UiO : Faculty of Law
University of Oslo

5G, the GDPR, and Cybersecurity

European Union Member State Purchase of ‘Safe’ 5G Equipment

Candidate number: 8003

Submission deadline: December 1, 2020

Number of words: 17,991

Table of contents

Research Question

What are the challenges and issues regarding European Union (EU) Member State purchase of fifth generation (5G) telecommunication technology from China, South Korea, and the United States considering the EU legal framework?

Sub Questions

- What is the transition to 5G?
- What EU legal framework is relevant?
- What is the difference between the EU privacy framework and the privacy framework of China, South Korea, and United States?
- Are there GDPR-like safeguards in non-EU jurisdictions by virtue of the Brussels Effect?
- Does the EU-cybersecurity framework assist Member States in 'safe' decisions?
- From whom should the EU purchase 5G equipment?

Methodology

The analysis describes the transition to 5G, why it is necessary, and briefly, how the network will initially be constructed. It presents, generally, the stakeholders involved, and some risks and vulnerabilities presented by the network. Subsequently, it analyzes the EU privacy framework, and potential exemplifications of that framework in China, South Korea, and the United States. It then examines some of the EU cybersecurity framework to determine if it aids in the selection of 'safe' 5G equipment. In concluding, two diverging approaches are presented based on the application of privacy and cybersecurity perspectives, respectively.

Limitations

The decision regarding the purchase of 5G equipment is happening around the globe. This analysis uses the EU as an example because of its focus on privacy and its international landscape. Rather than examine various nations globally, it explores the issues occurring in the EU because its Member States in some cases must adhere to EU law, and like other nations around the world Member States must also observe respective national laws. Each Member State has a differing level of expertise and thus the EU serves as an experimental filed of sorts. However, the analysis is conducted through the lens of EU privacy and cybersecurity and thus should be treated as such.

Chapter 1: The Transition to the 5G Telecommunication Network

What is 5G and Why Should We Care?

Telecommunication networking is amidst a transition to its fifth generation. Each subsequent generation, from the retrospectively named first generation (1G) through the fourth generation (4G) has included iterative technological advancements, the addition of new capabilities, and respective security concerns. Industry groups, governments, and the private sector are trying to anticipate the pros and cons of this transition for future global societies. It is believed that the shift to 5G technology will be unprecedented, allowing near ubiquitous reliance on mobile networks, transforming industry and increasing network reliance by implementation of machine-to-machine networking in addition to person-to person networking.[1] Through this transition, new verticals in the automotive, healthcare, transportation, and utility sectors are expected and new environments, such as sensor-rich urban environments, smart cities, smart homes and smart work are anticipated to become a reality.[2] The industry anticipates 1.5 billion users will be subscribed to a 5G network by 2024, with coverage forecasted to reach over 40 percent of the world's population by 2024.[3]

In its EU Coordinated Risk Assessment (Coordinated Risk Assessment), The Network and Information Systems Directive Cooperation Group (NIS Cooperation Group - which will be introduced in a subsequent section), noted that 5G revenues would be estimated at €225 billion in 2025 and thus makes 5G a key asset to the EU's competition in the global market.[4] However, revenues are just one part of the issue. Understanding the new technology can be quite complex and it seems that engineers, government experts, and the private sectors are still settling on a consistent set of terms for the specific technological advancements as the precise architecture of the technology is not 100 percent known. Furthermore, standards bodies are increasingly tackling the security issues which are expected to be both known and unknow and widespread due to the increased attack surface.[5]

A notable element of the transition from 4G to 5G is a shift from a hardware-based network to a network more reliant on software. Other significant new capabilities include

---

[1] Tim Rühlig and Maja Björk, "What to Make of the 'Huawei Debate'? 5G Network Security and Technology Dependency in Europe," *Utrikespolitiska Institutet* Paper No. 10 (2020): 5-6.

[2] Tech4i2, Real Wireless, CONNECT- Trinity College Dublin, InterDigital, "Identification and Quantification of Key Socio-economic Data to Support Strategic Planning for the Introduction of 5G in Europe," SMART 2014/0008 (2016): 23-28.

[3] "5G Estimated to Reach 1.5 Billion Subscriptions in 2024 – Ericsson Mobility Report," Ericsson.com, November 27, 2018, https://www.ericsson.com/en/press-releases/2018/11/5g-estimated-to-reach-1.5-billion-subscriptions-in-2024--ericsson-mobility-report.

[4] NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* (CG Publication 02/2019, 2019), 3.

[5] NIS Cooperation Group, *Coordinated Risk Assessment*, 7.

enhanced mobile broadband (eMBB) - which will allow faster and more reliable uploading and downloading as well as virtual and augmented reality (VR/AR); ultra-reliable and low latency communication (URLLC) - which will lower response time from the network allowing real-time services to operate; and massive machine-type communication (mMTC) – scalable and efficient networking that will allow machines and devices to connect to the internet,[6] i.e. the internet of things (IoT),[7] and will comprise what many experts are calling the fourth industrial revolution, or Industry 4.0.[8] In its Recommendation for Cybersecurity of 5G networks, the European Commission (the Commission)[9] adopted a definition of 5G, and although there are other definitions in existence,[10] the Commission's definition is used because the EU legal framework is assessed herein; the definition is as follows:

> "5G networks' mean a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations of mobile and wireless communications technology such 4G or 3G. 5G networks should be understood to include all relevant parts of the network."[11]

To expand on this definition for purposes of understanding the significance, the need, and the security risks involved in the transition, it may be helpful to breakdown in very simplified terms, the construction of the new network.

Construction and Capabilities of the 5G Network

To enable the advances, two types of networks will be constructed, Non-Standalone 5G (NSA) and Standalone 5G (SA). NSA will require less investment by building upon existing

---

[6] Rühlig and Björk, "Huawei Debate," 5-6. See also Soldani and Huawei Technologies Australia, "'5G' and the Future of Security in ICT," *29th International Telecommunication Networks and Applications Conference* (2019): 3.

[7] Matt Burgess, "What is the Internet of Things," *WIRED*, February 16, 2018, https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

[8] Bernard Marr, "What is Industry 4.0," *Forbes*, September 1, 2018, https://www.forbes.com/sites/bernard-marr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/.

[9] According to its website, the Commission – proposes and enforces legislation along with implementing policies and the EU budget.

[10] See definition in István Bozsóki et. al. under the supervision of ITU, *Setting the Scene for 5G: Opportunities & Challenges* (Geneva, Switzerland: ITU, 2018), 3; and GSMA 5G Taskforce, *5G Guide A Reference for Operators*, April 2019, 25 (see specifically the acknowledgment of differing perspectives on the definition of 5G).

[11] European Commission, *Commission Recommendation of 26.3.2019 Cybersecurity of 5G* Networks (Strasbourg, 2019), 5.

4G networks, as early as 2020,[12] and will mainly increase network speed.[13] To accomplish this, the network will use multiple spectrum bands and small cells to allow for the highest quality and most ubiquitous connection possible.[14] On the other hand, the SA configuration will require construction of an entirely new network but will eventually support all the above-mentioned capabilities (eMBB, URLLC, and mMTC) in addition to allowing capabilities such as network slicing – a layer of shared infrastructure dedicated to a specific use,[15] and voice over new radio (VoNR) – 5G's mobile voice capabilities.[16] But, why is a shift to 5G necessary?

Implementing a shift to the use of Internet Protocol (IP) for data traffic and increased minimum data rates, 4G saw significant speed improvement from 3G networks.[17] However, the technological advances as well as an expanded user base have led to congestion in the 4G network. Additionally, the second phase of SA 5G networks will allow Industry 4.0 to move forward full throttle. The operation of critical AI, such as autonomous cars, remote surgery devices, and other industrial robots requires the network to respond nearly instantly to assure reliable and real-time services. This will require a shift from the hard-wired-based 4G network to a software-based network using radio access networking (RAN) for cloud technology and available hardware infrastructure for edge computing, i.e. the "softwarization" and "cloudification" of the fifth generation of telecommunication networking,[18] also known as Software Defined Networks (SDN).[19] Edge computing leverages 5G networks in the vicinity of the end-user achieving the desired and necessary reduction in latency.[20]

However, the technology is anticipated to require, among other things, capacity building in trained personnel to maximize the potential benefits offered by the transition, to maximize implementation worldwide, and also to ensure the complex network is a secure network that will be able to withstand vulnerabilities.[21] This is not a new theme, but rather one of technology

---

[12] "NIS Cooperation Group," European Commission – Shaping Europe's Digital Future, accessed October 27, 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[13] Soldani, "5G," 3.

[14] Christian de Looper, "'What is 5G?' The Next-Generation Network Explained," *Digital Trends*, May 22, 2020, https://www.digitaltrends.com/mobile/what-is-5g/.

[15] Ericsson, "Network Slicing is Ready to Impact" *Digital Services (blog)*, accessed October 27, 2020, https://www.ericsson.com/en/digital-services/network-slicing.

[16] Soldani, "5G," 3. See also Rühlig and Björk, "Huawei Debate," 7.

[17] Sound, "Evolution of the G," *Stanford Management Science and Engineering* (blog), last modified July 11, 2017, https://mse238blog.stanford.edu/.

[18] Ianire Taboada and Himanshu Shee, "'Understanding 5G' Technology for Future Supply Chain Management," *International Journal of Logistics* 2: 3.

[19] NIS Cooperation Group, *Coordinated Risk Assessment*, 6.

[20] Najmul Hassan, Kok-Lim Alvin Yau, and Celimuge Wu, "Edge Computing in 5G: A Review," *IEEE Access* 7 (2019): 127283.

[21] See references to deficiencies in trained and specialized personnel in NIS Cooperation Group, *Coordinated Risk Assessment*, 20. See discussion on cybersecurity workforce gap in William Crumpler, and James Lewis, *The Cybersecurity Workforce Gap*, (Washington, D.C.: Center for Strategic and International Studies, 2019), 1-10, https://www.csis.org/analysis/cybersecurity-workforce-gap.

generally as it tends to continually outpaces society's ability to fully utilize and regulate it all while transforming job markets and determining the new skill sets required to tackle the potential issues and benefits it presents.[22] Naturally, as would be the case most large technological shifts, many stakeholders are involved, which will be explored in the proceeding sections.

Security and Vulnerability Concerns of the 5G 'Security Stakeholders'

The stakeholders in the shift from the 4G telecommunication network to 5G are somewhat different, and are affected by present complex geopolitical issues, the technology supply chain, privacy regulation, cybersecurity regulation, and more. Who contributes to the standards is important for a number of reasons including intellectual property royalties, interoperability, privacy, security, and connectivity to name just some of the reasons.[23] Also, due to the ubiquity and potential of the 5G network, global and multi-stakeholders across various regions and countries have been hard at work to shape and define 5G.[24] Among the interested groups, with differing and sometimes converging motivations and sway, are stakeholders from governments, industry, society, intergovernmental organizations, coalitions, and more. The subsequent introduction of stakeholders is not an exhaustive list, but rather an introduction to the stakeholders in a general sense and demonstrates the complexity of the network and competing interests.

Stakeholders in a Broader Context

Technical standards development emerged as a central issue in the development of 5G technology, [25] and suppliers seek to influence and contribute to the process. The International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies (ICTs) is responsible for, among other things, allocating the radio spectrum relevant to 5G and previous generations as well as developing minimum technical standards to ensure technologies seamlessly interconnect.[26] In its IMT-2020 (5G) alongside the other stakeholders it defines minimum standards for the systems, components, and related

[22] Mar Camacho et. al., *Capacity Building in a Changing ICT Environment* (Geneva, Switzerland: International Telecommunications Union, 2018), 5, https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.01-2018-PDF-E.pdf.

[23] Gisela Grieger, *5G in the EU and Chinese Telecom Suppliers*, (European Parliamentary Research Service, 2019), https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf.

[24] GSMA 5G Taskforce, *5G Guide A Reference for Operators*, 30.

[25] Xinsheng Ji et. al., "Overview of 5G Security Technology." *Science China - Information Sciences* 61, no. 8 (2018): 2 and 19.

[26] "About International Telecommunications Union (ITU)," ITU, accessed October 27, 2020, https://www.itu.int/en/about/Pages/default.aspx.

elements that support capabilities beyond previous generations' standards of IMT-2000 (3G) and IMT-Advanced (4G).[27]

Other stakeholder include the 3rd Generation Partnership Project (3GPP), which according to its website, is a collaboration of telecommunications standardization organizations, organizational partners, and market partners (including industry, academics, and more) that collaborate within various working groups. Per its website, 3GPP meets regularly with the goal of developing specifications for various technologies within the overall 5G umbrella, including 5G technologies such as RAN. The organizational partners include associations from around the globe, including, China, Europe, South Korea, and the U.S., which will be discussed in a forthcoming chapter.[28]

More specific to Europe, but also in consideration of a global focus, are the 5G Infrastructure Public Private Partnerships (5G PPP) and the European Telecommunications Standards Institute (ETSI). The respective websites indicate that the former is a joint initiative between the Commission and European ICT industry with security architecture, subscriber privacy, and authentication mechanisms among its focus. Whereas the latter is the recognized regional standards body for telecommunications and other networks and services; specifically pertaining to 5G the ETSI is working on privacy, Network Function Virtualization (NFV) security standardization and security functions, as well as Multi-Access Edge Computing (MEC) security standards within RAN that aims to deliver security and robustness.

More generally, the standards of the Internet Engineering Task Force (IETF), an open standards organizations, are relevant because 5G will use Internet protocols.[29] And various groups representing industry and the private sector, such as Global System for Mobile Communications (GSMA),[30] the organization representing mobile network operators (MNOs) from around the world[31] will be important for cooperation and collaboration in the further creation of standards. Additionally, organizations and coalitions focused on open and inclusive specifications, may become relevant as political, trade, and intellectual property challenges rear their heads.[32]

EU Stakeholders: Security and Vulnerability

Since this analysis will focus on privacy and security given the legal framework of the EU, it is important to introduce the security stakeholders from an EU perspective. According to

---

[27] Bozsóki, *Setting the Scene for 5G*, 19.

[28] "Partners," 3GPP, last modified 2020, https://www.3gpp.org/about-3gpp/partners.

[29] Ijaz Ahmad et. al., "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine* 2, no. 1 (2018): 42.

[30] The GSMA is also offering training courses on capacity building in the 5G network.

[31] For example, the GSMA.

[32] Some might see the O-RAN Alliance as an example.

the EU's Coordinated Risk Assessment,[33] the stakeholders include MNOs, suppliers of MNOs and their respective subcontractors, manufacturers of connected devices and relevant service providers, and other stakeholder such as service and content providers, as well as end-users.[34] Each of these stakeholders is also a corresponding "security stakeholder" that can assist in keeping the network more secure overall.[35] However, the security concerns and vulnerabilities in the 5G network will shift with the transition from NSA networks, building off architecture of previous generations and the SA networks of the future. The respective stakeholder concerns will be discussed following a cursory introduction of the general security and vulnerability concerns of 5G.

The security concerns regarding 5G range from the issues already existing on the 3G and 4G network, as the NSA networks will be built upon those networks, to security issues and vulnerabilities unique to the 5G network. For example, 3G allowed the migration of Internet security vulnerabilities and threats into the new network, and 4G enabled smart device proliferation, multimedia traffic, and new services along with their respective security concerns to migrate into the telecommunications network.[36] Subsequently, there will be constantly evolving additional security concerns.

Two groups working to address security concerns in the EU are the EU's cybersecurity agency (ENISA) and the NIS Cooperation Group. According to the Commission's website, ENISA provides support to Member States, EU institutions, and businesses in key areas involving cybersecurity, which includes implementation of the Directive on Security of Network and Information Systems (NIS Directive). The NIS Cooperation Group, which was created by the NIS Directive ensures cooperation and information exchange between and among EU Member States in the area of cybersecurity.[37] According to ENISA, in its report on security incidents in the telecommunication industry, specifically a section regarding multiannual trends collected in the year 2012 through 2018, the most frequent security incidents (as percentage of overall reported incidents) were as follows:

(1) 68 % system failures (36% hardware failures and 29% software bugs).
(2) 17 % human errors.
(3) 9 % natural phenomena.
(4) 4 % malicious actions (specifically Denial of Service attacks and damage to physical infrastructure).[38]

---

[33] Which, according to the title page of the report was conducted in 2019 by the NIS Cooperation Group and is a compiled report of risk assessment in the respective EU Member States.

[34] NIS Cooperation Group, *Coordinated Risk Assessment*, 9.

[35] NIS Cooperation Group, 9.

[36] ENISA, *Threat Landscape for 5G Network* (2019), 4.

[37] European Commission – Shaping Europe's Digital Future, "NIS Cooperation Group."

[38] As reported in ENISA, *Annual Telecom Security Incidents 2018* (2019), 14.

Based on the incidents reported in this period, system failure and human error are of greatest concern, which theoretically could continue given the nature of the construction of the 5G NSA network. This is notable because as mentioned earlier, the 5G networks while still reliant on hardware, will rely heavily on software networking and so software bugs are a huge concern. This may increase incidents in 5G networks as dependency on software increases. Furthermore, the complicity of the threat landscape can be seen to expand as demonstrated by ENISA in its Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (Threat Assessment), which lists a complex set of assets, threats, and scenarios which will require addressing (see specifically Annex A: Assets Map, Annex B: Threat Taxonomy Map, and Annex C: Mapping Risk Scenarios to Cyberthreats).[39]

The framework from its Coordinated Risk Assessment is used in the subsequent analysis, specifically regarding the introduction of security stakeholders; however, note that there are many approaches to risk assessment being used around the world and this is not the only good metric.[40] To that end, as it pertains to individual security stakeholders, the NIS Cooperation Group in the Coordinated Risk Assessment (stemming from the approach set out in ISO/IEC 27005[41] risk assessment methodology),[42] noted that general concerns for all security stakeholders include some additional as well as more specific security vulnerabilities, including vulnerabilities arising from: the failure of any other stakeholder to appropriately address security processes, especially within a specific stakeholder's category; the complexity of the 5G network; reliance of economies, societies, and critical functions on the 5G network; major security flaws; intentionally inserted backdoors; specific 5G technologies, such as SDN, network visualization functions (NVF), and an increased reliance on the cloud and its respective configuration; processes and features required to comply with lawful intercept requirements; data leakage between virtual environments or network slices; and vulnerabilities related to process or configuration-related issues.[43]

Furthermore, each stakeholder mentioned above will have its own set of security concerns and will have to work on capacity building to assure experts are mobilized. All stakeholders,

---

[39] ENISA, *Threat Landscape*, 80-83.

[40] Many nations and organizations use ISO/IEC framework but also have their own respective frameworks or best practices. For example, the NIST in the U.S. has various security and privacy framework that are sometimes used voluntarily or are mandated by law to be used by businesses, organizations, or agencies.

[41] ISO is a non-governmental international organization with an extensive global membership base that creates standards, and ISO/IEC 27005 is a set of standards from ISO pertaining to information security See https://www.iso.org/about-us.html. See also, https://www.iso27001security.com/html/27005.html. Not that there are other frameworks, best practices, and methodologies for Risk Assessment, but the EU uses ISO in its Coordinated Risk Assessment.

[42] According to Harris and Maymí in the *CISSP All in One Exam Guide*, other standards, best practices, and frameworks include Zachman Framework, TOGAF, DoDAF, MODAF, SABSA model, COBIT, NIST, COSO, and more; respective uses are highly context dependent, 15.

[43] NIS Cooperation Group, *Coordinated Risk Assessment*, 19-20.

but particularly MNOs will be concerned about vulnerabilities due to a deficiency of specialized and trained experts, deficiencies in the requirements of risk assessments including internal security controls, monitoring practices, security management systems, patch management, and other operational maintenance procedures, as well as non-compliance with 3GPP specifications and other industry best-practice standards.[44] Additional vulnerabilities specific to MNOs include bad architecture and design of the 5G network, bad physical security practices for the network and infrastructure, inadequate policies for local and remote access to network components, failure to appropriately address security in procurement, and deficient change management practices.[45]

Concerns relevant to suppliers are also worthy of assessment especially considering the increased role of software and third-party services in the 5G network.[46] In addition to technical security concerns, Member States have to contend with business concerns, dependency issues, supply chain considerations, geopolitical concerns, and threat-actor concerns.[47] Note that this isn't an assessment of every concern possible but just an assessment of major concerns related to the transition of the network and the sale of 5G equipment in the EU.

Relevant Legal Framework and General Assessment Criteria

Although, non-binding, in its Cybersecurity of 5G Networks recommendation, The Commission noted that the overall strategy of cybersecurity in the new network would require analysis of many different EU directives, regulations, etc. as well as the work of various cooperation groups. A careful analysis of the electronic communications regulatory framework, the Cybersecurity Act,[48] the NIS Directive,[49] the General Data Protection Regulation (GDPR),[50] and Member States' laws would be a good start. Additionally, considerations for the digital single market and to the cybersecurity concerns regarding critical functions and general resilience, capacity building and the basic tenets of confidentiality, integrity, and availability are also necessary.[51] Holistically, the legislative framework covers the topic, but each has a different focus.

One of the Cybersecurity Act's biggest claim to fame is providing a permanent mandate for ENISA.[52] It also creates an EU-wide certification scheme for ICT products, services, and

[44] NIS Cooperation Group, 20-21.

[45] NIS Cooperation Group, 21-22.

[46] NIS Cooperation Group, 22.

[47] See generally NIS Cooperation Group.

[48] Parliament and Council Regulation 2019/881, 2019 O.J. (L 151) (EU). [hereinafter Cybersecurity Act].

[49] Parliament and Council Directive 2016/1148, 2016 O.J. (L 194) (EU). [hereinafter NISD].

[50] Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) (EU). [hereinafter GDPR].

[51] European Commission, *Cybersecurity of 5G* Networks, 5.

[52] Cybersecurity Act, art. 3.

processes. While certification is voluntary unless otherwise proscribed by Union or Member State law, the Commission encourages making certification mandatory for 5G products, services, and processes after their development.[53] Although merely in its preamble, the Cybersecurity act mentions security-by-design and security by default being aims of the act in an effort to encourage implementing security at the earliest stages of design and development and to ensure that the most secure setting are implemented by default.[54]

Intimately related to ENISA is the NIS Directive. The NIS Directive created the NIS Cooperation Group which, as already mentioned, aids in ensuring strategic cooperation and the exchange of information among EU Member states regarding cybersecurity.[55] Although, matters of national security is a competence belonging to EU Member States, the EU's role is complementary and some hope harmonization can be an end goal.[56] Furthermore, the NIS Directive seeks to regulate various 5G stakeholders, such as Operators of Essential Services (OES) and Digital Service Providers (DSP) by requiring them to have in place appropriate and proportional technical and organizational measures to manage security risks Computer Security Incident Response Teams (CSIRTs).[57] Significantly, the Cooperation Group was also tasked with and has since created the Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (the Toolbox) identifying common best practices, and appropriate, effective, and proportionate risk management measures for Member States to mitigate identified cybersecurity risks.[58]

The GDPR expounds on the above-mentioned requirements by imposing security requirements including preventing unauthorized access to personal data and by regulating generally processors and controllers of personal data.[59] And, like the Cybersecurity Act it takes a stab at ensuring consideration during early development and design stages through the concept of data protection by design and default (sometimes referred to as Privacy by Design).[60]

Cumulatively and per the Commission's Recommendation, these pieces of legislation seek as one of their objectives to determine a common set of measures to mitigate and prevent potential privacy and cybersecurity risks.[61] Furthermore, the Recommendation encourages that these overarching goals be done through the assessment of the broader categories of technical consideration, which includes, inter alia, cybersecurity and vulnerability assessments, including but not limited to assessment of unauthorized access, cyber espionage, and potential for malicious acts during the design, development, procurement, deployment, operation, and

---

[53] European Commission, *Cybersecurity of 5G* Networks, 16.

[54] Cybersecurity Act, preamble (12) and (13).

[55] European Commission – Shaping Europe's Digital Future, "NIS Cooperation Group."

[56] Grieger, *5G in the EU*.

[57] NISD, art. 14 and 16. See also European Commission, *Cybersecurity of 5G* Networks, 13.

[58] Recommendation 14 and 15 in European Commission, *Cybersecurity of 5G* Networks.

[59] Recommendation 16 in European Commission, *Cybersecurity of 5G* Networks.

[60] GDPR, art. 25.

[61] Objective (1)(c) and 4(a) to (d) in European Commission, *Cybersecurity of 5G* Networks.

maintenance stages; strategic considerations, which includes, inter alia, risk of influence by a third country by assessing concerns regarding governance models, relevant cooperation agreements on security, adequacy decisions regarding data protection and privacy, and relevant multilateral, international, bilateral, or other treaty agreements and; for purposes of this discussion it is also prudent to explore market considerations.[62]

The bottom line is that when assessing Member States' purchase of safe 5G equipment, the respective States have a fair bit of latitude in tackling this complex issue. The criteria in which Member States are likely to assess when determining the path forward to safe 5G equipment will include: (1) security assessments – including technical, political, and legal, (2) regulatory framework and best practices, (3) strategic considerations – including the EU's goal of strategic autonomy and desire for diversity in the supply chain, and (4) economic realities. [63] However, the subsequent chapter's analysis will focus specifically on whether provisions in the GDPR contribute to an adequate assessment of safe 5G equipment.

Chapter 2: The Application and Extraterritoriality of the GDPR

Currently, the purchase of 5G equipment is a Member State issue since there is no binding regulation exactly on point and the guidance and recommendations are still developing.[64] Member States are going to approach safe 5G equipment based on their own respective assessments and this could potentially affect the long-term security of the network. The larger 5G-equipment suppliers come from various parts of the world (China, Finland, Sweden, South Korea, and the U.S.) and each have their own business, technical, political, and legal agendas. Barring an EU-wide regulation, Member States will have to decide based on applicable EU laws as well as their own national laws, political agenda, technical and strategic considerations who to purchase their equipment from.

However, experts around the world have noted that the transition to 5G if coordinated properly may allow the opportunity for security to be a more integrated part of the architecture,[65] unlike the development of the architecture of the internet which at least initially developed in a more technical, ad-hoc manner leaving security considerations to the end users, i.e. the end to end concept.[66] However, if Member States take very different stances regarding the purchase of 5G equipment, due to a lack of EU wide foreign and security policies, the market

---

[62] See recommendation 20 in the European Commission, *Cybersecurity of 5G* Networks.

[63] Grieger, *5G in the EU*.

[64] Noah Barkin, "Judy Asks: Should Europe Ban Huawei's 5G?" Carnegie Europe, January 30, 2020, https://carnegieeurope.eu/strategiceurope/80928.

[65] Christopher Krebs, Ajit Pai, Shane Tews, Paul Eisler, Sujit Raman, and Diane Rinaldo, "5G, Security, and the Internet of Things," July 22, 2020, Internet Governance Forum USA 2020, 41:45, https://www.igfusa.us/5g-security-and-the-internet-of-things/.

[66] Lee Bygrave, *Internet Governance by Contract* (Oxford: Oxford University Press, 2015), 17.

risks fragmentation and could limit the EU's influence in the development of 5G standards. [67] However, with 500 million consumers, the European market is the world's largest trading bloc and so 5G manufacturers and suppliers are likely to want to sell their goods in the EU.[68]

In assessing the research question, it is then relevant to ask whether the GDPR as the harmonizing regulation in this context and thus arguably the Brussels Effect can assist in adequately assessing what constitutes safe 5G equipment? To begin, an assessment of 5G processing of personal data will determine the applicability of the GDPR.

Application of the GDPR, Territoriality, and the Brussels Effect

If data isn't personal it is not within the scope of the GDPR. [69] The GDPR defines personal data as "any information relating to an identified or identifiable natural person," and includes references to identifiers such as name, ID number, location data, online identifier, and more.[70] Protection of personal data, while not an absolute right,[71] is recognized in the EU's constitutional framework as a fundamental right.[72] This is exemplified through the Court of Justice of the European Union's (CJEU) jurisprudence, which approaches personal data in a broad manner, through a fundamental rights lens.[73]

Additional considerations related to personal data are the concepts of pseudonymisation, and anonymous information. Anonymous and pseudonymous are categories of information, with the former information being outside the scope of the application of the GDPR and the latter requiring data to be treated as personal.[74] Anonymous information is information that "does not relate to an identified or identifiable natural person" or is "personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable."[75] However, ensuring anonymity is difficult because the "mere possibility of identification" renders data personal, even if the identification is done through a combination of information not directly attributable to an individual independently; information need not be in the hands of a controller/processor, but accessible without disproportionate effort.[76] The confounding issue is that it

---

[67] Rühlig and Björk, "Huawei Debate," 25.

[68] "Facts and Figures on the EU's Position in Global Markets," European Commission – EU Position in World Trade, accessed October 27, 2020, https://ec.europa.eu/trade/policy/eu-position-in-world-trade/.

[69]Samson Esayas, "'The Role of Anonymisation' and Pseudonymisation Under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach," *European Journal of Law and* Technology 6, no. 2 (2015), 2.

[70] GDPR, art. 4.

[71] GDPR, rec. 4.

[72] Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014), 58.

[73] Bygrave, *Data Privacy Law*, 58.

[74] James Clark, "GDPR Series: Anonymisation and Pseudonymisation," *Privacy & Data Protection* 18, no.1 (2017): 2.

[75] GDPR, rec. 26.

[76] Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing AG, 2017), 2 - discussing the ruling in Breyer case (C-582/14)).

is extremely difficult to render data anonymous with emerging technology leading to additional data or metadata that makes seemingly anonymous information personal data.

Given the aforementioned factors, assessing whether personal data is involved in a scenario requires a context specific analysis done on a case-by-case basis. However, because big data is at the heart of 5G we will make the generalized assumption that personal data is likely to be pervasive throughout the new networks.[77] Whether it be through location data at use in edge computing, or the aggregation of identifiers or seemingly innocuous metadata in the hands of different controllers, privacy poses a challenge in 5G.[78] And as already mentioned, anonymizing data is extremely difficult given the sheer volume of data in existence due to the anticipated ubiquity and large amount of use cases for the 5G network. Identifiability will certainly be a likely possibility. It may at times be possible to anonymize data, but this will likely be more the exception than the norm and when in doubt such data should be treated as personal data. Furthermore, even if personal data has been pseudonymized along the value chain, this data will need to be treated as personal. Thus, the GDPR is highly likely to be applicable. But, beyond the EU, how does this apply?

The territorial scope in Article 3 of the GDPR asserts that the regulation can sometimes apply to processing of personal data of data subjects who are in the Union by controllers or processors established outside the EU if processing relates to the offering of goods or services (in which payment or the exchange of personal data often suffices), or if processing relates to monitoring behavior or tracking on the internet.[79] This is important in an international context because Member States are looking beyond the EU to purchase 5G equipment. This means non-EU suppliers failing within the scope of Article 3 will need to apply the GDPR. However, is the GDPR sufficiently protective in the primary non-EU supplier jurisdictions? For this, we look the Bradford's Brussels Effect.

The Brussels Effect posits that in some cases, the EU through its legal institution and standards exports its rules to the rest of the world. By exploring if GDPR-like safeguards are in place in non-EU jurisdictions producing 5G equipment, this analysis can determine if the GDPR by virtue of the Brussel's Effect can influence the safe purchase of 5G equipment by respective Member States. In other words, does the GDPR act as and 'trading currency' with regards to 5G equipment by incentivizing non-EU companies to adopt GDPR-like privacy and security provisions in hopes of selling equipment in the EU market, as well as perhaps simplifying privacy compliance schemes?[80] If the answer is yes, can Member States subsequently rely on the

[77] Prajwol Kumar Nakarmi, Christian Schaefer, and Dario Casella, "5G and the EU General Data Protection Regulation," *Ericsson Blog*, December 11, 2017, https://www.ericsson.com/en/blog/2017/12/5g-and-the-eu-general-data-protection-regulation.

[78] Ahmad et. al., "Overview of 5G Security," 39.

[79] GDPR, art. 3(2)(a) & (b) and rec. 24.

[80] Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, no. 1 (2012): 17.

application of GDPR safeguards in non-EU markets to assure the safe purchase of 5G equipment? Or are the safeguards inadequate?

GDPR Safeguards

With the application of the GDPR being highly likely several safeguards will be required. And although highly context dependent, these safeguards generally include both organizational and material requirements for an entity meeting the requirements of controller or processor per the regulation. The following safeguards are likely to be applicable in some form to the non-EU suppliers of 5G equipment when supplying to Member States and thus the safeguards are introduced generally before assessing their potential effectiveness in the subsequent section.

Organizational requirements refer to obligations of companies to adhere to the GDPR's risk-based approach to data security or be subject to fines up to 20,000,000 EUR or 4% of total worldwide annual turnover.[81] This includes the principle of accountability, which is directly enforceable[82] and which requires controllers to ensure compliance with the GDPR, and be able to prove this compliance to the Supervisory Authorities.[83]

To ensure compliance, controllers must implement appropriate technical and organizational measures before beginning process operations, including internal policies, the use of scalable programs to implement data protection principles and other measures that meet Article 25, data protection by design and by default, as elaborated below.[84] Additionally, the basic principles of processing including, inter alia, lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and additionally records of processing activities relevant to one's status as controller, joint controller, or processor must be adhered to.[85]

In addition to the above-mentioned principles and requirements regarding security of personal data, the material requirements include general rules that processing of personal data is prohibited unless certain legal exceptions apply. This refers to the idea that controllers and processors must have a legal basis for processing and comply with certain provision of the GDPR depending on the type of data being processed.[86] For example, Article 6 lists such

[81] Voigt and Von Dem Bussche, *The GDPR*, 31.

[82] GDPR, art. 83(5).

[83] Voigt and Von Dem Bussche, *The GDPR*, 31.

[84] Voigt and Von Dem Bussche, 32 citing rec. 78 and the Art. 29 WP Opinion 3/2010 on the Principle of Accountability.

[85] Voigt and Von Dem Bussche, 32-33 and GDPR, art. 5 and 24-31.

[86] GDPR, art. 6-11 and rec. 32,33,38, and 40-57.

lawful bases of: consent, contract, legal obligation, vital interest, public task, and legitimate interest.[87]

It is prudent for companies, controllers, and processors to remember that Data Protection Impact Assessments (DPIA) are often required and that additional considerations are essential in the case of automated process and the processing of special categories of data or the data of children.[88] Furthermore, controllers and processors should ensure that those acting under their authority process personal data per their instructions and in accordance with EU and Member State law, as necessary. This includes consideration of adequacy or appropriate safeguards are in place in the case of international transfers of personal data, per Articles 45-49, and that safeguards should be tested, assessed, evaluated, and adjusted based on respective findings. [89]

The requirements contained in Article 25 - Data protection by design and default are particularly relevant to this discussion. Article 25(1), springs from the policy discourse commonly known as "Privacy by Design,"[90] and it is the idea that the conditions of processing data are fundamentally set by the software and hardware used in technology.[91] Therefore, when producers and manufacturers create their products, they should consider the principles required by the GDPR when creating their respective software and hardware. For example, considerations regarding minimally invasive use of data, data minimization, pseudonymization, and anonymization should be at the forefront of mind.[92] Furthermore, Article 25(2) emphasizes that by default, data should be lean, locked, and confidential, using only data that is necessary, and having the most privacy focused settings implemented by default.[93] Data subjects who are non-savvy with regards to technology should not have to consider opting in to secure regimes; the privacy should be inherent or baseline in the respective products or tools. According to the European Data Protection Board, (EDPB), the "main design objective is the effective implementation of the principles and rights of data subjects into the processing."[94]

The bottom line is that at the heart of these safeguards are consideration for data subjects, a risk-based approach with the goal of security being appropriate to evaluated risks, and the consideration for data privacy and data security at all stages of development and

---

[87] GDPR, art. 6. See also, the "Lawful Basis for Processing," Information Commissioner's Office, accessed October 27, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

[88] GDPR, art. 8-10, 22, and 35.

[89] GDPR, art. 5(1)(f), 25(1) to (3), 32(1) to (4), 45-46, and rec. 39, and 74-78. See also C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2019:1145. [hereinafter Schrems II].

[90] Christopher Kuner, Lee Bygrave, Christopher Docksey, and Laura Drechsler, *The EU General Data Protection Regulation (GDPR)* (Oxford: Oxford University Press USA – OSO, 2020), 573.

[91] Voigt and Von Dem Bussche, *The GDPR*, 62.

[92] Voigt and Von Dem Bussche, 62.

[93] Voigt and Von Dem Bussche, 63.

[94] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (2019), 25.

processing.[95] Article 32(1)(b) of the GDPR offers a connection to EU directives and legal instruments pertaining to cybersecurity, such as the work of ENISA and the security by design concept. Seeking out mature certifications or codes of conduct as well as examining guidance released by ENISA and the NIS Cooperation Group can aid the evaluation.

ENISA and the NIS Cooperation Group have guidance and publications that assist with specific implementation of safeguards, inter alia, security by design in IoT,[96] state of the art in IT security,[97] secure convergence in cloud and IoT technology,[98] as well as guidance on technical and strategic risk assessment to help protect critical assets. The EU Coordinated Risk Assessment,[99] the toolbox of risk mitigating measures[100] and its respective follow-up report[101] also help. Considerations of privacy and security safeguards should be considered during the entire lifecycle from inception to implementation. As discussed later, the importance of diversity of the supply chain, decreasing dependencies on single actors, assessments and protection of critical assets for proper implementation of safeguards, and a concern of non-EU or state-backed actors, particularly those having cyber offensive strategies and those lacking legislative or democratic checks and balances[102] relevant to the safeguards affecting the 5G supply chain should be stressed.[103]

Privacy as an Exemplification of the Brussels Effect

To explore the influence of EU privacy outside the EU, we return to the Brussels Effect. Before doing so, it is important to note that the EU's influence of data privacy worldwide has narratives alternative to Unilateral Regulatory Globalization, described herein. Among the narratives are EU data protection influence as a preservation of an economic position and also as

---

[95] Note that Article 1 of the GDPR also references regard to the free movement of personal data and specifically states in 1(3) that " the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with protection of natural persons with regard to the processing of personal data" which perhaps requires a balancing or consideration of the DSM.

[96] See generally ENISA, *How to Implement Security by Design for IoT* (2019), https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot.

[97] ENISA, "What is State of the Art" in IT Security?" *ENISA*, February 7, 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security#:~:text=The%20document%20published%20on%20the,advice%20and%20recommendations%20for%20action.&text=The%20document%20can%20serve%20as,classification%20of%20security%20measures%20implemented.

[98] Christina Skouloudi and Gema Fernandez, "Toward Secure Convergence of Cloud and IoT," *ENISA*, September 2018, https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot.

[99] NIS Cooperation Group, *Coordinated Risk Assessment*.

[100] NIS Cooperation Group, *EU Toolbox of Risk Mitigating Measures (*CG Publication 01/2020, 2020).

[101] NIS Cooperation Group, *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity* (CG Publication 02/2020, 2020).

[102] NIS Cooperation Group, *Coordinated Risk Assessment*, 22.

[103] NIS Cooperation Group, 25.

an exemplification of or focus on the protection of human rights.[104] Over 40 years, Europe has slowly and consistently developed norms based on the principles of "democracy, the rule of law, social justice and human rights."[105] Through its treaties and constitutional framework it reflects protection of personal data as protecting fundamental human rights and freedoms,[106] and its external influence can be viewed as an exemplification of that. Furthermore, its characteristics reflect requirements present in already existing human rights instruments.[107] Another perspective views the EU's influence as gaining strength through its combined market power and other factors, such as its regulatory capacity.

According to Bradford, the Brussels Effect requires a sufficiently large market with the institutional structures capable of enforcing regulations, a preference domestically for strict regulatory standards with the aim of regulating inelastic targets.[108] Furthermore, the standards must be advantageous to follow in that they outweigh the benefit of implementing more lenient standards in other jurisdictions, i.e. a company voluntarily implements the strict standards worldwide making the other regulations obsolete in the process.[109]

A prominent example of Unilateral Regulatory Globalization is the EU's privacy framework, aka the GDPR and the Supervisory Authorities, opinions, guidance,[110] that stem from the regulation. The EU's regard for privacy as a fundamental right and its preference for a comprehensive and strict regulatory regime enabling the potential of high fines has spread throughout the world with the adoption of similar provisions occurring globally.[111] Furthermore, once captured by the material and territorial provisions of the GDPR, many large multinational companies operating in the EU opt to implement the GDPR requirements worldwide to ease compliance burdens and perhaps even to obtain competitive advantages by gaining consumer trust.[112] While arguments can be made that this form of adoption rendering non-EU privacy regimes obsolete, concerns on the effectiveness of this method still remain and this is discussed in the next chapter. Also, some acknowledge arguments that the EU's external policies reflect

---

[104] See discussion on the policy thrust of the Data Protection Directive including realization of the internal market and privacy in the face of technical and economic developments in Bygrave, *Data Privacy Law*, 57.

[105] Graham Greenleaf, "'The Influence of European Data' Privacy Standards Outside Europe," *International Data Privacy Law* 2, no. 2 (2012): 92.

[106] Kuner, Bygrave, Docksey, and Drechsler, *The EU General Data Protection Regulation*, 106.

[107] Bygrave, *Data Privacy Law*, 101 discussing EU characteristics present in Convention 108 and ECHR Article 8.

[108] Bradford, 11.

[109] Bradford, 17.

[110] Bradford, 48-63.

[111] See Greenleaf's assessment of distinctive European data privacy indicators globally – 33 or 39 non-EU countries' privacy laws indicated evidence of influence unique to identified European data privacy indicators - in "The Influence of European Data."

[112] Gregory Voss and Kimberly Houser, "A personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies," *American Business Law Journal* 56, no. 2 (2019): 330.

imperialistic objectives,[113] while others see the EU's objectives stemming from a need to preserve a single market without undermining European companies,[114] or "as an expression and specialized branch" of human rights law.[115] Regardless, it's not without its limits and it's not the only avenue to regulatory globalization.[116] Other limitations relating to, among other things, economic realities, national security, geopolitics, and existing dependencies need to be acknowledged as well; this will be done in a brief manner in the subsequent analysis.

With all that in mind, it will be important to turn to an assessment of worldwide 5G equipment producers to see whether the GDPR adequately regulates in this arena. Will the safeguards truly have the intended effects when exported abroad and will the lack of a harmonized cybersecurity regime affect Member State's decisions ultimately? This can potentially be answered by an assessment of the safeguards implementation in foreign jurisdictions hoping to market and sell 5G equipment in the EU and EEA.

Chapter 3: Application of GDPR Safeguards in the Jurisdictions of Primary Non-EU Suppliers of 5G Equipment: China, South Korea, and the U.S.

The 5G Players

In addition to the EU, the primary 5G equipment providers are mainly based in China, South Korea, and the United States.[117] One might infer that the primary non-EU providers would like to sell their equipment to EU Member States as the EU is the world's largest trading bloc.[118] In theory, this requires respective suppliers to comply with EU data protection framework, to the extent the material and territorial scope of Article 2 and 3 of the GDPR are met, in addition to their own domestic laws, regulation, standards, and other obligations.

Therefore, it is important to explore concerns regarding whether non-EU obligations work with or are in tension with the EU data protection framework. An analysis of the following questions aim to address that concern. Do any of the primary non-EU 5G equipment providers have adequacy decisions in place with the EU? For the countries without adequacy decisions in

---

[113] Ian Manners, "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40, no. 2 (2002): 240.

[114] Bradford, "The Brussels Effect," 36.

[115] Bygrave, *Data Privacy Law*, 12.

[116] Bradford, "The Brussels Effect," 44 and 48 and considerations, inter alia, for market-driven harmonization, political harmonization, and consortium or business-based influence.

[117] According to Forbes, Ericsson, Nokia, Huawei, ZTE, Samsung, Cisco, Dell, and HPE are among the top players: Will Townsend, "Who Is 'Really' Leading in Mobile 5G, Part 4: Infrastructure Equipment Providers," *Forbes*, July 19, 2019, https://www.forbes.com/sites/moorinsights/2019/07/19/who-is-really-leading-in-mobile-5g-part-4-infrastructure-equipment-providers/.

[118] EU Commission – EU Position in World Trade, "Facts and Figures."

place, are there GDPR-like safeguards in place, and if so, what are those safeguards? Finally, are these safeguards and manifestations of EU law, to the extent they exist, adequate safeguards, why or why not?

Do China, South Korea, or the United States Offer Adequate Privacy?

According to Chapter V of the GDPR transfers to third countries can only take place if controllers and processor adhere to GDPR safeguards, this includes onward transfers across or to and from EU borders. Article 45 states that third countries and international organizations can only transfer personal data to a third country if the Commission has determined the country can ensure an adequate level of protection, via an "adequacy decision" or "partial adequacy" for a specific sector.[119] There are other manners in which cross border transfers may occur, such as binding corporate rules, derogations, and others but adequacy is at the top of the hierarchy.[120]

An adequacy decision offers a comparable or "essentially equivalent" level of protection as to the protection offered in the EU.[121] While a third country is not expected to offer identical protection, it must by means of its domestic law or international commitments offer a level of protection essentially equivalent read in light of the EU Charter of Fundamental Rights.[122] To arrive at an adequacy decision, the Commission considers a system as a whole to determine if the privacy protections offer a strong level of protection comparable to the EU, and also assesses rules on access to personal data by public officials, for national security purposes, and for law enforcement.[123] The consideration of access to personal data by public authorities builds upon the case law of the European Court of Human rights and the Article 29 Working Party's Adequacy Referential.[124] If adequacy decisions exist, the country or international organization is then offered the benefit of access to the EU single market.[125] Adequacy decisions are constantly monitored and can be changed at a later date.[126]

With that in mind, determining if there are adequacy decisions in place in the jurisdictions in which the major non-EU 5G equipment providers operate is a good starting point. To

---

[119] Commission Staff Working Document Accompanying the Document Communication from the Commission to the European Parliament and the Council Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation SWD (2020) 115 final (June 24, 2020). [hereinafter SWD 2020 115 final].

[120] GDPR, art. 46-49.

[121] Schrems II. See also GDPR, art. 45 and rec. 104.

[122] See paragraph 73 of Schrems II.

[123] SWD 2020 115 final.

[124] SWD 2020 115 final.

[125] SWD 2020 115 final.

[126] GDPR, rec. 103.

make that determination, the Commission's list of adequacy decisions can guide, i.e. are China, South Korea, or the U.S. listed among jurisdictions considered adequate?[127]

If not, then is there protection offed for personal data that can be compared to the level of protection offered in the EU? In other words, are there considerations for any of the safeguards mentioned in Chapter 2? What access do public authorities have to personal data with regards to national security and law enforcement purposes in the respective jurisdictions? Another relevant consideration is to ask if any of the mentioned countries offers domestic or relevant international commitments regarding privacy, although this will not be directly assessed herein.

In asking these questions, this analysis aims to assess whether there are GDPR safeguards in place considering the Brussel's Effect. It should be noted that this analysis is just a summary and that comparisons to the EU system will be assessed as a whole rather than in depth.

China

Adequacy and Comparative Level of Protection

China has been slower to develop a privacy regime, such as the one in the EU. As of September 2020, there is no adequacy decision in place between the EU and China. However, like many other countries, China has been modifying its privacy regime in recent years.

Being slow to develop its privacy framework gave China an opportunity to consider "legal transplantation" of other countries' or systems' rules and initial privacy considerations made it appear as if China may import EU framework by implementing a comprehensive law covering personal data of citizens.[128] However, it initially chose to take an approach similar to the sectoral approach exemplified by the U.S., with a patch work of laws offering limited protection.[129] The Chinese laws focus heavily on consumers and citizens do not enjoy the same protection.[130]

The Cybersecurity Law ("CSL") enacted in 2016 and entering into force in 2017, has a definition of personal data that is similar to that of the GDPR and the CSL's principles have

[127] "How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," Adequacy Decisions, accessed October 27, 2020, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[128] Emmanuel Pernot-Leplay, "'China's Approach' on Data Privacy Law: A Third Way Between the U.S. and the EU," *Penn State Journal of Law & International Affairs* 8, no. 1 (May 2020): 53.

[129] Pernot-Leplay, "China's Approach," 54 and 70.

[130] Pernot-Leplay, 54.

been improved to enhance privacy protection.[131] The CSL requires network operators collecting and using personal information to adhere to a number of important privacy principles, specifically legality, propriety, necessity, requiring consent be obtained from the person whose data is gathered, and that rules for collection and use be published while explicitly stating the purposes, means, and scope for use and collection.[132] However, the provisions suffer from vagueness and have required implementation of accompanying guidance text, some binding and others non-binding.[133]

With regards to personal data protection, the guidance is non-binding. However, it should be noted that the non-binding nature of the law arguably goes beyond other voluntary Western-style guidance because the regulator is to refer to the guidance as a "quasi-implementing rule" that serves as a "reference point," showing how the regulator is to view and consider data privacy.[134] While many of the GDPR safeguards listed in Chapter 2, such as enforcement through fines, appropriate technical and organizational measures, the use of risk assessments, and some basic principles of data protection, are exemplified in the CSL and accompanying guidance and specifications, it is a quite different and unique model that is difficult to compare to the EU framework.[135] Furthermore, from the EU perspective it arguably still suffers from major flaws.

Although one could discuss potential concerns regarding China's lack of a centralized data protection regulator, its difficulty reconciling the use of data for AI and privacy concerns, or its more relaxed use of implied consent in certain circumstances,[136] the main concern for this analysis is China's focus on cyber-sovereignty and surveillance of personal data by government officials. In fact, eight of the 10 most surveilled cities are in China, with one city, Chongqing, having approximately one CCTV camera per 5.9 citizens.[137] This and other big data surveillance methods are meant to keep citizens secure in the eyes of the government, but what is certainly at stake is their respective privacy.[138]

---

[131] Pernot-Leplay, 73.

[132] Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., November 6, 2016, effective June 1, 2017) art. 41, translated by New America https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. [hereinafter CSL]

[133] Pernot-Leplay, "China's Approach," 73.

[134] Pernot-Leplay, 75 quoting Barbara Li, Anna Gamvros, and Tom Wong's, *"China Data Privacy: New Guidance to Strengthen Protection of Personal Data*).

[135] Pernot-Leplay, 116, and CSL art. 17, 21, 26, 41, 66, and 68.

[136] Samm Sacks, et. al., "China's Emerging Data Privacy System and GDPR," *Center for Strategic & International Studies,* March 9, 2018. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

[137] Charlie Campbell, "'The Entire System is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World," *Time,* November 21, 2019, https://time-com.ezproxy.uio.no/5735411/china-surveillance-privacy-issues/.

[138] Note the discussion on the Chinese Social Credit System, which is relevant to this discussion but will not be presented in depth herein See Campbell, "The Entire System is Designed to Suppress Us."

The Chinese principle of cyber-sovereignty arguably allows China to perpetuate its ideas and values exclusively on the internet within its borders.[139] It is in opposition of a democratic and multi-stakeholder Internet construct and in concept would allow a country to ensure sovereignty over cyberspace with regards to Internet architectures, content, data flows, and to block foreign content for security purposes.[140]

Additionally, China has a data localization provision the extents of which[141] have not been seen in EU, U.S., or South Korea, specifically the requirement that certain data be stored locally and the prohibition, except in limited situations, of cross border transfers.[142] Specifically, Article 37 of the CSL, indicates that personal information gathered for critical information infrastructure or other important data collected during operations must be stored within China.[143]

However, the most interesting quality of the Chinese framework for purposes of this discussion is China's differentiation between protection of personal information by private entities and enhanced access to personal information by government officials.[144] While there are many laws, regulation, standards, best practices, and more that currently factor into an emerging Chinese privacy framework, there are still numerous laws on record "made for the purpose of state security, public security, censorship, and taxation" that allow the Chinese government to access information in a range of sectors.[145]

So, despite its recent adoption of EU-like framework, the protection of personal data and essential safeguards such as Privacy by Design[146] are undermined by potentially pervasive government access.[147] The government's control over information, censorship, and other concerns make an adequate assessment of such concept in a specific and useful manner rather difficult which is an important consideration when purchasing 5G equipment. Furthermore, China doesn't necessarily strive to fit within the EU privacy framework and many believe that China

---

[139] Pernot-Leplay, "China's Approach," 107.

[140] Pernot-Leplay, 108.

[141] See Yuxi Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous," *University of Washington Henry M. Jackson School of International Studies* (blog), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/ (noting that other jurisdictions have data localization requirements, but not as extensive as China's.

[142] CSL, art. 37.

[143] CSL, art. 37.

[144] Pernot-Leplay, "China's Approach," 107.

[145] Zhisheng Wang, "'Systematic Government Access' to Privacy-Sector Data in China," *International Data Privacy Law* 2, no. 4. (2012): 241. For example, Wang lists information, finance, trade, travel, and entertainment as some of the sectors where government access is extensive. See also Pernot-Leplay, "China's Approach," footnote 286 noting that "there is no restriction on the Chinese government's power to request companies to provide access to personal information without the need for a court order."

[146] See specifically examples regarding integrity and confidentiality in European Data Protection Board, *Guidelines 4/2019,* 23.

[147] Aljazeera, "In Land of Big Data, China Sets Individual Privacy Rights," *Aljazeera*, May 26, 2020, https://www.aljazeera.com/news/2020/05/26/in-land-of-big-data-china-sets-individual-privacy-rights/.

would like to see its privacy norms adopted externally[148] in a manner similar to the EU framework's global reach; this is sometimes referred to as the Beijing Effect.[149]

South Korea

Adequacy and Comparative Level of Protection

South Korea is an interesting jurisdiction to watch from a privacy perspective for several reasons. According to the South Korean Herald, South Korea is ranked number one in phone and Internet use worldwide, with nine in 10 Korean adults owning and using a smart phone.[150] Internet speeds are also among the fastest in the world.[151] As such, South Korea was an early adopter of certain Internet services and regulation, some of which have privacy implications.[152] What's notable is that as a democracy younger than a quarter century, formerly engaged in strong state surveillance, its privacy law takes place in the context of post-authoritarian leadership. [153] Furthermore, its response to the recent COVID-19 pandemic has seen success through the compilation of electronic transaction data,[154] mobile phone location logs, and surveillance camera footage of citizens.[155] By aggregating the information, Korean health officials have been able to provide extremely in depth contract tracing and is providing information to its society that would arguably comprise personal data in the eyes of the EU – because in the aggregate it is potentially identifiable.[156] Although it is important to consider the use of this data is in the context of a public health crisis, the access and acceptance of this method warrants further contemplation.

However, in June 2020, the Commission published a Working Staff Document to accompany its GDPR implementation report.[157] In the accompanying document, it noted that the adequacy process was at an advanced stage with South Korea and credited recent legislation

---

[148] Jeffrey Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *New America*, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

[149] Bradford, "The Brussels Effect," 25.

[150] Sohn Ji-young, "Korea No. 1 Worldwide in Smartphone Ownership, Internet Penetration," *The Korea Herald,* June 24, 2018.

[151] Greenleaf, *Asian Data Privacy Law,* 124.

[152] Greenleaf, *124*.

[153] Greenleaf, 125.

[154] Note that even before COVID-19, the Korean government collected substantial transaction data for investigating tax fraud. This data was retroactive. Justin Fendos, "How "Surveillance Technology' Powered South Korea's COVID-19 Response," *Brookings*, April 29, 2020, https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/.

[155] Fendos, "Surveillance Technology."

[156] Fendos, explaining that patients are identified by nymber, but detailed information about their location and timeframes in addition to surveillance footage is used to inform the public of potential risk of exposure.

[157] SWD 2020 115 final.

leading to the "establishment of an independent data protection authority equipped with strong enforcement powers" as progressing the dialogue. So, while at the present time there is not an adequacy decision in place, it appears as if this could be in the EU-South Korean future. With that in mind, what if any GDPR-like measures and safeguards are in place to offer a comparative level of protection.

According to some experts, South Korean data protection principles are among the strongest in Asia.[158] South Korea's data privacy framework initially failed to meaningfully limit data collection by its government and additionally didn't bear strong enforcement mechanisms.[159] However, privacy is constructed as a fundamental right established in South Koreas constitution,[160] and in recent years the regime has been updated with other meaningful changes. Revised in 2011, South Korea's Personal Information Privacy Act ("PIPA") is a culmination of its development of data privacy in both the public and private sectors over the last few decades.[161] PIPA is comprehensive law (with the exception of some specific privacy acts taking precedence), covers both the private and public sectors, and contains principles, common criteria, and enforcement mechanisms. [162]

On its face, South Koreas privacy framework exemplifies an approach like that of the EU. Similarities includes PIPA's definition of personal information which is similar to the EU in that it contemplates combinations of non-identifying information used in combination to identify a living person as personal information.[163] Recent amendments have distinguished pseudonymized and anonymous data from the scope of the definition of personal information, similar to the GDPR.[164] In addition, it includes several EU principles, such as minimal collection, deletion, direct marketing limitations, and sensitive data protection.[165]

Furthermore, the nation seems to have gained momentum currently regarding making changes to align with EU privacy in the areas of Privacy by Design and enforcement. For example, as recent as February 2020, the Korean Internet, and Security Agency ("KISA") issued guidelines on automated processing, IoT, and Privacy by Design suggesting privacy threats

---

[158] Graham Greenleaf and Whon-il Park, "'South Korea's Innovations' in Data Privacy Principles: Asian Comparisons," *The Computer Law and Security* Report 30, no. 5 (2014): 492.

[159] Greenleaf and Park, "South Korea's Innovations," 493.

[160] The Constitution of the Republic of Korea, last amended October 29, 1987, art. 16, 17, and 18 (S. Kor.). translated by WIPO https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr061en.pdf.

[161] Greenleaf and Park, "South Korea's Innovations," 493.

[162] Greenleaf and Park, 495.

[163] Personal Information Protection Act, art. 2 (S. Kor.), translated in Korea Internet & Security Agency https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3.

[164] Chris Kang, Sun Hee Kim, and Doil Son, "South Korea: Korea Introduces Major 'Amendments' to Data Privacy Laws," *Mondaq,* March 2, 2020, https://www.mondaq.com/privacy-protection/898830/korea-introduces-major-amendments-to-data-privacy-laws#:~:text=On%209%20January%202020%2C%20the,Act')%20and%20the%20Act%20on.

[165] Greenleaf and Park, "South Korea's Innovations," 504. Note that as of 2014 South Korea had not implemented data export restrictions, automated processing controls, or prior checking.

should be considered in advance rather than after infringement occurs.[166] However, there is still a concern over specific acts, such as the Act on the Promotion of Information and Communication Network Utilization and Information Protection ("Network Act") and the Act on the Use and Protection of Credit Information ("Credit Information Act") continuing to govern sector-specific information in a lax manner.[167] It remains to be seen and verified whether the recent amendments[168] on three significant data protection laws will have an effect on the EU-South Korean adequacy discussion.

United States

Adequacy and Comparative Level of Protection

Up until July 16, 2020 the United States and EU had an adequacy decision in place. However, the U.S. finds itself in familiar territory again with the invalidation of its adequacy decision. This time the mechanism, known as Privacy Shield, was invalidated by the CJEU in a long-awaited judgment of the *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (Schrems II) case.[169] At the crux of the decision was a concern over U.S. surveillance decisions not being limited to what is strictly necessary and proportionate as required by EU law,[170] and a lack of judicial redress and effective remedy for EU data subjects regarding the surveillance, as required by EU law.[171] Without and adequacy decision in place, an assessment of the U.S. privacy framework might shed some light on whether there are GDPR-like measures and safeguards in place offering a comparative level of protection for personal data to that seen in the EU.

Although privacy is not mentioned in the U.S. constitution, the concept of privacy in some form or another has existed in the U.S for some time.[172] For example, emergence of federal privacy laws can be seen in the 70s with the introduction of the Fair Credit Reporting Act of 1970 and the Privacy Act of 1974, and in the decades since a patch work of broader framework principles, sectoral and state privacy laws, and case law has emerged although it is highly context dependent. [173]

---

[166] KISA, "Personal Information Protection Should Be Applied from the Planning Stages of IoT Service."

[167] Ko, et. al., "Structure and Enforcement of Data Privacy Law in South Korea," 101.

[168] Kang, Kim, and Son, "Amendments."

[169] Schrems II.

[170] Charter of Fundamental Rights of the European Union, December 12, 2007, O.J. (C 303), art. 52 [hereinafter CFR]. See Also Caitlin Fennessy, "The 'Schrems II' Decision: EU-US Data Transfers in Question," *International Association of Privacy Professionals*, July 16, 2020, https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[171] See art. 47 of the CFR.

[172] Bygrave, *Data Privacy Law*, 99.

[173] Bygrave, 99 and 110.

It should be noted from the outset that there is tension between the U.S. and the EU regarding privacy. Partially to blame is a policy position by the U.S. to continue to shape the online world in continuation of its initial grip over the Internet's development and its hand in setting those standards as well as its tendency to "afford market mechanisms greater latitude in setting data privacy standards" than EU law.[174] However, up until recently it has seemed as if the U.S. and the EU also share values considered important in EU privacy framework such as upholding of civil liberties and democratic ideals.[175]

More specifically, the GDPR measures and safeguards that can be said to be exemplified in U.S. law are somewhat in existence. While it could be fruitful to dig into specific sectoral laws[176] embodying GDPR-like measures or safeguards, the law that is most relevant to this discussion is the California Consumer Privacy Act (CCPA). As one of the largest economies in the world,[177] and one in which other state businesses hope to operate within the recent privacy changes in California are seen by some as likely to nudge the U.S. in the direction of stricter privacy. As California begins to enforce the CCPA it is assumed that businesses in other U.S. states, or otherwise within the scope of the law, will potentially begin to adhere to the framework.

The provisions within CCPA that are like the GDPR are certain definitions**,** protections for those under the age of 16, and the right of access to personal information.[178] For example personal information is defined broadly under the CCPA, although not as broadly as the GDPR.[179] Additionally, "aggregate consumer information" and "deidentified data" are excluded from the CCPA like anonymous information is excluded from the scope of the GDPR.[180] Medical data covered by other U.S. legal frameworks and personal information processed by credit reporting agencies is not within the scope.[181] In addition, although it is not as strong as the GDPR's provisions there are some accountability-related requirements regarding training staff[182] to deal with consumer requests.[183] Regarding penalties and enforcement, there is an administrative remedies for non-compliance but actions must be brought by California's

---

[174] Bygrave, 107.

[175] Bygrave, 107.

[176] Pernot-Leplay, "China's Approach," 59-60 discussing generally the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act, the 1996 Health Insurance Portability and Accountability Act, etc.

[177] Kieran Corcoran, "California's Economy is Now the 5th-biggest in the World," *Business Insider*, May 5, 2018, https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5?r=US&IR=T.

[178] Alice Marini, et. al., "Comparing Privacy Laws: 'GDPR v. CCPA,'" *Future of Privacy Forum,* December 18, 2019: 5. https://fpf.org/2019/12/18/comparing-privacy-laws-gdpr-v-ccpa/.

[179] Marini, et. al., "GDPR v. CCPA," 13.

[180] Cal. Civ. Code §1798.140(e), (o),(t),(q), §1798.145, and Marini, et. al., "GDPR v. CCPA," 9.

[181] Cal. Civ. Code §1798.140(o)(1) and (2), and Marini, et. al., "GDPR v. CCPA," 5.

[182] Cal. Civ. Code §1798.130.

[183] Marini, et. al., "GDPR v. CCPA," 5.

Attorney General and given the infancy of the law the effects are still being measured.[184] There is also the potential for civil remedies for individuals through the court system, but they only pertain to failure of security measures and data breaches, not the entire law.[185] As a whole, the CCPA significantly strengthens privacy protections, however it is perhaps wrongly dubbed a GDPR-equivalent and its scope and protections are much weaker than the EU standard. One last important note is that California has placed a new privacy law as a ballot initiative which will be voted on in the upcoming 2020 election.[186] So there is potential on the horizon for more EU-U.S. privacy alignment.

Summary of Comparative Findings

After examining the privacy and data protection framework in place in China, South Korea, and the United states it is evident that the GDPR safeguards are not adequately in place in the respective jurisdictions. We may debate subjectively which of the three systems is the 'safest,' but the bottom line is that none are adequate per the GDPR. None of them have an adequacy decision in place, even though they may have existed in the past or are close or a possible option for the future. Thus, the GDPR is insufficient in assisting Member States' decisions on the question of which major non-EU 5G equipment supplier can provide 'safe' equipment from a privacy and data protection perspective. The companies within China, South Korea, and the United States will have to adhere to the national laws in their corresponding nations and therefore will be unable to reliably provide the level of protection required by the EU framework. With that in mind, what will help Member States in making their decisions moving forward? The following chapter will look at the NIS Directive as well as work of ENISA and the NIS Cooperation Group to see if it aids in assisting Member States. Additionally, it will briefly explore the geopolitical, economic realities, and market consideration to determine if the legal framework is adequate when assisting Member States.

Chapter 4: Cybersecurity and The Supply Chain

Before diving into the work of ENISA and the NIS Cooperation Group, it is again important to acknowledge that the EU is merely being used as an example in this analysis. This is a global issue, and the EU is merely an interesting example because of its international landscape and the varying level of expertise of each Member State.

With that in mind, the analysis will shift gears and go beyond the GDPR because it cannot, in this scenario, alone assist Member States in purchasing 5G equipment. From a legal

[184] Cal. Civ. Code §1798.155.

[185] Cal. Civ. Code §1798.150.

[186] See proposed measure "The California Privacy Rights Act of 2020."

perspective, there are many other directives, recommendations, and guidance as introduced in Chapter 1 that may be helpful, and it cannot be underestimated that many issues factor into these decisions. Cybersecurity and supply chain issues offer a view into challenges presented by 5G. The cybersecurity concepts will be described in the proceeding sections, but first for context, supply chain concepts are introduced.

Supply Chain Concepts

Among the important concepts related to a discussion of supply chain and 5G are supply chain management ("SCM") and supply chain integration ("SCI").[187] Without meaning to enter the debate regarding the definition of SCM, a consensus definition offered by some scholars is:

> "the management of a network of relationships within a firm and between interdependent organizations and business units consisting of material suppliers, purchasing, production facilities, logistics, marketing, and related systems that facilitate the forward and reverse flow of materials, services, finances and information from the original producer to final customer."[188]

Also, relevant to the discussion is SCI, which is defined as:

> "collaborative inter- and intra-organisational management on the strategic, tactical and operational business processes to achieve effective and efficient flows of products, information and funds to provide the maximum value to the end customer at the lowest cost and greatest speed."[189]

These definitions are important due to the complexity of the 5G network and all the actors and stakeholders involved. The planning, sourcing, making, delivery, returning, and enabling[190] of the technology are all critical to a secure supply chain in 5G and will require careful consideration by all involved, including Member States in their acquisition of equipment. In the case of 5G, decision should be made beyond merely economics, due to the necessity of securing the network. If 5G is being operated in critical functions of society, the most efficient and cheapest technology might not be 'best'. Beyond the market and supply chain, the discussion requires Member States assess technical and strategic considerations.

---

[187] Taboada and Shee, "Understanding 5G," 2.

[188] James Stock and Stefanie Boyer, "Developing a Consensus Definition of Supply Chain Management: A Qualitative Study," *International Journal of Physical Distribution & Logistics Management* 39, no. 8 (2009): 706.

[189] Tharaka De Vass, Himanshu Shee, and Shah Miah, "The Effect of Internet of Things on Supply Chain Integration and Performance: An Organisational Capability Perspective," *AJIS. Australasian Journal of Information Systems* 22 (2018): 2.

[190] Taboada and Shee, "Understanding 5G," 4 (referencing APICS).

To begin, highlights from the NIS Cooperation Group and ENISA recommendations will be examined to determine if they provide meaningful assistance relevant to assessing equipment purchase. Then, additional framework and its respective conclusions will be introduced followed by a report on the progress of implementation. Next, the analysis will examine some Member States' realities in hopes of getting a closer view into geopolitical, supply chain, and market issues and considerations. The goal is to provide a window into the reality of what is occurring to offer a critical assessment on the functioning of the framework and a suggestion for a way forward. Again, note that this is a cursory examination of the issue and this analysis should be treated as such.

NIS Cooperation Group and ENISA

At the heart of the discussion are two issues, not always mutually exclusive, privacy, as already discussed, and cybersecurity. Although there are many definitions of cybersecurity used around the world, it is generally agreed that the security-related concepts center around the "CIA triad" of confidentiality, integrity, and availability.[191] Two of the entities currently working to assist Member States on the issue of cybersecurity specifically as it relates to 5G technology are the NIS Cooperation Group and ENISA.[192] To specifically address cybersecurity, cyber threats, and general issues surrounding the CIA triad as they relate to 5G, Member States can look to the work of these entities.[193] However, at issue is the sufficiency of these entities to guide Member State decisions on the purchase of 5G equipment.

In the Coordinated Risk Assessment, the NIS Cooperation Group identified main threats and threat actors, indicating that a shift in the security paradigm is necessary moving forward into the transition to 5G.[194] Some of the relevant findings included the concern over an increased use of software and third-party suppliers and how resulting dependencies for critical societal functions is a concern for not only the threat landscape, but the supply chain.[195] Furthermore, and in consideration of the CIA triad, there are concerns about non-EU or state-backed actors potentially exploiting the new network and this concern is exacerbated by the complexity and number of stakeholders involved. [196] To address this concern, the work will be ongoing and should consider not only the supply chain and purchase of network equipment but also the

---

[191] ENISA, *Threat Landscape*, 47.

[192] Note that although the Body of European Regulators for Electronic Communications (BEREC) is relevant to this analysis, it will not be discussed because the guidance by ENISA and the NIS Cooperation Group is sufficient for purposes of this analysis.

[193] Also, note that the certification of IT products and services found in the EU Cybersecurity Act, while voluntary, should be monitored for further development.

[194] NIS Cooperation Group, *Coordinated Risk Assessment*, 32.

[195] NIS Cooperation Group, 31-32.

[196] NIS Cooperation Group, 32.

dependency on suppliers and consideration of supplier risk profiles.[197] The risk assessment suggested, inter alia, identifying gaps in laws and frameworks to address discovered risks and issues, increasing regulatory capacity, and focusing on technical standards development.[198]

To follow up on the Coordinated Risk Assessment, the NIS Cooperation Group with the support of ENISA and the Commission, published the first iteration of the 5G Toolbox. In Table 4, it presents steps Member States can follow when using the Toolbox.[199] Honing in on many of the same issues identified in the Coordinated Risk Assessment, the Toolbox provides a set of key actions for Member States to address these issues. To compliment the Toolbox, ENISA published a threat assessment for the fifth generation of mobile telecommunications networks ("Threat Landscape") which details the technical aspects of the networks and the threats pertaining to the specific aspects of the 5G network that may inform more directly as Member States move forward in building their networks. The Commission followed up with a communication endorsing the measures in the Toolbox and calling on Member States to take first steps to implement the measures.[200] Member State progress was then assessed in the Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity ("Progress Report"), published July of 2020.[201]

The Progress Report followed up on Member State's implementation of the strategic measures ("SM") and technical measures ("TM") identified in the Toolbox[202] that relate back to risks identified in the Coordinated Risk Assessment.[203] In a nutshell, it recommended Member States implement the following "highest effectiveness measures": (1) strengthening regulatory capacity, [204] (2) assessing risk profiles of supplies and proceeding accordingly regarding those that are high risk, especially as it relates to critical and sensitive assets, [205] (3) avoiding dependency on single suppliers, especially high-risk suppliers, [206] (4) diversifying the 5G supply chain to keep it sustainable and not dependent on single and/or high-risk suppliers, [207] and (5) ensure strong security requirements in the 5G environment. [208] The Progress Report also determined that Member States have many remaining concerns, but for purposes of this

[197] NIS Cooperation Group, 22, and 32.

[198] NIS Cooperation Group, 31-33.

[199] NIS Cooperation Group, *EU Toolbox,* 17.

[200] NIS Cooperation Group, *Report on Progress.*

[201] NIS Cooperation Group, *EU Toolbox.*

[202] See Table 1 in NIS Cooperation Group, *Report on Progress*, 6.

[203] NIS Cooperation Group, *Coordinated Risk Assessment*, 24-29. See also Table 1 Risk categories and scenarios in the NIS Cooperation Group, *EU Toolbox*, 5.

[204] See SM 01 and 02 from Table 1 in the NIS Cooperation Group, *Report on Progress*, 6-7.

[205] See SM 03 and 04 from Table 1 in NIS Cooperation Group, 6, footnote 7, and page 7.

[206] See SM 05 and 06 from Table 1 in NIS Cooperation Group, 6-7.

[207] See SM 07 from Table 1 in NIS Cooperation Group, 6-7.

[208] See TM 01 to 08 and 11 from Table 1 in NIS Cooperation Group, 6-7.

discussion the remaining concerns surround state interference in the 5G supply chain, [209] a general lack of diversity in Member State networks, and dependency on particular suppliers.[210]

The earlier discussion surrounding privacy is also highly relevant to these issues. Although privacy is sometimes viewed as a separate piece of the puzzle, it is highly relevant in the security context, is seen in the Coordinated Risk Assessment's mention of data protection agreements, and in consideration of all the parties involved, many of which will potentially be controllers and processors either now or at some time in the future. The extent to which the respective parties can ensure proper GDPR safeguards, security will be enhanced. However, if safeguards are lacking – for example, where governments are allowed access to EU data subjects' personal data, where seemingly anonymous data is used in the aggregate, or if the basic principles of data protection are not built into the hardware and architecture of the equipment (Privacy by Design), there are accompanying risks.

Given all the above-mentioned concerns, it is relevant to consider more specifically some of the issues and risks listed among the above-mentioned framework as they are intimately related to Member State purchase of equipment. Specifically, the determination of risk profiles of suppliers, threats posed by States or State-backed actors, and supply chain considerations.

Risk Profiles

A risk profile determines how risky it is to purchase equipment from a particular supplier. According to the Coordinated Risk Assessment, the risk profile can be assessed based on various factors, including likelihood of a non-EU actor interfering with the supplier, a link between a particular supplier and a government, legislation in the supplier's country, specifically whether there are democratic checks or data protection agreements, the composition of corporate ownership of the supplier, suppliers' abilities to assure supply, government influence on manufacturing and other aspects, and the quality of the suppliers' products including consideration of cybersecurity and the supply chain of the respective parts.[211] An additional consideration may be notices issued by EU authorities or Member State national authorities.[212]

Threats Posed by States or State-backed Actors

[209] Note that the Report on Member States' Progress found State interference through the 5G supply chain to be the most relevant and least mitigated, 8.

[210] NIS Cooperation Group, *Report on Progress*, 7-8.

[211] NIS Cooperation Group, *Coordinated Risk Assessment*, 22-23.

[212] NIS Cooperation Group, 23.

The potential threats for the 5G network are many[213] and include threats posed by States or State-backed Actors. To guide the determination of relevance, the Coordinated Risk Assessment suggested consideration of two parameters: (1) resources – considering the capabilities of a State or State-backed actor, and (2) motivation – intent or reasons for potentially attempting attacks on the 5G network.[214] Of particular relevance, the Coordinated Risk Assessment mentions nations with cyber offensive initiatives,[215] insiders or subcontractors, or potential for motivations of IP theft or cyber terrorism.[216] Some of which will be explored further herein.

Supply Chain Security and the Reality of Member States Decisions

Returning to the assessment criteria presented in the first chapter - technical, strategic and market considerations - we see the Commission's Recommendation and analysis in this chapter drawn from the work of the NIS Cooperation Group and ENISA has the potential to significantly assist in the pursuit of a more secure 5G network. However, the difficulty lies in the geopolitical, supply chain, and market considerations. With Member States having different priorities relating to those categories there is a risk of fragmentation of the EU's joint approach and the risk of decoupling[217] or the bifurcation[218] of the 5G network. This potential divide, resulting in part from tension caused by a trade war between China and the U.S., places Member States squarely in the middle of the battle field.[219] So how can the framework described above help, and what is the political and economic reality in various Member States?

We see the framework being implemented in various ways and at various stages of maturity. Exemplifying many of the posed risks like national security concerns, supply chain considerations, security or risk based concerns, threats posed by States or non-EU State-backed actors, and others, Estonia, France, Italy, and Sweden have implemented various pre-authorizations or conditions for the approval of suppliers, hardware, or software in various parts of the network.[220] In Estonia and Sweden, conditions come in the form of amendments to their respective Electronic Communications Acts, with the former giving the government the power to

---

[213] See specific mentions of, among other things, disruption, spying on traffic or data, modification or rerouting, and destruction or alteration in NIS Cooperation Group, *Coordinated Risk Assessment,* 12.

[214] NIS Cooperation Group, *Coordinated Risk Assessment*, 13.

[215] The discussion on cyber offensive strategies and capabilities, although relevant to this discussion will not be discussed in depth. However, it should be noted that China and the United States are each advertising cyber offensive capabilities (see Max Smeets and Herber Lin, "Offensive Cyber Capabilities: To What Ends?" *NATO CCD COE Publications*, 10th International Conference on Cyber Conflict (2018): 56.), whereas South Korea, perhaps strategically, is not advertising cyber offensive capabilities. Perhaps this contributes to the ability of South Korea to continue discussion with the Commission on a potential adequacy decision.

[216] NIS Cooperation Group, *Coordinated Risk Assessment,* 14.

[217] Rühlig and Björk, "Huawei Debate," 22.

[218] Eurasia Group, "'White Paper': The Geopolitics of 5G," *Eurasia Group* (November 2018): 4.

[219] Rühlig and Björk, "Huawei Debate," 25.

[220] See generally NIS Cooperation Group, *Report on Progress*.

impose obligations, which will be regulated through secondary legislation, requiring application for the use of communications network hardware and software to guarantee national security, and the latter requiring permission to use radio transmitters only if they will not cause harm to national security.[221] In France, a new law requires prior authorization from the Prime Minister before rolling out or operating sensitive 5G or future generation networks. The restriction, prohibition, or imposed requirements or conditions can be related to the supply, deployment, and operation of 5G equipment.[222] Under Italy's Golden Power law, the government receives a notification when an extra-EU supplier is potentially to be used by MNOs and an inter-ministerial Coordination Group advises the Government on a potential veto of the contract based on technical analysis or imposition of SM.[223]

Technical Measures, Strategic Considerations, and the Market

Although it is difficult to put Member State actions squarely within the realm of one specific category of the assessment criteria, technical concerns are being considered by Member States in various ways. Leading the charge, at least in reporting to the NIS Cooperation Group, is Austria who has implemented a number of measures under its Telecom Network Security Regulation, specifically the requirement for MNOs to comply with ISO/IEC 27001 information security practices, 3GPP standards, and ENISA's recommendation on Security Aspects of Virtualization.[224] The strategy of security and implementation of technical consideration is seen by many experts and scholars as among the most important aspects since, as we'll see in the proceeding analysis that strategic and market considerations are where the more complicated and potentially intangible issues arise.[225]

Strategic considerations being implemented by Member States include, inter alia, maintaining a diverse network, i.e. a network that is as "open and inclusive" as possible and focused on technology implementing technological standards preferably developed from open sources.[226] Diversity is thought to encourage vendors to participate to prevent reliance on any one supplier with the idea being different vendors and suppliers aren't likely to face the same issues at a

---

[221] NIS Cooperation Group, *Report on Progress*, 12.

[222] See reference to The Law N 2019-810 of 1st of August 2019 in NIS Cooperation Group, *Report on Progress*, 12.

[223] NIS Cooperation Group, *Report on Progress*, 18.

[224] NIS Cooperation Group, 13, 30, and 33.

[225] See discussion on the importance of encryption and network security in Rühlig and Björk, "Huawei Debate," 29. See also discussion on key security challenges in 5G in Ahmad et. al., "Overview of 5G Security," 37. See also the conclusion on the landscape of 5G network security threats in Khan, et. al., "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials* 22, no. 1: 239-240.

[226] Rühlig and Björk, "Huawei Debate," 27.

given time.[227] This approach potentially alleviates dependency concerns, increase resilience, and avoids single points of failure,[228] which are a strategic consideration intimately related to diversity.

In fact, dependency is a concern for many reasons, such as interoperability,[229] concerns over security, potential for the use or abuse of political leverage, and more. For example, if a Member State wants to switch or diversify suppliers and has implemented a supplier in a legacy network not adhering to broader or globally embraced technological standards. As already mentioned, the build out of the 5G NSA relies on the existing infrastructure of the 4G network. Currently, 4G equipment from Huawei and ZTE is a large percentage of many Member States' networks[230] and this is potentially a concern with these companies being considered a security risk by some[231] as well as a threat to the supply chain[232] as well as the concern that China could require political concessions from Europe based on market position of its suppliers in Member States networks.[233] An example of this issue is in Germany, where 60% of the network is dependent on Huawei.[234] Despite technical experts' concern over the supply chain security of Huawei equipment,[235] the dependency is difficult to address due to, among other reasons, the trade relationship between German automakers and China.[236] On the flip side, the Czech Republic with a dependence on Huawei mobile infrastructure in the 80-90% range, received a security warning from its National Cyber and Information Security Agency ("Nukib") and was thought to be

---

[227] Rühlig and Björk, 15.

[228] NIS Cooperation Group, *Coordinated Risk Assessment*, 15.

[229] NIS Cooperation Group, 23.

[230] See discussion showing dependence on Huawei mobile infrastructure to be 80-90% in Belgium and Czech Republic, 60% in Germany and Poland, 50-60% in the United Kingdom, 50% in Denmark, and 30% in France in Rühlig and Björk, "Huawei Debate," 23.

[231] See discussion on the Czech government's cybersecurity agency's directive warning that Huawei and ZTE potentially pose a threat to national security, https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html.

[232] See discussion on the U.S. restrictions affecting the supply chain security of Czech 5G technology in Marc Santora and Hana de Goeij, "Huawei Was a 'Czech Favorite' Now? It's a National Security Threat," *New York* Times, February 12, 2019, https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html. See also, National Cyber Security Centre in Response to US Sanctions, "Huawei to be Removed from UK 5G Networks by 2027," press release, July 14, 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027. See also Patrick Donahue, "Merkel Resists Full Ban on Huawei, Making Germany an Outlier," *Bloomberg*, September 23, 2020, https://www.bnnbloomberg.ca/merkel-resists-full-ban-on-huawei-making-germany-an-outlier-1.1498030, reference to security hawks in Berlin.

[233] Rühlig and Björk, "Huawei Debate," 23.

[234] Rühlig and Björk, 23.

[235] Rühlig and Björk, 27.

[236] Katrin Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts:' Automakers," *New York Times*, January 16, 2020, https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html. See also Dragne & Asociatii, "Germany and Austria: Forerunners of 5G Security Measures?" *Lexology*, July 1, 2020, https://www.lexology.com/library/detail.aspx?g=2719d29a-30e5-458d-8977-9e514c2eadce.

considering whether it should limit or ban the Chinese equipment, but this directive was met with threats of legal action as well as potential trade consequences by China.[237]

Note that it is also important to consider that theoritcally Europe is susceptible to the same kind of political leverage by other large markets it depends on for technology, such as the U.S.[238] and South Korea. Furthermore, dependency on products produced in the U.S., such as software[239] and the avoidance of involvement in patent wars "looming behind Trump's entity list"[240] encourage the quest for diversity of suppliers of 5G equipment and its accompanying components. Also, as current politics demonstrate, reliance on former partnerships can become tenuous at times.

Returning to the situation of the Czech Republic, and to emphasize the discussion in Chapter 3 emphasizing privacy risks presented by Chinese law's differentiation between privacy in the public and private sector, when the head of the Nukib, Dusan Navrátil, raised the alarm bells, he cited China's National Intelligence Law as among his concerns. Specifically, expressing that the law requires Chinese companies to "support, provide assistance and cooperate in the authoritarian nation's national intelligence work wherever they work."[241] The Nukib's directive was at odds with the President Zeman's views on Huawei and drove a wedge in the Czech government.[242] Prior to issuance of the directive, Huawei had for four years prior had a contract to fulfill the communication needs of the President and his staff.[243] Shortly thereafter, Navrátil was removed from his position as the Prime Minister expressing concern allegedly not related to the issuance of the directive, although outwardly it gives at least the appearance of impropriety. Despite the high quality of Chinese equipment being up for debate, the specific aspect that looms large is the link of between the Chinese government and Huawei and ZTE.[244] At any rate, this example demonstrates how economic, political, and security concerns can be at odds and additionally, the concern over China's potential to access personal data or other information through its National Intelligence Law. Note that there have also been concerns over U.S.[245] and

---

[237] Santora and de Goeji, "Czech Favorite."

[238] Rühlig and Björk, "Huawei Debate," 21.

[239] Rühlig and Björk, 22.

[240] Rühlig and Björk, *27.*

[241] Santora and de Goeji, "Czech Favorite."

[242] Santora and de Goeji.

[243] Santora and de Goeji.

[244] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *CFR,* August 6, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant, discussing China and the blurring between what is public and private.

[245] See the discussion on the Schrems II judgment as it relates to, inter alia, section 702 of the U.S. Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12333, and other U.S. laws, regulations, etc. that do not limit the access of the U.S. government to EU data subjects personal data to what is strictly necessaryin Kristina Irion, "Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law," *European Law Blog,* July 24, 2020, https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/.

South Korean surveillance.[246] However, do governance models or democratic checks offer an advantage for South Korea or the United States? Although, a deep dive into the analysis of governance models and democratic checks will be left for future analyses, and with the caveat that it is highly dependent on political systems, trade, and more, perhaps the 'safest' choice between the two is South Korea.

A discussion on market considerations would not be complete without a discussion of efficiency and cost. As patents and influence over standards influences how technology is used and how royalties flow, it is important to consider.[247] In late 2019, it was reported that Huawei was leading the charge, at least with declared patents and contributions to 5G technical standards.[248] Additionally, the use of its equipment will purportedly significantly lower the cost and speed up the implementation of 5G in the near term.[249] At times, Member States have found themselves at odds in a conundrum regarding whether cheapest is best and how this factors into other privacy, security, political, and trade concerns. For example, in Poland it was alleged that a ban of Huawei was pending when in September of 2019, Poland and the United States signed a joint declaration regarding trusted and reliable 5G suppliers. The declaration expressed the need for consideration of supplier control by a foreign government without independent judicial review, transparency of ownership structure, and record of ethical corporate behavior. [250] The alleged exclusion of Huawei from its network came after a Chinese Huawei employee and former Polish security official was arrested on spying allegations.[251] However, banning Huawei would have consequences as prices would increase and delays in implementation would be likely.[252]

In sum, Member States appear to be tackling the issue surrounding purchase of 5G equipment by considering the requirement of prior authorization of or the ability to veto the operation of certain suppliers in various parts of the market. Also, there seems to be momentum surrounding a requirement that purchased equipment come from suppliers complying with standards, such as ISO, 3GPP, etc. as well as making ENISA guidance on specific network aspects mandatory. Furthermore, there is a general emphasis on the need to consider technical and security related aspects a priority, to diversify the 5G-network to reduce dependencies and vendor lock-in, and to generally avoid situations where political leverage could become an issue. Finally, it

---

[246] See Fendos, "Surveillance Technology," discussing the pervasive use of individuals' "electronic transaction data, mobile phone location logs, and surveillance camera footage" during the COVID pandemic.

[247] IPlytics, "Who is Leading the 5G Patent Race?" *IPLYTICS*, November 2019, https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf.

[248] Eurasia Group, "White Paper," 8-9.

[249] Gwénaëlle Barzic, "Europe's 5G to Cost $62 Billion More if Chinese Vendors Banned: Telcos," *Reuters,* June 7, 2019, https://www.reuters.com/article/us-huawei-europe-gsma-idUSKCN1T80Y3.

[250] "U.S. – Poland Joint Declaration on 5G," Whitehouse.gov Foreign Policy, last modified September 5, 2019, https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

[251] Anna Koper and Joanna Plucinska, "'Poland' to Hold Off Blanket Ban on Huawei 5G Gear Due to Cost Concerns," *Reuters,* April 16, 2019, *https*://www.reuters.com/article/us-poland-huawei-idUSKCN1RS0QI.

[252] Koper and Plucinska, "Poland."

seems as if price while being an important consideration will become one element in the bigger picture – along with seeking out high quality equipment and ensuring a secure supply chain.

Summary of the Assessment

With the above-mentioned complexities explored, it is important to consider the general adequacy of the framework and explore where Member States should focus to ensure a sound decision. While the framework is helpful, there is more work to be done. There are issues specific to Member States which cannot be solved by the framework alone. Complex and interrelated decisions contemplating trade, politics, and existing infrastructure must be considered. Some scholars believe that due the Europe's overall vulnerability it's a positive development that EU Member States delegated the process of coordination to the Commission,[253] because the purchase of safe equipment for the EU is perhaps a different question than the safe purchase of 5G equipment for respective Member States. Moving forward towards a coordinated approach and with a focus on standards development is prudent because there is power in the in the EU's combined market position.

Chapter 5: Conclusion

Summary of the Analysis

This analysis examined the transition to 5G, how the new networks will be constructed, who the global stakeholders are, and some of the security and vulnerabilities of the new network. It used EU Member States purchase of 5G technology from China, South Korea, and the United States as an experimental field to assess whether the GDPR could adequately assist Member States in determining a safe option. Beyond that, the EU cybersecurity framework, specifically that of ENISA and the NIS Cooperation Group was introduced to assess whether the additional guidance could assist Member States.

First and foremost, the analysis discovered that the challenges and issues surrounding safe 5G purchase are many. The overall security of the 5G network can be compromised by many things, including vulnerabilities resulting from the deficient processes of any other security stakeholder.[254] This concern is exacerbated by the complicity of the network given all the components involved, the shift to "softwarization" and "cloudification,"[255] as well as other issues identified and already occurring in the 4G network, such as human errors and errors in

[253] Rühlig and Björk, "Huawei Debate," 25.

[254] NIS Cooperation Group, *Coordinated Risk Assessment*, 19-20.

[255] Taboada and Shee, "Understanding 5G," 3.

process.[256] Additionally, there is potential for malicious or state-backed interference in the network,[257] Industry 4.0, IoT, and the fact that the network at times supports the functioning and operation of sensitive and critical aspects of society requiring a commitment to ensuring the best process possible. With lack of trained and specialized experts, capacity building and arguably cooperation will be indispensable qualities of the long-term success of the network, even after a 'safe purchase' is made.

Second, the GDPR cannot alone adequately assist Member States in determining a safe option because privacy in isolation is not sufficient and one could argue that the Brussels Effect hasn't yet spread sufficiently throughout the legislative framework of the non-EU jurisdictions selling 5G equipment.

Although many GDPR safeguards could assist greatly in theory, like the principles in Chapter II, the risk-based approach and consideration for the rights and freedoms of data subjects, Privacy by Design, security by design, and the requirement that controllers and processers remain accountable for compliance or risk large fines, surveillance and access by public officials and non-EU governments is still an undermining factor. Furthermore, the lack of adequacy decisions in the respective jurisdictions speaks for itself. Although the U.S. used to have an adequacy decision in place, this has been recently upended by the decision in Schrems II.[258] This case expressed concerns regarding a lack of restrictions regarding government access to EU data subjects personal data as well as a lack of proper remedy,[259] so to the extent there has been progress with new privacy frameworks (for example, the CCPA[260] or CPRA[261]), these issues still remain. Like the U.S., and of the greatest concern in China is its National Intelligence Laws that potentially allow the government significant access to information which could be personal data of EU data subjects.[262] It seems as if South Korea may have the best privacy framework in place, and it is at an advanced stage in adequacy discussion with the Commission. However, it remains to be seen its privacy framework will continue to show remnants of an authoritarian surveillance states, as exemplified by their COVID-19 response.[263]

Third, since privacy in isolation was not enough to inform a safe purchase decision, the analysis looked beyond the GDPR and ventured into the extensive cybersecurity framework of the NIS Directive, ENISA, and the NIS Cooperation Group, and quickly mentioned the Cybersecurity Act. The fact that the Cybersecurity Act's ICT certification may become mandatory in

---

[256] ENISA, *Security Incidents*, 14.

[257] The NIS Cooperation Group identified "state interference through 5G supply chain as being both the most relevant and least mitigated" by EU Member States in NIS Cooperation Group, *Report on Progress*, 8.

[258] Schrems II.

[259] Fennessy, "Schrems II."

[260] Cal. Civ. Code §§1798.100-1798.199.

[261] The proposed California Privacy Rights Act of 2020.

[262] Wang, "Systematic Government Access," 222.

[263] Fendos, "Surveillance Technology."

the future doesn't help Member States in the present moment. However, the remaining cybersecurity framework stemming from the Act's creation of ENISA and its subsequent work as well as the work of the NIS Cooperation Group, is potentially helpful. There is still a lot of work to be done, but Member States can use the work of ENISA to address concerns in specific aspects of the network,[264] as well as the work of the NIS Cooperation Group specifically the Coordinated Risk Assessment, and the Toolbox to address risks and vulnerabilities and especially to work towards building capacity and regulatory framework in areas of deficiency, and coordinating to the extent possible.

However, serious issues exist, and they currently hinder a verifiably safe option for purchase. For example, existing dependencies on a particular supplier make decision based on security or privacy difficult, as the situations in Germany and Czech Republic show. This also makes diversity of the network a difficult feat. At this juncture, these decisions are largely political decisions of the respective Member States. Furthermore, the current global political tensions make decisions particularly difficult and lead to concerns over a secure supply chain and ultimately interoperability and the creations of standards.

A Way Forward: Privacy Leads Member States One Way, While Cybersecurity Leads to Another

From strictly a privacy perspective, the safest option may be to stay local – in other words to purchase from EU companies. However, this also presents its own issues, such as single points of failure, availability of equipment, and generally a lack of diversity as recommended by the Coordinated Risk Assessment.

The next safest choice based on the privacy analysis, would arguably be South Korea due to its current privacy framework and the fact that it is at an advanced stage in a potential adequacy decision.[265] Recently, it created an independent data protection authority with strong enforcement power,[266] and KISA issued guidelines on automated processing, IoT, and an emphasis on Privacy by Design.[267] Its data protection principles are among the strongest in Asia,[268] and privacy is constructed as a fundamental right per the South Korean Constitution.[269] The

---

[264] See Annex C: Mapping Risk Scenarios to Cyberthreats in ENISA, *Threat Landscape*.

[265] SWD 2020 115 final.

[266] SWD 2020 115 final.

[267] KISA Press Release, "Personal Information Protection Should Be Applied from the Planning Stages of IoT Service," February 19, 2020, https://www.kisa.or.kr/notice/press_View.jsp?cPage=1&mode=view&p_No=8&b_No=8&d_No=1884&ST=&SV=.

[267] "U.S. – Poland Joint Declaration on 5G," Whitehouse.gov Foreign Policy, last modified September 5, 2019, https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

[268] Greenleaf and Park, "South Korea's Innovations," 492.

[269] The Constitution of the Republic of Korea, last amended October 29, 1987, art. 16, 17, and 18 (S. Kor.), translated by WIPO at https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr061en.pdf.

PIPA is comprehensive act, and with some exceptions, covers both the private and public sectors.[270] However, the caveat is there is evidence of remnants of the ability to use data to surveil, as evidenced by the recent pandemic and the use of the Network Act and the Credit Information Act.[271] So, it remains to be seen if South Korea will use its fast internet speeds and early innovation to stay on a path that is in line with the EU legal privacy framework.

Furthermore, a purchase from exclusively one or two nations, and based exclusively on privacy concerns alone, contradicts the EU Coordinated Risk Assessments mitigation measure of diversity in the 5G network. Diversity of the 5G network is important for many reasons, and although it is not devoid of disadvantages, such as slowing implementation, a potential increase in cost in the near term,[272] and shifting strategies in some cases, it is a good bet for Member State safe purchase of equipment. This is because through diversity, Member States and the EU can reduce the dependencies on any one supplier that result in vendor lock-in and parties having sway over Member States.[273] Sourcing from one supplier increases risk in the overall resilience of the network and increases the potential for a single point of failure.[274] Diversity can potentially secure the supply chain in the long term because different suppliers aren't likely to face the same supply issues at the same time.[275] If there are more players involved in the 5G network in theory, competition is increased,[276] prices go down in the long run,[277] and competition and open participation has the potential to increase quality.[278]

Capacity building is also especially important to long term success of Member State purchase of safe equipment since the network will be complex and will include both known and unknown risks. With the ongoing need to address risks and mitigate vulnerabilities, the current workforce gap puts the security of the network at risk.[279] All nations need to have experts who are trained at combating the cybersecurity challenges of confidentiality, integrity, and availability who can learn to understand the new technology involved in the new 5G NSA and SA network with a goal of creating the most robust and resilient network possible and enabling

---

[270] Greenleaf and Park, "South Korea's Innovations," 495.

[271] Haksoo Ko, et. al., "Structure and Enforcement of Data Privacy Law in South Korea," *International Data Privacy Law* 7, no.2 (2017): 101.

[272] This increase in cost can come as a result of many things, such as purchasing more expensive equipment that is perceived as more secure, through political decisions to exclude or include certain suppliers that result in economic consequences perhaps forcing Member States to make decisions based on factors other than cost.

[273] See the examples of Germany and the Czech Republic in Chapter 4.

[274] *Coordinated Risk Assessment*, 23.

[275] Rühlig and Björk, "Huawei Debate," 15.

[276] See discussion of Japan's approach to creating a diverse 5G network to avoid vendor lock-in, and secure supply chains in Mihoko Matsubara, "'Japan's 5G' Approach Sets a Model for Global Cooperation," *Lawfare*, September 14, 2020, https://www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation.

[277] Matsubara, "Japan's 5G."

[278] Matsubara.

[279] See reference to deficiencies in trained and specialized personnel relating to 5G networks in NIS Cooperation Group, *Coordinated Risk Assessment*, 20. See also Crumpler and Lewis, *The Cybersecurity Workforce Gap*.

society to fully utilize and regulate the market and network.[280] EU Member States and nations around the globe should encourage the acquisition of knowledge in this field, thus investing in the long-term success of the network. Whether it be through research and development, academics, or academies and workshops such as those at the ITU[281] or GSMA,[282] an increased number of experts could aid in security.

Beyond this, and as we have seen by the examples in Chapter 4, the decisions are largely based on political decisions of the Member States as well as national security concerns. However, this analysis posits or at least is hopeful that the EU will eventually find itself harmonized and cooperating as the network will only be as strong as its weakest link and as we've seen through the Brussels Effect, the EU may find its voice through its combined market power, regulatory capacity, preference for strict rules, predisposition to regulate inelastic targets, non-divisibility of standards,[283] and especially a concern for the protection of fundamental human rights and the digital single market.[284]

[280] Camacho, et. al., *Capacity Building*, 5.

[281] Camacho, et. al.

[282] Per their website, https://www.gsma.com/training/capacity-building/capacity-building-courses/, GSMA is also offering training courses on capacity building in the 5G network.

[283] Bradford, "The Brussels Effect," 11.

[284] Bygrave, *Data Privacy Law*, 57.

Table of Reference

Ahmad, Ijaz et. al. “Overview of 5G Security Challenges and Solutions.” *IEEE Communications Standards Magazine* 2, no. 1 (2018): 36-43.

Aho, Brett, and Roberta Duffield. "Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China." *Economy and Society* 49, no. 2 (2020): 187-212. doi: 10.1080/03085147.2019.1690275.

Aljazeera. “In Land of Big Data, China Sets Individual Privacy Rights.” *Aljazeera*, May 26, 2020. https://www.aljazeera.com/news/2020/05/26/in-land-of-big-data-china-sets-individual-privacy-rights/.

Barkin, Noah. “Judy Asks: Should Europe Ban Huawei’s 5G?” *Carnegie Europe*, January 30, 2020. https://carnegieeurope.eu/strategiceurope/80928.

Barzic, Gwénaëlle. “Europe’s 5G to Cost $62 Billion More if Chinese Vendors Banned: Telcos.” *Reuters,* June 7, 2019. https://www.reuters.com/article/us-huawei-europe-gsma-idUSKCN1T80Y3.

Bennhold, Katrin and Jack Ewing. “In Huawei Battle, China Threatens Germany Where It Hurts: Automakers.” *New York Times*, January 16, 2020. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html.

Bozsóki, István et. al. under supervision of ITU. *Setting the Scene for 5G: Opportunities & Challenges* (Geneva, Switzerland: International Telecommunications Union, 2018), 1-38. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-E.pdf.

Bradford, Anu. *The Brussels Effect*. New York: Oxford University Press, 2020.

Bradford, Anu. “The Brussels Effect.” *Northwestern University Law Review* 107, no. 1, (2012): 1-68.

Burgess, Matt. "What is the Internet of Things? WIRED explains." *WIRED*, February 16, 2018. https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

Bygrave, Lee. *Data Privacy Law*. Oxford: Oxford University Press, 2014.

Bygrave, Lee. *Internet Governance by Contract*. Oxford: Oxford University Press, 2015.

Cal. Civ. Code §§1798.100-1798.199.

Camacho, Mar et. al. *Capacity Building in a Changing ICT Environment*. Geneva, Switzerland: International Telecommunications Union, 2018. https://www.itu.int/dms_pub/itu-d/opb/phcb/D-PHCB-CAP_BLD.01-2018-PDF-E.pdf.

Campbell, Charlie. "'The Entire System is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World." *Time*, November 21, 2019. https://time-com.ezproxy.uio.no/5735411/china-surveillance-privacy-issues/.

Charter of Fundamental Rights of the European Union, December 12, 2007, O.J. (C 303) 14.12.2007.

Clark, James. "GDPR Series: Anonymisation and Pseudonymisation." *Privacy & Data Protection* 18, no. 1 (2017): 10-12.

Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament and the Council Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation SWD (2020) 115 final (June 24, 2020).

Corcoran, Kieran. "California's Economy is Now the 5th-biggest in the World." *Business Insider*, May 5, 2018. https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5?r=US&IR=T.

Court of Justice of the European Union, "The Court of Justice Invalidates Decision 2016/1250 On the Adequacy of the Protection Provided by the EU-US Data Protection Shield." Press Release No 91/20 July 16, 2020. https://curia.europa.eu/jcms/jcms/Jo2_7052/en/.

Crumpler, William and James Lewis. *The Cybersecurity Workforce Gap*. Washington, D.C.: Center for Strategic and International Studies, 2019. https://www.csis.org/analysis/cybersecurity-workforce-gap.

Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., November 6, 2016, effective June 1, 2017), translated by New America at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2019:1145. (Shrems II)

De Looper, Christian. "'What is 5G?' The Next-Generation Network Explained." *Digital Trends*, May 22, 2020. https://www.digitaltrends.com/mobile/what-is-5g/.

De Vass, Tharaka, Himanshu Shee, and Shah Miah. "The Effect of Internet of Things on Supply Chain Integration and Performance: An Organisational Capability Perspective." *AJIS Australasian Journal of Information Systems* 22 (2018): 2. doi:10.3127/ajis.v22i0.1734.

Ding, Jeffrey, Paul Triolo, and Sacks, Samm. "Chinese Interests Take a Big Seat at the AI Governance Table." *New America*, June 20, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

Donahue, Patrick. "Merkel Resists Full Ban on Huawei, Making Germany an Outlier." *Bloomberg*, September 23, 2020. https://www.bnnbloomberg.ca/merkel-resists-full-ban-on-huawei-making-germany-an-outlier-1.1498030.

Dragne & Asociatii, "Germany and Austria: Forerunners of 5G Security Measures?" *Lexology*, July 1, 2020, https://www.lexology.com/library/detail.aspx?g=2719d29a-30e5-458d-8977-9e514c2eadce.

ENISA. *Annual Telecom Security Incidents 2018.* 2019. doi:10.2824/350004.

ENISA. *How to Implement Security by Design for IoT*. 2019. https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot.

ENISA. *Threat Landscape for 5G Network.* 2019. doi:10.2824/49299.

ENISA. "What is State of the Art" in IT Security?" *ENISA*, February 7, 2019. https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security#:~:text=The%20document%20published%20on%20the,advice%20and%20recommendations%20for%20action.&text=The%20document%20can%20serve%20as,classification%20of%20security%20measures%20implemented.

Ericsson. "5G Estimated to Reach 1.5 Billion Subscriptions in 2024." Last modified November 27, 2018. https://www.ericsson.com/en/press-releases/2018/11/5g-estimated-to-reach-1.5-billion-subscriptions-in-2024--ericsson-mobility-report.

Ericsson. “Network Slicing is Ready to Impact.” *Digital Services* (blog) accessed October 27, 2020. https://www.ericsson.com/en/digital-services/network-slicing.

Esayas, Samson. “‘The Role of Anonymisation’ and Pseudonymisation Under the EU Data Privacy Rules: Beyond the ‘All or Nothing’ Approach.” *European Journal of Law and* Technology 6, no. 2 (2015), 1-23.

Eurasia Group. “White Paper: The Geopolitics of 5G.” *Eurasia Group* (November 2018): 1-19.

European Commission – EU Position in World Trade. “Facts and Figure on the EU’s Position in Global Markets.” Accessed October 27, 2020. https://ec.europa.eu/trade/policy/eu-position-in-world-trade/.

European Commission. *Commission Recommendation of 26.3.2019 Cybersecurity of 5G* Networks. Strasbourg, 2019.

European Commission. “How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection.” Adequacy Decisions. Accessed October 27, 2020. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Commission – Shaping Europe’s Digital Future. “NIS Cooperation Group.” Accessed October 27, 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

European Data Protection Board. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2019. 25. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

Fendos, Justin. “How Surveillance Technology Powered South Korea’s COVID-19 Response.” *Brookings*, April 29, 2020. https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/.

Fennessy, Caitlin. “The Schrems II’ Decision: EU-US Data Transfers in Question.” *International Association of Privacy Professionals*. July 16, 2020. https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

Greenleaf, Graham. *Asian Data Privacy Laws*. Oxford: Oxford University Press, 2014.

Greenleaf, Graham, and Park, Whon-il. "South Korea's Innovations in Data Privacy Principles: Asian Comparisons." *The Computer Law and Security Report* 30, no. 5 (2014): 492-505. doi:10.1016/j.clsr.2014.07.011.

Greenleaf, Graham. "The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law 2*, no. 2 (2012): 68-92.

Grieger, Gisela. *5G in the EU and Chinese Telecom Suppliers*. European Parliamentary Research Service: 2019. https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf.

GSMA 5G Taskforce. *The 5G Guide A Reference for Operators*. April 2019, 1-283. https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf.

Han, Qilong, Shuang Liang, and Hongli Zhang. "Mobile Cloud Sensing, Big Data, and 5G Networks Make an Intelligent and Smart World." *IEEE Network* 29, no. 2 (2015): 40-45. doi: 10.1109/mnet.2015.7064901.

Harris, Shon, and Fernando Maymi. *CISSP All-in-One Exam Guide*, 8th Edition. 1st ed. McGraw-Hill, 2018.

Hassan, Najmul, Yau, Kok-Lim Alvin, and Wu, Celimuge. "Edge Computing in 5G: A Review." *IEEE Access* 7 (2019): 127276-27289. doi:10.1109/access.2019.2938534.

IPlytics. "Who is Leading the 5G Patent Race?" *IPLYTICS*, November 2019. https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf.

Irion, Kristina. "Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law." *European Law Blog*, July 24, 2020. https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/.

ITU. "About International Telecommunications Union." *ITU*. Accessed October 27, 2020. https://www.itu.int/en/about/Pages/default.aspx.

Ji, Xinsheng et. al. "Overview of 5G Security Technology." *Science China - Information Sciences* 61, no. 8 (2018): 1-25. doi:10.1007/s11432-017-9426-4.

Ji-young, Sohn. “Korea No. 1 Worldwide in Smartphone Ownership, Internet Penetration.” *The Korea Herald*, June 24, 2018.

Kang, Chris, Sun Hee Kim, and Doil Son. “South Korea: Korea Introduces Major ‘Amendments’ to Data Privacy Laws.” *Mondaq*, March 2, 2020. https://www.mondaq.com/privacy-protection/898830/korea-introduces-major-amendments-to-data-privacy-laws#:~:text=On%209%20January%202020%2C%20the,Act')%20and%20the%20Act%20on.

Khan, Rabia et. al. “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions.” *IEEE Communications Surveys & Tutorials* 22, no. 1: 239-240. doi:10.1109/COMST.2019.2933899.

KISA Press Release. “Personal Information Protection Should Be Applied from the Planning Stages of IoT Service.” February 19, 2020. https://www.kisa.or.kr/notice/press_View.jsp?cPage=1&mode=view&p_No=8&b_No=8&d_No=1884&ST=&SV=.

Ko, Haksoo, John Leitner, Eunsoo Kim, and Jonggu Jeong. "Structure and Enforcement of Data Privacy Law in South Korea." *International Data Privacy Law* 7, no. 2 (2017): 100-14.

Kumar, Prajwol Nakarmi, Christian Schaefer, and Dario Casella. “5G and the EU General Data Protection Regulation.” *Ericsson Blog*, December 11, 2017. https://www.ericsson.com/en/blog/2017/12/5g-and-the-eu-general-data-protection-regulation.

Kuner, Christopher, Lee Bygrave, Christopher Docksey, and Laure Drechsler. *The EU General Data Protection Regulation (GDPR)*. Oxford: Oxford University Press, 2020.

Manners, Ian. “Normative Power Europe: A Contradiction in Terms?” *Journal of Common Market Studies* 40, no. 2 (2002): 235–258. doi:10.1111/1468-5965.00353.

Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul De Hert. "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation." *The Computer Law and Security Report* 35, no. 6 (2019): 105336. doi: 10.1016/j.clsr.2019.06.007.

Mayer, Robert, and Paul Eisler. “Whitepaper: Securing the Internet of Things.” *USTelecom* (April 2019): 1-10.

Mihoko Matsubara. “Japan’s 5G Approach Sets a Model for Global Cooperation.” *Lawfare*, September 14, 2020. https://www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation.

Maizland, Lindsay and Andrew Chatzky. “Huawei: China’s Controversial Tech Giant.” *CFR*, August 6, 2020. https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

Marr, Bernard. “What is Industry 4.0? Here’s a Super Easy Explanation for Anyone.” *Forbes*, September 1, 2018. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/.

National Cyber Security Centre in Response to US Sanctions, “Huawei to be Removed from UK 5G Networks by 2027,” press release, July 14, 2020. https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

NIS Cooperation Group. *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* (CG Publication 02/2019, 2019), 1-33. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

NIS Cooperation Group. *EU Toolbox of Risk Mitigating Measures* (CG Publication 01/2020, 2020). 1-45. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

NIS Cooperation Group. *Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity* (CG Publication 02/2020, 2020). 1-44. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

Parliament and Council Directive 2016/1148, 2016 O.J. (L 194) (EU). (NISD)

Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) (EU). (GDPR)

Parliament and Council Regulation 2019/881, 2019 O.J. (L 151) (EU). (Cybersecurity Act)

Pernot-Leplay, Emmanuel. “China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the EU.” *Penn State Journal of Law & International Affairs* 8, no. 1 (May 2020): 51-116. https://elibrary.law.psu.edu/jlia/vol8/iss1/6.

Personal Information Protection Act, (S. Kor.), translated in Korea Internet & Security Agency https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3.

Rühlig, Tim and Maja Björk. “What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe.” *Utrikespolitiska Institutet* Paper No. 10 (2020): 1–36. https://www.ui.se/butiken/uis-publikationer/ui-paper/2020/what-to-make-of-the-huawei-debate-5g-network-security-and-technology-dependency-in-europe/.

Sacks, Samm et. al. “China’s Emerging Data Privacy System and GDPR.” *Center for Strategic & International Studies*, March 9, 2018. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

Santora, Marc and Hana de Goeij. “Huawei Was a Czech Favorite. Now? It’s a National Security Threat.” *New York Times*, February 12, 2019. https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html.

Skouloudi, Christina and Gema Fernandez. “Toward Secure Convergence of Cloud and IoT.” *ENISA*, September 2018. https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot.

Smeets, Max and Herbert Lin. "Offensive Cyber Capabilities: To What Ends?" *NATO CCD COE Publications*, 10th International Conference on Cyber Conflict (2018): 55-72. https://ccdcoe.org/uploads/2018/10/Art-03-Offensive-Cyber-Capabilities.-To-What-Ends.pdf.

Soldani, David and Huawei Technologies Australia. "5G and the Future of Security in ICT." *29th International Telecommunication Networks and Applications Conference* (2019): 1-8. doi:10.1109/ITNAC46935.2019.9078011.

Sound, Saran Singh. “Evolution of the G.” *Stanford Management Science and Engineering* (blog). Last modified July 11, 2017, 11:48 AM PT. https://mse238blog.stanford.edu/2017/07/ssound/1g-2g-5g-the-evolution-of-the-gs/.

Stock, James, and Stefanie Boyer. "Developing a Consensus Definition of Supply Chain Management: A Qualitative Study." *International Journal of Physical Distribution & Logistics Management* 39, no. 8 (2009): 690-711. doi:10.1108/09600030910996323.

Taboada, Ianire, and Shee, Himanshu. "Understanding 5G Technology for Future Supply Chain Management." *International Journal of Logistics* (2020): 1-15. doi:10.1080/13675567.2020.1762850.

Tech4i2, Real Wireless, CONNECT- Trinity College Dublin, InterDigital. "Identification and Quantification of Key Socio-economic Data to Support Strategic Planning for the Introduction of 5G in Europe." *SMART* 2014/0008 (2016). doi:10.2759/56657.

The Constitution of the Republic of Korea, last amended October 29, 1987, (S. Kor.). translated by WIPO. https://www.wipo.int/edocs/lexdocs/laws/en/kr/kr061en.pdf.

Townsend, Will. "Who Is 'Really' Leading in Mobile 5G, Part 4: Infrastructure Equipment Providers." *Forbes*, July 19, 2019. https://www.forbes.com/sites/moorinsights/2019/07/19/who-is-really-leading-in-mobile-5g-part-4-infrastructure-equipment-providers/.

Voigt, Paul, and Von Dem Bussche, Axel. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing AG, 2017. doi: 10.1007/978-3-319-57959-7.

Voss, Gregory, and Kimberly Houser. "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies." *American Business Law Journal* 56, no. 2 (2019): 287-344.

"U.S. – Poland Joint Declaration on 5G." Whitehouse.gov Foreign Policy, last modified September 5, 2019. https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

Wang, Zhizheng. "Systematic Government Access to Private-sector Data in China." *International Data Privacy Law* 2, no. 4 (2012): 220-29. doi:10.1093/idpl/ips017.

Wei, Yuxi. "Chinese Data Localization Law: Comprehensive but Ambiguous." *University of Washington Henry M. Jackson School of International Studies* (blog). https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/ .

3GPP. "Partners." accessed October 27, 2020. https://www.3gpp.org/about-3gpp/partners.