survey of Network Virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, 2010.

[6] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile Cloud Computing: A Survey," *Future generation computer systems*, vol. 29, no. 1, pp. 84–106, 2013.

[7] "Universal Declaration of Human Rights," United Nations General Assembly resolution 217 A, accessed: 2018-04-30. [Online]. Available: http://www.un.org/en/universal-declaration-human-rights/

[8] M. Liyanage, I. Ahmad, A. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[9] L. T. Sorensen, S. Khajuria, and K. E. Skouby, "5G Visions of User Privacy," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–4.

[10] J. H. Moor, "Towards a Theory of Privacy in the Information Age," *ACM SIGCAS Computers and Society*, vol. 27, no. 3, pp. 27–32, 1997.

[11] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User Privacy, Identity and Trust in 5G," *A Comprehensive Guide to 5G Security*, p. 267, 2018.

[12] R. Di Taranto, S. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch, "Location-aware Communications for 5G Networks: How Location Information can Improve Scalability, Latency, and Robustness of 5G," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 102–112, 2014.

[13] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppanen, and M. Valkama, "High-Efficiency Device Positioning and Location-Aware Communications in Dense 5G Networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 188–195, 2017.

[14] P. Schneider and G. Horn, "Towards 5G Security," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1165–1170.

[15] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 159–166.

[16] J. Ruiter and M. Warnier, "Privacy regulations for cloud computing: Compliance and implementation in theory and practice," in *Computers, privacy and data protection: an element of choice*. Springer, 2011, pp. 361–376.

[17] Huawei, "5G Security: Forward Thinking," Huawei White paper, Tech. Rep., 2015.

[18] P. De Hert and V. Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals," *Computer Law & Security Review*, vol. 28, no. 2, pp. 130–142, 2012.

[19] B. J. Evans, "Much ado about Data Ownership," *Harv. JL & Tech.*, vol. 25, p. 69, 2011.

[20] K. Lee, "Security Threats in Cloud Computing Environments," *International journal of security and its applications*, vol. 6, no. 4, pp. 25–32, 2012.

[21] P. Rost, A. Banchs, I. Berberana, M. Breitbach, M. Doll, H. Droste, C. Mannweiler, M. A. Puente, K. Samdanis, and B. Sayadi, "Mobile Network Architecture Evolution Toward 5G," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 84–91, 2016.

[22] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software Defined Networking for Security Enhancement in Wireless Mobile Networks," *Computer Networks*, vol. 66, pp. 94–101, 2014.

[23] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[24] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147–165, 2016.

[25] Z. Yan, P. Zhang, and A. V. Vasilakos, "A Security and Trust Framework for Virtualized Networks and Software-Defined Networking," *Security and communication networks*, 2015.

[26] M. Chen, Y. Zhang, L. Hu, T. Taleb, and Z. Sheng, "Cloud-based Wireless Network: Virtualized, Reconfigurable, Smart Wireless Network to enable 5G Technologies," *Mobile Networks and Applications*, vol. 20, no. 6, pp. 704–712, 2015.

[27] C. B. Kuner, *Transborder Data Flows and Data Privacy Law*. Oxford University Press, 2013.

[28] Ericsson, "5G Security," Ericsson White paper, Tech. Rep., June 2015.

[29] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, "Software Defined Privacy," in *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*. IEEE, 2016, pp. 25–29.

[30] BARR Group, "Embedded Systems Safety and Security Survey," 2017.

[31] N. Chu, "Protecting Privacy after Death," *Nw. J. Tech. & Intell. Prop.*, vol. 13, p. ii, 2015.

[32] C. L. Miltgen and H. J. Smith, "Exploring Information Privacy Regulation, Risks, Trust, and Behavior," *Information & Management*, vol. 52, no. 6, pp. 741–759, 2015.

[33] S. Listokin, "Industry Self-regulation of Consumer Data Privacy and Security," *J. Marshall J. Info. Tech. & Privacy L.*, vol. 32, p. 15, 2015.

[34] C. Taylor and L. Wagman, "Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare," *International Journal of Industrial Organization*, vol. 34, pp. 80–84, 2014.

[35] M. J. Culnan, "Protecting Privacy Online: Is Self-regulation Working?" *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 20–26, 2000.

[36] S. G. Hoffman, *Regulation of Cloud Services Under US and EU Antitrust, Competition and Privacy Laws*. Peter Lang International Academic Publishers, 2016.

[37] J. Campbell, A. Goldfarb, and C. Tucker, "Privacy Regulation and Market Structure," *Journal of Economics & Management Strategy*, vol. 24, no. 1, pp. 47–73, 2015.

[38] "Rights of the Data Subject," Regulation (EU) 2016/679 : General Data Protection Regulation (GDPR), accessed: 2018-04-30. [Online]. Available: https://gdpr-info.eu/chapter-3/

[39] G. Asharov, D. Demmler, M. Schapira, T. Schneider, G. Segev, S. Shenker, and M. Zohner, "Privacy-Preserving Inter-domain Routing at Internet Scale," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 3, pp. 147–167, 2017.

[40] N. Shaikh, M. Krishnan, and G. Gulawani, "Enhancing Privacy and Security on a SDN Network using SDN Flow Based Forwarding Control," Jun. 29 2017, uS Patent App. 15/179,726.

[41] D. Pitt, "Trust in the Cloud: The Role of SDN," *Network Security*, vol. 2013, no. 3, pp. 5–6, 2013.

[42] B. Liang, *Mobile Edge Computing*. Cambridge University Press, 2017.

[43] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[44] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile Edge Computing? A Key Technology Towards 5G," *ETSI White Paper*, vol. 11, 2015.

[45] J. N. Okoye, "Privacy by Design," Master's thesis, NTNU, 2017.

[46] A. Cavoukian and M. Chibba, "A Regulartor's Perspective: Leading the Way with Privacy by Design," *Cyber security in future Internet, security and privacy by design. OUTLOOK, Visions and research for the wireless world*, no. 11, 2014.

[47] J.-H. Hoepman, "Privacy Design Strategies," in *IFIP International Information Security Conference*. Springer, 2014, pp. 446–459.

[48] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G Security: Analysis of Threats and Solutions," in *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*. IEEE, 2017, pp. 193–199.

[49] H. Li and H. Jin, "SDPMN: Privacy Preserving MapReduce Network Using SDN," in *Cloud Computing and Big Data (CCBD), 2014 International Conference on*. IEEE, 2014, pp. 109–115.