KONRAD ADENAUER STIFTUNG

Data Innovations and Challenges in South Korea

From Legislative Innovations for Big Data to Battling COVID-19

Kyung Sin Park, Korea University, Open Net Association
Natalie Pang, National University of Singapore

DATA AND INNOVATION
IN ASIA-PACIFIC

www.kas.de

CONTENT

PREFACE

Data fuels digital change. It forms the basis for numerous new products and services and can bring about specific advantages such as personalised medicine, autonomous driving, or more efficient administration. While data may be indispensable for the generation of new knowledge and may aid rational decision-making in the spheres of politics, society, and the economy, it brings with it an element of fear stemming from issues such as vulnerable consumers, privacy concerns, and the possibility of algorithm-based decisions being executed independent of human control.

The ability to collect and process ever-increasing amounts of data is a **key to innovation and growth**. For states such as Germany with a globally networked and high-tech economy, this presents enormous opportunities – especially due to the increasing amount of non-personal data made available through industrial processes as well as public sources. However, neither Germany nor Europe is fully exploiting the innovative potential of data for the benefit of society, the economy, science, and the state. The collection and analysis of data does not have to be in conflict with the **European approach to data protection, which marks an important standard for the responsible handling of data** in the global context.

Numerous US and Chinese companies have occupied central strategic positions in the digital economy in recent years. These include cloud systems, digital payment systems, online trading, and Artificial Intelligence (AI). **Despite some notable successes, Europe and Germany still lack a comprehensive vision for the "age of data".** Nevertheless, in the spring of 2020, the European Commission launched its roadmap for digital policy – a "Data Act" to create a single European data market is planned for 2021.

Against this background, it is worth taking a **comparative look at the Asia-Pacific region** as it is generally considered the region that currently leads in both global innovation and economic growth.

Hence the Konrad Adenauer Foundation's regional programme "Political Dialogue" based in Singapore started a large-scale study in September 2019 on *Data and Innovation in Asia-Pacific*. We want to turn our gaze away from Silicon Valley to other important "data nations" in order to investigate the ambiguous and not-at-all-clear **connection between the use of digital data and the innovative capacity of economic and social systems**. However, we will not limit our analysis to technical and economic issues as the exploration of this ambiguous connection inevitably involves the fundamental political question concerning the *systemic competition* between liberal-democratic societies and authoritarian development models – in particular, that of the People's Republic of China – with regard to the manner in which data is attained and used. To put it more pointedly, the question is: in times of omnipresent data generation and its use by increasingly AI-based systems, is the ability to innovate only to be had at the price of the complete disclosure of private data to governments and corporate actors? Or can an alternative approach, one balancing both the protection of basic rights and promotion of innovation, be found?

The study was carried out in collaboration with the National University of Singapore (NUS) and was supported by the country offices of the Konrad-Adenauer-Stiftung in Asia-Pacific. We selected **Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan** as the contexts to be examined. We

looked at the areas **of transport, finance, administration, health, and Industry 4.0** to understand how added value for society and the economy can be created through modern data use.

We aim to contribute to the discussion on how to balance data usage and data protection in order to promote innovation in this digital age.

The following questions guided us in this study:

Narratives

How do companies, state actors, and civil society understand the handling of data – especially personal data – and the ethical assessment of such use? What are the prevailing narratives in each country?

Legal Bases

What are the laws and regulations that apply to the collection, use, storage, provision, disclosure, retention, and disposal of personal and non-personal data? What is the status of the development of legislation for these matters and how do different stakeholders deal with the issues of data protection and data portability between different (private and public) systems?

Ecosystem

Data is part of a larger "innovation ecosystem". Its potential can only be realised through interaction with other innovation-promoting elements. What specific legal, technological, infrastructural, cultural, and economic aspects of a country shape the respective ecosystems and determine performance?

In Singapore, Japan, and Taiwan, the study is also supplemented by a representative population survey on data culture.

We hope that the diverse pictures presented on the subject of data and innovation in Asia will provide food for thought in Germany, Europe, and Asia itself.

Dr. Peter Hefele
Director Asia and the Pacific

SUMMARY

1. Like many modern democracies, the South Korean government has placed much focus on information technology and the value of data in generating innovations. Infrastructurally, the country presents a fertile context for innovation, having high rates of broadband and smartphone penetration and use. At the same time, a digital divide exists in populations such as the elderly and low income.

2. A **state-paternalistic approach** to data innovation prevails, with the government having to provide express approval and legal direction before innovations can happen. While this stipulates the terms by which innovation may happen, such a prospective, cautious approach may also have the effect of curtailing the full possibility of innovative potential. This is seen in how innovators often have to wait for legal direction and precedent, and prospectively specify the use of data before carrying out innovative projects. This approach also disturbs the serendipitous element of innovation, where breakthroughs result from free explorations of data.

3. In 2020, South Korea passed **three major legal amendments** to its data privacy laws to promote data innovation: The Personal Information Protection Act (PIPA), the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act) and the Act on the Use and Protection of Credit Information (Credit Information Act), collectively known as the "Three Laws of Data". They are aimed at strengthening regulatory supervision and to introduce the concept of 'pseudonymised data'.

4. **However, major legal conundrums remain** in the PIPA, and how it relates to the European General Data Protection Regulation (GDPR), which have major implications on how data is used. The foremost concern has to do with non-consensual processing of citizen data. The GDPR stipulates that non-consensual data processing may be justified by the production of socially beneficial results such as in public interest archiving, scientific research or statistical purposes, otherwise known as ARS purposes, but the PIPA relies too much on data 'pseudonymisation' and ends up making it a sufficient condition for derogating some of data subjects' rights such as access, erasure, correction, and opt-out.

5. Experts interviewed also opine **the laws' disproportionate focus on consent and data subjects' control on data processing.** In South Korea, the predominant understanding of data protection law is that it gives data subjects control over data about themselves. In other words, personal data is understood primarily as being the property or under the control of the individuals represented by the data, and data protection is seen in terms of preserving data control by owners, rather than ensuring data privacy. While affording control to data subjects over personal data, this approach may have stifled data innovation in cases where consent is required.

6. The consent-centric data protection law ended up relied too much on pseudonymization as a basis of non-consensual use and ended up deprecating data subjects' rights such as right to access or erasure even outside the ARS context. This creates a loop hole whereby ill-intended data controllers may evade affordance of such data subjects' rights simply by pseudonymizing the data. This is important for data privacy because it is through exercise of access and other rights that data subjects can protect themselves.

7. **Civil society voices have attempted to balance government and industrial direction, although mistrust has led to a climate of mutual conflict.** Pseudonymisation-backed non-consensual processing (including data linkage) and data portability were deemed encroachments on the individuals' data sovereignty, with oppositional sentiment fuelled by negative, past experiences associated with the resident registrational number (RRN) system. To civil society groups, pseudonymisation-backed non-consensual processing and data portability all became 'dangerous' activities that needed to be somehow administered under a publicly sanctioned environment.

8. The COVID-19 pandemic presents a case example to study the trade-offs between data consent/privacy and public good. Unlike most countries around the world, South Korean infectious disease regulations permit the non-consensual use of data. This aspect was exploited towards exceptionally precise and efficacious contact tracing in curbing COVID-19 – integrated personal data, credit card information, mobile phone location information and surveillance camera data were utilised. In comparison, most other countries adopt voluntary contact tracing methods, which have had limited efficacy as it depends on citizen compliance and trust in proper data security and handling by authorities.

9. The post-COVID era will necessitate serious, country-level discussions of what data innovation means in the data age. Aside to sorting out legal requirements and digital infrastructure, decision makers would need to be cognisant of the importance of building mutual trust between government, industry and citizenry, so that data innovation is adopted in not only a permissive but transparent environment. While data innovation is often undertaken for reasons associated with strengthening public administration and economic growth, citizen transparency and being clear about the social, long-term benefits of innovation can go a long way to fostering wider acceptance of innovation while mitigating suspicion and discontent.

INTRODUCTION AND CONTEXT

This project aims to examine key developments in data policy and innovation in South Korea, focusing on the domains of regulations and health. It is part of a series of reports surveying seven different Asian territories to deepen understanding of innovation and data policies, and contribute to debates which often focus on European models of data protection such as the General Data Protection Regulation (GDPR).

Like many modern democracies, the South Korean government has placed much focus on information technology and the value of data in generating innovations. The Personal Information Protection Act (PIPA) to regulate the use of personal data was introduced in South Korea in 2011 and since then there have been many technological developments in the country.

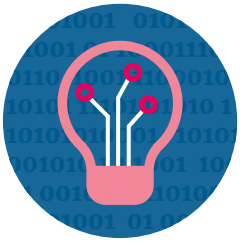
The Moon Jae-In administration in 2017 outlined a five-year roadmap aimed at bringing South Korea into a new digital era (Rosenberg, 2019). A key initiative of this roadmap is the I-Korea 4.0, which acts as a policy direction for the country to enter the Fourth Industrial Revolution. Under the purview of the Ministry of Science and ICT, its objectives include reforming the research and development system to encourage disruptive innovation, and investing in technologies such as artificial intelligence (AI), internet of things (IoT) and 5G network (Government of the Republic of Korea, n.d.).

The COVID-19 pandemic led the government to introduce a number of measures, which must be understood against the backdrop of eHealth innovation in South Korea. As the country moves forward from the pandemic's economic fallout, the government is also stepping up its drive for innovation to help lift the economy (D.-H. Kim, 2020). It unveiled the "K-New Deal" in 2020, a 160 trillion won investment aimed at creating 1.9 million jobs by 2025 in the digital and green sectors (Kim, 2020).

In this regard, this report analyses two emergent discourses on data innovation in Korea:

1. the South Korean government's legislative initiatives in 2020 designed to promote data innovations, namely the "Three Laws of Data"

2. E-health, with a focus on the South Korean government's use of personal data for the purpose of COVID-containment.



Digital Context

South Korea has earned a reputation as one of the most wired countries in the world. The country ranks among the highest in Asia in terms of digital infrastructure, coming in 2nd behind Singapore out of 11 Asian economies including Taiwan, Hong Kong and Japan, and 5th when considered globally (The Economist Intelligence Unit, 2016). It is known for its extensive broadband reach, fast connections as well as ease of access and affordability of those connections, which create a fertile environment for businesses to go digital.

In 2018, the country's rate of internet penetration and internet use was reportedly at 95.1% and 90.3% respectively, and around 89.5% of the population owned a smartphone (National Information Society Agency, 2018). Notably, South Korea was the first country to commercialize 5G services, doing so in April 2019 and reaching 5G subscription numbers of more than 1.6 million people by June of that year, accounting for 77.5% of 5G subscribers worldwide (Korea Information Society Development Institute, 2020).

At the same time, there appears to be a digital divide among socially disadvantaged populations such as the elderly, physically disabled, low-income earners and rural dwellers. The digital utilization rate of these groups stood at around 70% of ordinary citizens in 2019 (Yonhap News Agency, 2020). For example, the elderly population's Internet usage is reportedly at 59.9%, and 65.2% in terms of smartphone use (National Information Society Agency, 2018). More recently, it has been suggested that compared to the general population, the elderly do own and use information devices (e.g., computers, mobile devices) at a comparable rate (90.6%), but at a reduced level of digital literacy (51.6%) and with less frequency and diversity of use (63.9%; Jun, 2020).

Innovation and Regulatory Landscape

The innovation and regulatory landscape in South Korea comprises a number of key stakeholders:

- **The Presidential Fourth Industrial Revolution Committee:** Launched in October 2017, the committee consists of 20 civilians and five government officials who discuss government policies concerning the fourth industrial revolution as well as ways to implement plans effectively (Sohn, 2017).

- **The Ministry of Science and ICT**: It oversees South Korea's efforts to accelerate innovation and to reform regulations and systems for new industries such as AI and biotechnology.

- **I-Korea 4.0:** A key project of the current South Korean administration, this plan outlines the government's strategy to push for intelligent infrastructure, 5G and smart mobility.

- **Laws on data privacy**: The Personal Information Protection Act (PIPA) was enacted in 2011 to integrate two separate laws that used to regulate the use of personal data in the public and private sector, and serves as a general statute covering data privacy issues in South Korea. PIPA was amended in 2020 to streamline regulatory supervision and to introduce the concept of 'pseudonymised data'. Other regulations on data privacy include the Act on the Promotion of the Use of the Information Network and Information Protection, as well as the Credit Information Use and Protection Act.

South Korea's data culture poses several unique challenges that could impede the country's drive towards innovation.

First, in terms of data sharing, government departments actively make efforts to open up and share public information. **Their efforts, however, have overly focused on making public sector data available, without sufficiently encouraging their use in the private sector**. For example, the 2013 Act on the Promotion of Public Data Provision and Use facilitates the sharing and promotion of open public data, and the "Korea Public Data Portal" operated by the Ministry of Public Administration compiles open data from local and central governments. Yet, businesses do not seem to make much use of this openly available data (Park and Park, 2019). As a 2018 report suggested, only about 3.2% of open data from local governments have been used amounting to only 567 officially recognized use cases, of which most are based on public data specific to Seoul. One reason for this lack of interest is that such open data is often limited to a specific region. Consequently, use cases of public data have been limited to data visualization, rather than business applications (Lim, 2018).

As a 2018 report suggested, only about 3.2% of open data from local governments have been used amounting to only 567 officially recognized use cases, of which most are based on public data specific to Seoul.

Second, **state paternalism has resulted in a regulatory environment where innovations cannot begin without the express approval of the government, and without explicit government direction on how exactly data can be used.** One infamous example of this is that, until 2015, government-issued electronic certificates were required for every online payment in exclusion to other payment security methods (The Korea Herald, 2014). Many successful innovations are the result of serendipitous, divergent exploration and data innovations are no exception, requiring experimentation into different possibilities of using data. However, many otherwise valid concerns for privacy were addressed through only ex ante regulation that aimed at prospective behavioural control over actors, as opposed to ex post regulation that 'wait and see' how the actors respond in various creative ways toward privacy. Such a regulatory model stamped out the possibility for such serendipities. For instance, although repurposing personal data for statistical and other anonymous uses was already allowed under existing law, it took major legislative and regulatory changes in 2020 that spelled out exactly how such repurposing can be done, before the private sector could begin investing in such data repurposing.

Third, **the 13-digit resident registration number (RRN) assigned to all individuals in South Korea as a tool to authenticate one's identity in the country remains a risk for potential breach of data.** This is because both public and private data controllers have required an individual's registration number in order for them to enjoy a service, thus having access to these numbers would also mean access to a huge trove of an individual's personal data traversing various public and private services (Park, 2014). The pervasive use of these identity numbers has further complicated discourse on data governance, leading to greater mainstream awareness and calls for stronger security measures and data protection laws.

Fourth, **the presence of strong laws protecting against defamation** (Park, 2017; Haggard and You, 2014) **has had an impact on data culture in South Korea**. Since the early 2000s, there has been a marked increase in the use of defamation laws by politicians and governments against their critics, leading to an erosion of freedom of expression. These laws punish diffusion of even truthful, non-privacy-infringing statements as long as they are deemed "insulting" or "reputation-lowering". While such laws are intended to create a culture of courtesy and generosity toward others they can also be abused to suppress people's right to know and freedom of speech, creating a general climate of restraint that could have a chilling effect on innovation and encourage overzealous application of data protection principles. For instance, court judgment databases are generally not made available to the public before each judgment goes through the costly process of de-identification, charged to the users at the rate of KRW 1,000/judgment even for one-time viewing (Lee, 2019).

Court judgment databases are generally not made available to the public before each judgment goes through the costly process of de-identification, charged to the users at the rate of KRW 1,000/ judgment even for one-time viewing.

Most recently, amendments have been introduced to existing data privacy laws to streamline regulatory supervision, and to introduce the concept of 'pseudonymised data' which could further affect the data culture in South Korea. The laws affected are the Personal Information Protection Act (PIPA), the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act) and the Act on the Use and Protection of Credit Information ('Credit Information Act'). Given the novelty of these amendments, this report will discuss in greater detail the effects of these changes in the next chapter.

Case 1

The Three Laws of Data

In January 2020, the South Korean legislature passed amendments to its data privacy laws to promote data innovation. These amendments aimed to streamline regulatory supervision and to introduce the concept of 'pseudonymised data'. The laws in question are the **Personal Information Protection Act (PIPA)**, the **Act on the Promotion of Information and Communications Network Utilisation and Information Protection (Network Act)** and the **Act on the Use and Protection of Credit Information ('Credit Information Act')**, collectively known as the **"Three Laws of Data"**.

The purpose of these laws was to adopt the European Union's General Data Protection Regulation (GDPR) which allows for the non-consensual use of personal data for public interest archiving, scientific research or statistics purposes, (otherwise known as **ARS purposes**). It was hoped that data innovations would be promoted through these exceptions, though whether or not this would be effective may be too early to tell since the exceptions only came into effect in August 2020.

Scope of Non-consensual Scientific Use

Under the GDPR, such non-consensual, scientific uses of data may be allowed if users abide by the principle of data minimisation, in which data collected and processed should be used, and not retained beyond, for reasons clearly stated in advance. One major guideline to this principle is the **pseudonymisation of data**. Pseudonymisation refers to processing personal data in a manner such that the data in question cannot be attributed to a specific individual (i.e. the data subject) without the use of additional information. One example of this is to replace explicit identity data markers, e.g. individuals' RRNs with a separate set of codes so that the personal data in question is 'depersonalized', and can no longer be identified without knowledge of the relationship between the new codes and RRNs.

However, civil society actors such as Progressive Network Center Jinbonet, People's Participatory Solidarity for Democracy, etc. disagreed with the passing of these amendments. Specifically, **the most important point of contention was whether such non-consensual use of personal data for ARS purposes includes for-profit research**. They argue that pseudonymised data is still personal data even under the GDPR, and that non-consensual use of personal data can only be justified for research that can contribute to the expansion of society's knowledge (Lee, 2019).

Civil society advocates demanded that the use of data for non-consensual scientific research be limited to "academic research", while the government and industry players pointed out that the GDPR allows "privately funded research" to be done without explicit consent, under the ARS exception outlined in GDPR Recital 159. The civil society response was that "privately funded research" explicitly allowed by the GDPR must still be academic in some sense because the need to take into account the purpose of "European Research Area" set forth in Treaty Forming European Union requires research to be readily accessible within EU across national boundaries (GDPR Recital 159) (Lee, 2019). Civil society actors also explained that Korea is a different environment that requires customised regulations in the context of South Korea's pervasive use of the RRN, which makes it much more difficult to de-identify or pseudonymize data.

A conversation with European Commission's data protection official reveals that despite the arguments made by South Korea's civil society actors, commercial, for-profit research is indeed included in ARS exceptions. According to the official in question, the "European Research Area", which aims to create a single, borderless market for research, innovation and technology across the European Union, is designed to compel researchers to publish research findings to the public.[1] This is to justify the use of citizens' non-consensual personal data as being in the public interest, and is consistent with the views of other regulators that non-consensual scientific use of personal data is justified by social benefits arising out of such scientific research[2], and that as long as such social benefits exist, for-profit research can be conducted under that exemption.[3] Given this precedent, it could also have been possible for South Korea's PIPA's ARS exception to be conditioned on the public availability of research findings rather than the nature of the funding organisation. In other words, **the government and the civil society could have compromised so that for-profit scientific research be allowed to be carried out based on non-consensual use of pseudonymised data as long as its benefits are somehow made available to the public**.

1 A phone conversation between Kyung Sin Park and European Commission, DG Justice and Consumers, Unit C4 – International Data Flows and Protection

2 See European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research, January 2020. "For the purposes of this Preliminary Opinion, therefore, the special data protection regime for scientific research is understood to apply where each of the three criteria are met: 1) personal data are processed; 2) relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight; 3) the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests."

3 See Information Commissioner's Office, What Are the Conditions for Processing?. "Commercial scientific research may therefore be covered, but you need to demonstrate that it uses rigorous scientific methods and furthers a general public interest. However, commercial market research is unlikely to be covered, unless you meet this requirement."

However, such a compromise did not take place in South Korea. Despite the concerns from civil society, the amendments to the PIPA act were passed in January 2020 in the original form proposed by the government. **The law adopts the same GDPR language, i.e. "privately funded research" but fails to refer the need to make available research findings to the public as GDPR's preamble does**. Conflicts were fierce. Even before the amendment passed, the first commercial attempt at data linkage resulted in civil society actors filing a criminal complaint against the data controllers (Kim, 2017), which was eventually dismissed by state prosecutors who agreed with the government's opinion encouraging such linkage, i.e., that non-identifiable information cannot be viewed as personal information. Such legal opinion appears to have established a precedent for the private use of de-identified personal data. (Yang, 2019).

Impact of Pseudonymization on Data Subjects' Rights of Access, Rectification, Restriction and Objection

Furthermore, t**he lack of consensus between civil society and the government with regards to these amendments has resulted in "legislative flaws"** that neither had anticipated. Since there was little constructive discourse and recognition of mutual interests, legal amendments were made with minimal scrutiny or input from civil society voices.

The flaws originated from the fact that South Korea's PIPA's ARS exception does not hinge primarily upon the nature of further processing of data but on pseudonymisation. This is in contrast to the GDPR, where exemptions allowing non-consensual processing of personal data depend primarily on whether or not such processing is socially beneficial (i.e., science, statistics, public interest archiving). Pseudonymization is simply one of the measures implemented under the principle of data minimization, a plus factor and privacy-enhancing measure for allowing such non-consensual use (GDPR 89(1)). Pseudonymising the data is neither a necessary nor a sufficient precondition of non-consensual ARS processing. **In contrast, Korea's PIPA focuses too much on pseudonymization (PIPA 28-2) as an enabling factor**.

The bottom line of non-consensual ARS use governance did not suffer much since pseudonymized data could be used non-consensually only for ARS purposes anyway (PIPA 28-2), a result similar to GDPR. However, the consent power for use and transfer of data is not the only right that data subjects have. Data protection laws give data subjects other rights such as the right to inspect data about them held by data controllers, opt out of certain uses, and delete or correct data about them ("other data subject's rights").

Now, the GDPR exempts from other data subjects' rights as well as from consent power for the ARS processing. GDPR does so because the social benefits of such processing, including innovation, will be impeded if quality of data is deprecated by potentially excessive access and erasure requests by data subjects (GDPR 89(2)). Therefore, data subjects' rights to rectification, restriction and objection to processing may be forfeited if they are likely to seriously impede the realisation of ARS purposes. This is where Korea's PIPA widely departs from GDPR, complicating and contradicting the intended purpose of ARS exemptions. **While GDPR's exemption from other data subjects' rights is based on the social benefit accompanying ARS processing, in contrast, Korea's PIPA's exemption from those rights is based on pseu-**

donymization of data (PIPA 28-7). Therefore, any data controller can evade the duty to afford data subjects access, erasure, and objection simply by pseudonymising the data even if it is not planning to use the resulting data for ARS purposes.

The government's explanation for this loophole is that, in order to assuage concerns that pseudonymized data may be reidentified, causing loss of privacy, PIPA 28-5 was legislated to ban re-identification for all purposes. Logically, affording data subjects the rights to access, erasure, etc., is impossible without re-identification anyway. If the data are not identifiable, data controllers will not know what data to make available to the data subjects trying to exercise their access rights.

However, this explanation leads to frustration of the very purpose of creating the new category of data called pseudonymized data: pseudonymisation is a deliberate process where the possibility of re-identification is preserved. If it is legally impossible to re-identify pseudonymised data, that data is no longer pseudonymous but may as well be called anonymous, and it will be entirely outside the purview of personal data protection law. This goes against the fundamental tenet that pseudonymised data remains personal data. GDPR's intent to create the middle way to encourage innovation while protecting privacy is vanished.

Furthermore, **pseudonymisation is a process explicitly encouraged by GDPR for security and privacy purposes (GDPR 32, 40) but it is now made 'dangerous' to data subjects by the Korean law**. German data protection law requires pseudonymization as part of security measures (BDSG Article 64) and privacy by design (Article 71) and also requires that personal data be pseudonymized or anonymized as soon as possible and as much as possible to the extent compatible with the purpose of collection (BDSG Article 71). Storing all unique identifiers of data files such as names, credit card numbers, social security numbers, etc., in the form of encrypted codes is a routine practice. Korean law even requires residence registration numbers to be stored only in encrypted form.[4] It is not a good policy to couple such routinely used and sometimes legally compelled forms of data processing with such deprivation of rights.

What is even worse, now that pseudonymisation has become a 'dangerous' process for data subjects, the **government has come up with cumbersome procedures for pseudonymisation, which makes it difficult for data controllers to engage in security measures involving pseudonymisation and encryption**. Pseudonymisation and encryption are still 'data processing' and therefore doing so non-consensually still requires some legal basis (GDPR 6) but given that pseudonymisation is explicitly encouraged by GDPR for privacy and security, in "all conceivable cases", pseudonymisation will be considered compatible with the original purpose of collection (Hintze and El Emam, 2019). However, because of the government restrictions on pseudonymization, the well-intentioned data controllers will be disincentivised from taking pseudonymization for privacy-enhancing and security-enhancing purposes. What is worse, sensing the danger associated with pseudonymisation, civil society has ironically been opposing pseudonymisation (Newsis, 2021), a measure encouraged and often required by GDPR and data protection laws around the world, including South Korea. **Without pseudonymisation, data innovations would be severely hampered as non-consensual ARS processing usually needs to be preceded by pseudonymisation as a privacy/security-enhancing pre-requisite.**

4 See Article 7 of Korea's Personal Data Security Measures Standard (a regulation promulgated under and interpreting Korean Personal Information Protection Act)

Need for Better Communication

It seems that confrontation and the lack of communication between the civil society and the government may have led to this conundrum. **The civil society expressed concern that non-consensual ARS use of pseudonymised data could still lead to data being re-identified.** The concerns of civil society actors are valid given past negative experiences with policies deemed excessively intrusive such as the RRN regime (Sweeney & Yoo, 2015). As such, they were not willing to readily agree to legal reforms allowing more liberal use of personal data, whether benchmarked to GDPR or not, before the fundamental lack of anonymity imposed by the RRN system is addressed.[5]

Wanting to assuage such concerns, **the government legislated through PIPA that all instances of reidentification of pseudonymised data would be banned without exception with criminal penalties attached** (PIPA 28-5). The end result: Right of access, erasure/correction, and objection are curtailed for all pseudonymized data. The government improvidently assumed that the civil society would welcome a criminal ban of re-identification.[6] The truth is that civil society certainly would not have wanted such a ban if they were properly informed that the right of access, erasure/deletion, etc. would be rendered unenforceable by such ban. Also, such a ban is unprecedented since there are substantive reasons why personal data are pseudonymised as opposed to anonymized. For instance, German data protection law states that identifiers and pseudonymised data may be "combined", amounting to reidentification for ARS purposes.[7]

Discussions are ongoing to resolve this misunderstanding. First of all, exemptions from other data subjects' rights must be limited to the non-consensual use for ARS purposes. Pseudonymisation by itself should not deprive data subjects of the right of access and other rights. After Open Net filed a constitutional challenge and made a submission to European Data Protection Board, the country's data protection authority PIPC issued a reading to that effect.[8] Secondly, the ban on re-identification must be loosened to allow re-identification for the purpose of affording data subjects' rights.

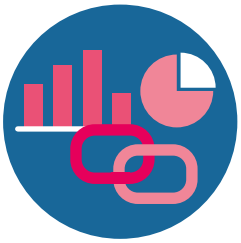
5 Interview with Byoungil Oh, Yeokyung Chang

6 Interview with Inho Lee, Interview with Jongsoo Yoon

7 See BDSG (2019), Article 27 (3), "Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose."

8 Park, Kyung Sin. (2021). March 2021 Letter to European Commission and European Data Protection Supervisor on Korea's GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions Retrieved from http://opennetkorea.org/en/wp/3239; "Personal Information Protection Commission, Supplementary Rule #4, Notification No 2021-1 of the Personal Information Protection Commission (PIPC), Annex I of the European Commission's draft adequacy Decision concerning the Republic of Korea; Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea, September 24, 2021, p. 21–22.

While the Three Laws of Data are aimed at promoting data innovations, they may end up paralysing data innovation although several experts that were interviewed for this study cautioned that it is too soon to tell what the impact of these amendments are. It is especially noteworthy that the pre-existing law already allowed the personal data to be used non-consensually as long as it is used for scientific purposes in a manner not identifying individuals. The 2020 amendment was a rushed attempt to emulate GDPR that may have instead made data innovations more difficult.[9] Furthermore, data subjects lose out a great deal, both because 'good' data controllers cannot easily administer privacy/security-enhancing pseudonymisation measures and also because, if they somehow succeed in doing so, data subjects' access, erasure/deletion, and opt-out rights are deprived.



Data and Database Linkages

Another problem with the Three Laws of Data concerns data linkage. Linking databases previously created for disparate purposes is a key component of big data processing. Out of the key features of big data (velocity, volume, and versatility (3V)), versatility is the most prominent feature, associated with the potential of drawing unanticipated insights from unprecedented combinations of databases otherwise considered mutually unrelated. Linking a pre-existing database (e.g., book rental records of public libraries) with another pre-existing data (e.g., hospital records) to figure out, for instance, a relationship between data subjects' book-reading habits and their health constitutes "repurposing" of personal data which normally requires data subject's consent. GDPR's provisions on non-consensual ARS processing come in handy to allow such data linkage. GDPR does not, however, have special provisions on data linkage but simply includes 'combining personal data' under a general rubric of 'processing', to which the ARS exception applies.

However, **PIPA stipulates that only specially licensed "dedicated data linkage agencies" (PIPA, Article 28-3) can link databases**. The proposed reason is that data linkage involves non-consensual repurposing of personal data that is more invasive than other repurposing. Therefore, the process of data linkage must be subjected to public governance, including insurance and financial liability requirements in case of data breach, so the theory goes. However, this creates two problems that would impact other state-paternalistic programs such as RRNs and government-issued electronic certificates. First, such dedicated data linkage agencies will become a weak link in data security as more and more data is concentrated and stored with them, even if temporarily. **An additional, implicit consequence of such data sharing is that these agencies will undoubtedly obtain knowledge of researchers' research agendas, which could cause chilling effects on innovative research efforts in this regard**, in that researchers may be discouraged from sharing their data as well as agendas with the agencies in question.

9 See Pre-2020 PIPA Article 18(2)4, "Where personal information is provided in a manner keeping a specific individual unidentifiable necessarily for such purposes as compiling statistics or academic research".

Data Portability

The amendments to the Three Laws of Data have also sought to facilitate data portability. **Data portability, a data subject's right to have one data controller transfer their personal data to another**, has the dual purpose of enhancing data subjects' interests (i.e., having to exercise the right to access and then sending the data may be more cumbersome than having the data controllers transfer it directly between them[10]) and lowering switching costs, thereby mitigating market dominance of the existing data controllers. Data portability is included not in PIPA but stipulated in the Credit Information Protection Act, a sector-specific data protection for credit information.

From the perspective of financial institutions, the amendments will support the development of innovations such as "MyData" projects. MyData is a government-led platform which gives licensed companies access to customer information from a range of sources. While the focus is on financial information, other firms such as telecom, retail and IT firms are also seeking regulatory approval to launch MyData services (Lee, 2020). On the customers' part, one can manage financial information across multiple service providers, receive more personalised services and switch providers easily if they choose by exercising data portability rights. As the name suggests, this system is based on the view that data is the property of its subjects, who should have control over it. Bank Salad, a fintech company, was chosen to pilot the MyData platform: By making use of data from telecom and retail companies, it can tailor services such as loan comparison and interest rate setting based on credit ratings and payment history (Kim, 2020).

In line with state paternalism, the Credit Information Act only allows "credit information businesses" that are licensed under stringent, minimum capital and security requirements to receive data for data portability purposes. This creates two problems. The first is similar to that plaguing dedicated data linkage agencies: **concentration of data among the licensed organisations, leading to a higher risk of breach**. The second issue is that **this concentration will create "data silos", thus entrenching data monopolies and discouraging healthy competition in the market, contrary to the legislative purpose of the provisions**. This is why, ironically, Internet companies in Korea opposed the data portability provisions as they will be required to turn over their customers' information (albeit pursuant to data subject's requests) to the licensed institutions operating MyData services.

For example, retail and e-commerce companies are opposing the sharing of customer transaction information with credit information companies, but the Financial Services Commission argues that shopping information and data from commercial transactions can be considered credit information by law. **Some companies are thus considering shifting their online payments to subsidiary IT firms which cannot be covered by the Credit Information Act in order to avoid sharing such extensive customer information** (Sung, 2020). There is intense competition to win regulatory approval from the Financial Supervisory Service, which is now assessing the applications of 38 companies. As one representative from KT Corporation, South Korea's largest national telecom company explained, they cannot afford to lose such an opportunity as they would then be obliged to provide data collected by their own firm to the firms that are successful in their bids for approval (Kim, 2020).

10 For this reason, one of the experts calls the data portability right an "access plus" right.

Common Root of the Problems: Consent-centered Privacy does not leave room for balancing

According to experts interviewed, these challenges have the same root: the laws' disproportionate focus on consent and data subject's control on processing. In South Korea, the predominant understanding of data protection law is that it gives data subjects control over data about themselves. In other words, personal data is understood primarily as being the property or under the control of the individuals who generate it. Such an understanding is buttressed by existence of the truth defamation law by which one can control even what others think of them by barring access to inconvenient facts about him or herself (Park, 2017). Short of the ARS exceptions mentioned above, non-consensual data use is not only considered a crime but prosecuted as a crime under Korean data protection laws. While civil society groups advocated for cutting back on criminal prosecution for defamation, citing international human rights standards, they appear not to have paid attention to the criminal penalties for data processing under PIPA.

Because such absolute control by the individual data subject is presupposed, communication between the civil society and government has been confrontational. Pseudonymisation-backed non-consensual processing, data linkage, and even data portability were deemed encroachments on the individuals' data sovereignty. The past experiences associated with the RRN system only intensified the tension. To civil society groups, pseudonymisation-backed non-consensual processing was deemed dangerous and had to be reined in by the overzealous restriction on re-identification which obliterated data subjects' right of access, and has led to restrictive licensing of data linkage agencies and MyData agencies. This is despite the fact that data portability is in practice a strengthening of data subjects' right of access.

Experts interviewed argued that the goal of data protection law is not to give data subjects control over data about themselves as if they own the data about themselves. The purpose of the data protection law is privacy rather than ownership, and subject consent should be one in many ways to regulate how personal data can be used. These experts added that the real reason for data protection law should actually be other data subjects rights such as the right to inspection, erasure, and objection.[11] For that reason, according to them, GDPR allows five different legal bases for the non-consensual processing of personal data while there are no such broad exemptions on the rights of access, erase/delete and opt-out. However, Korean PIPA allows non-consensual use only along very narrow exceptions while not protecting access and other rights robustly as in the aforementioned case of pseudonymised data.

11 Interview with Jinkyu Lee, Interview with Inho Lee

Such consent-centered data protection law suppresses freedom of speech and social innovations as in the cases of court judgment databases and online whistle-blowing (Park, 2021). Data innovations are not just for economic purposes but can be put to social ends and the pursuit of justice as well. For instance, public access to court judgment databases can enhance the rule of law by strengthening transparency and thereby confidence in the legal system. **Korea's PIPA is, though considered creative and strong, lacking in allowing such use of personal data for social benefit**. GDPR lists five non-consensual bases for processing and one of them is 'public interest'.[12] Korean PIPA does not have such a basis for processing. As a result, a whistle blower on the police's oppressive interrogation tactic was booked for a PIPA violation when the video showing the interrogating officer's face was released to a local TV channel (Choi, 2020; Yoon, 2020). A hospital employee who turned over to the police the video of doctors in surgery rooms for medical fraud was also indicted for a PIPA violation.[13]

At the same time, such consent-centered data protection law allows data controllers to exploit data without substantive data protections simply by obtaining consent from data subjects, often through lengthy terms and conditions. For recent examples, an AI chat app publicly disclosed the information on identifiable data subjects in virtual chats with third parties (Lee, 2021) and the Kakao Map also publicly disclosed the tags that the users created on different locations (Kim, 2021). Both apps' first line of defense was that the data subjects consented to such use and disclosure on the terms and conditions produced at the time of collecting the data. **In all, the focus on individual control and consent both allows PIPA to be used to suppress civil freedoms and absolves data controllers of responsibility for maintaining standards of privacy**.

12 GDPR, Article 6 (1) (e) "[when] the processing is necessary for carrying out a task in public interest"

13 Seoul Eastern District Court, 2020. 7.9 decision, 2019no1842.

Case 2

E-health and Contact Tracing

A goal of the Moon administration is to develop South Korea into a thriving medical innovation hub through the use of big data in the health and medical industry. Various ministries are involved in this initiative, including the Ministry of Health and Welfare, the Ministry of Science and ICT and the Ministry of Trade, Industry and Energy.

In 2018, the government revealed plans to build a bio database for medical big data comprised of the genetic and biometric data of 10 million patients in collaboration with six major hospitals and players in the bio and healthcare sector to develop new solutions and products. One example application is a biosensor that can be installed in cars to detect unusual health symptoms in drivers, alerting necessary emergency services where necessary. (Bae, 2018) The government also announced that by 2029, it would want to collect the medical information of one million cancer and rare incurable disease patients and their families, and non-patients, to better understand the causes of these diseases, and develop personally customized novel drugs as well as new medical technologies (Seo & Lee, 2019).

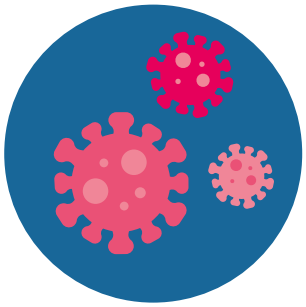
In order to promote public medical big data and health information exchange, there is also a concerted effort to integrate public health data with other public data such as population census data, household income and expenditure survey data from Statistics Korea; as well as birth- and death-related data from the Ministry of the Interior and Safety. Through this initiative, the government aims to promote the use of data among South Korean researchers, similar to processes already in place in the United Kingdom and Canada (Kim et al., 2018).

However, a key concern that has risen from these initiatives is the use of data for the purpose of ARS. As discussed in the earlier section, civil society actors are concerned about the use of citizens' data for for-profit research. They had argued that the non-consensual use of personal data can only be justified for research that can contribute to the expansion of society's knowledge.

A medical doctor interviewed for the study emphasised that the goal for researchers is to improve their field of study, and doing so requires access to data.[14] As such, he suggested that in discussing the use of medical data, stakeholders should think about the value and benefit that such data could bring in order to improve the medical industry in South Korea. Within the medical sector, Seoul National University Hospital's Big Data Review Board, for instance, began accepting requests for enormous amounts of patient data accumulated in a consortium of hospitals for big data research such as deep learning visual recognition of diseases using 250,000 breast X-ray images and 1,200 CT scan images in 2015 (Lee & Park, 2019).

There is also a concern regarding data privacy risks associated with a large amount of compiled health and medical data. There have been cases of data leakage in governmental health databases, with individuals receiving disciplinary sanctions for illegally browsing personal information and a reported case of a medical information programming company illegally extracting patients' clinical and prescription data and selling the data to a multinational firm (Kim et al., 2018).

Appropriate safeguards to protect the data against loss, theft and data leakages should be put in place. These could include detailed rules and procedures regarding data pseudonymisation and setting up procedures to grant access to data, as well as monitoring how such data is being used should be put in place (Lee et al., 2019).



COVID-19

While a pandemic can be disruptive, it can also introduce conditions that will spark innovations. This is especially so in the context of healthcare and disaster response, as these areas impact the well-being of people in a very direct manner. Innovations developed in these areas can also enhance the impacts of the private sector without adversely sanctioning innovations emerging from it (Park, 2015; 2016).

Existing systems of disaster response have focused on building platforms to integrate various data in real time. In these systems judgements and decisions about how to respond are mostly left up to human agents. Due to increased complexities of disasters, there is very limited time available for human decision makers to conduct their evaluations. As such, **system-based disaster response and prediction that are highly reliable and based on credible real-time unstructured data has become essential**. However, a system that connects and analyzes various data such as complex human gene data, disease symptom and treatment data, and correlations between diseases, can also **encounter many limitations due to data privacy, making it different from other scientific areas**. As such, legal developments are much needed to look into how data can be shared by and between researchers and medical institutions.

COVID-19 may have provided the impetus as well as context to address the gap in data sharing in healthcare and disaster response. A distinguishing feature of South Korea's approach to dealing with the COVID-19 outbreak is identifying and notifying residents who might have been exposed to patients.

14 Interview with Byung Joo Park

This contact tracing system was built in the wake of the 2015 Middle East Respiratory Syndrome outbreak that infected 186 people and killed 36 others in the country. Laws were then revised to allow the government to use cell phone data, credit card histories and surveillance cameras to track infected patients. For example, in South Korea, most private and public sector organizations are required to comply with the PIPA. However, under the infectious disease regulations, government agencies are permitted to obtain and use personal data non-consensually for contact tracing purposes. Arguably, this exception allowed the government to curb its once-raging COVID-19 outbreak by affording exceptionally precise contact-tracing by health authorities – to collect, process and widely disclose personal data for public health preservation.

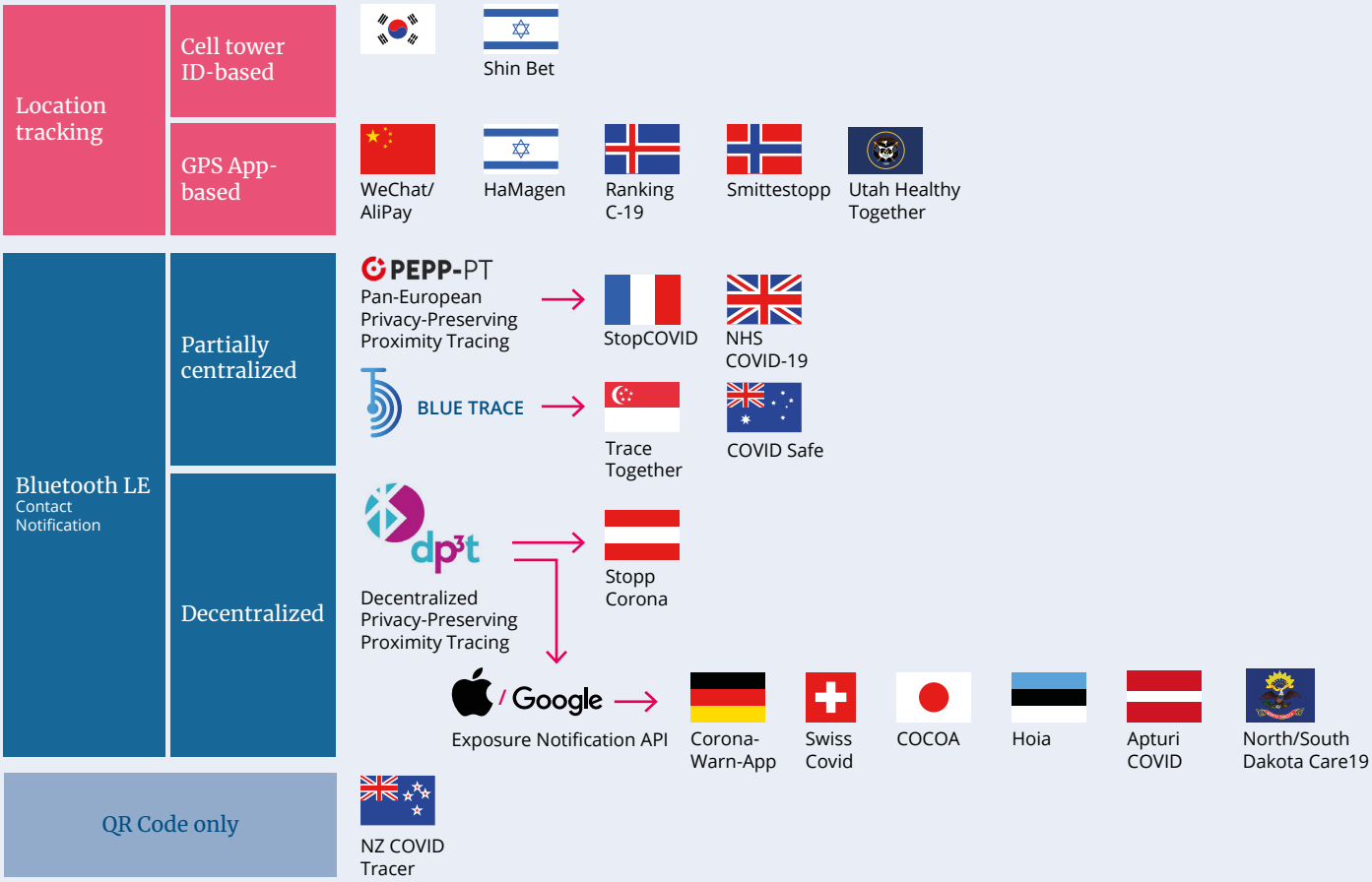
In South Korea, most private and public sector organizations are required to comply with the PIPA. However, under the infectious disease regulations, government agencies are permitted to obtain and use personal data non-consensually for contact tracing purposes.

Authorities were allowed to not only track the location of patients against patients' will but to also acquire locations of an almost indiscriminately large number of individuals in order to identify and notify who were simply in the vicinity of patients. As an illustration, when authorities found out that a COVID-19 patient had visited a nightclub in the city's clubbing hotspot, they conducted a cell tower search and identified about 10,000 phones that were in the same area as the patient for more than 30 minutes. A SMS text was then sent to those identified numbers overnight, requesting that they get tested for the virus (Scott & Park, 2021).

The number of testing done per capita is not very high in South Korea compared to other countries. It is through the above described identification of contacts by mass location tracking (different from the location-tracking of patients) that that the government could direct their testing resources toward the people with relatively higher risk. (Park, 2020)

There are contact tracing efforts in other countries but such methods often require the consent of users because of privacy concerns, i.e. citizens must download apps to notify contacts of their conditions and be notified about contacts' conditions. Therefore, the efficacy of such methods depends on individuals' willingness to comply with voluntary contact tracing and adopting tracking apps. There are two challenges associated with this voluntary contact tracing approach: The first is that, naturally, owing to concerns about data privacy, response to such measures is typically lukewarm. Second, for individuals who do not agree to data-based contact tracing, or tracking apps, effective contact tracing becomes difficult, whether to verify the locations (whether relative or absolute) of COVID-19 cases, or to quickly notify individuals who may have been in close contact with those infected.

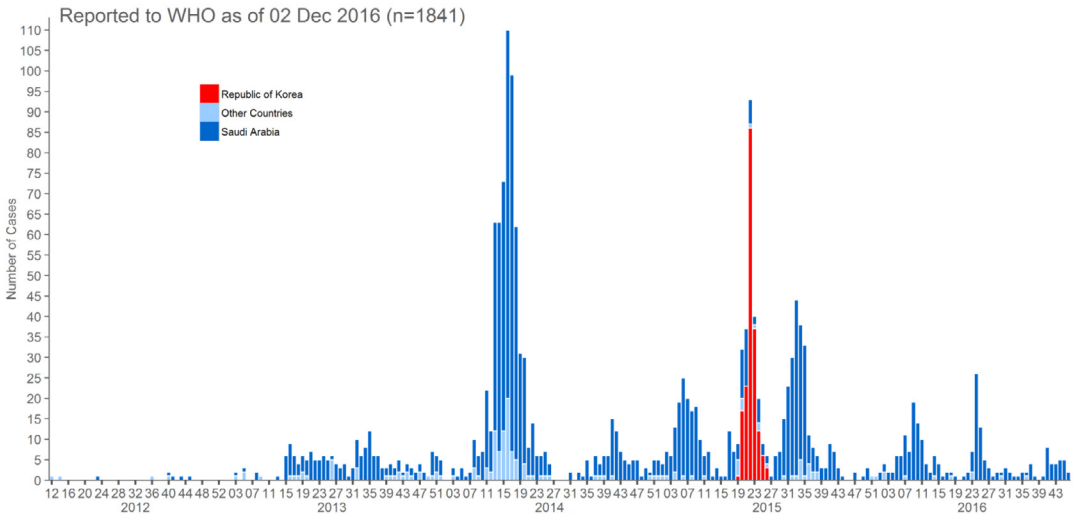
Figure 1: Overview of location tracking methods in different countries



Source: Sang-Chul Park, Tracing and sharing of patient itineraries: domestic and international evaluation (이동경로 추적 공개: 국내외 법적평가), Presentation at the Webinar "ICT-based Responses to COVID and Privacy" (COVID-19 에 대한 ICT 기반 대응과 프라이버시) on June 25 2020: https://youtu.be/36D84HFIdHc (Korean only) Modified/translated by KS Park

As depicted in figure 1, **South Korea and Israel are the only countries that instituted mandatory location tracking** (at least for all those carrying mobile phones) using cell-phone location information, and its efficacy was noted early on (Servick, 2020). All other countries' location tracking are based on the apps that people need to download to be part of the contact tracing system. However, Israel's mobile phone tracking system was recently shut down by the decision of the Supreme Court, which argued against the legitimacy of the programme in April 2020. It resumed for only 3 weeks in July (Altshuler & Hershkowitz, 2020).

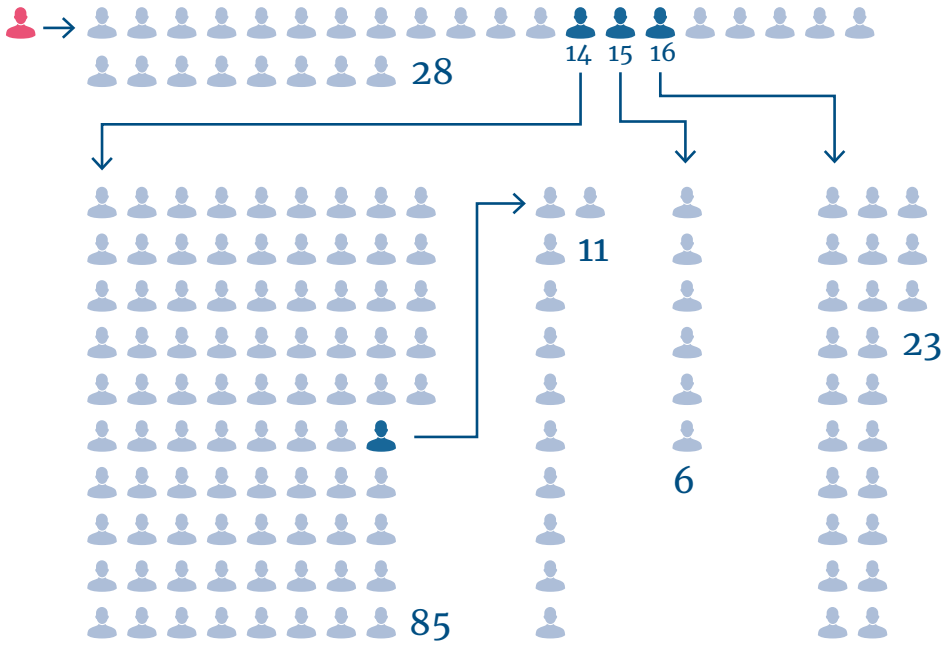
Figure 2 WHO MERS-CoV Global Summary and risk assessment
Confirmed global cases of MERS-CoV



Source: 5 December 2016, WHO/MERS/RA/16.1, World Health Organization

The reason for the uniquely mandatory nature of Korea's contact tracing arose out of her experience with MERS patients 5 years before COVID-19 hit. As you can see in the figure 2, Korea was the only country that suffered substantially from MERS outside Saudi Arabia.

Figure 3: Spread of MERS: Five Super-Transmitters infected 153 out of 186, 82.5%



Source: Korean Society of Infectious Diseases', White Paper on Chronicles of MERS, June 2017, p. 25

As you can see in figure 3, out of the total of 186 patients, Patients No. 1, 14, 15, 16, and 76 infected 28, 6, 85, 23, and 11 people respectively (82.5%). What is more important, each of the four "super-spreaders" lied about their whereabouts when they came to the hospital with symptoms. No. 1 omitted his trip to Saudi Arabia (the original epicenter of MERS) and No. 14 and 16 their respective visits to the hospital where No. 1 was treated and thereby infected others. No. 76 lied about her visits to the hospital where No. 14 had been treated (Kim, 2015). In addition, No. 35 who had attended a 1,500-people meeting and a 300-people conference was in high-publicity altercation with authorities on when symptoms first appeared and he should have quarantined instead of going to these meetings (Koo, 2015). The new law allowing mandatory tracking was passed on July 6, 2015 in order to respond to this 'dishonest' patients problem that caused infection of 79% of the total MERS patients and it is the very law that activated the massive mandatory contact tracing for COVID 5 years later.

The new law allowing mandatory tracking was passed on July 6, 2015 in order to respond to this 'dishonest' patients problem that caused infection of 79% of the total MERS patients and it is the very law that activated the massive mandatory contact tracing for COVID 5 years later.

Yet, there were serious privacy concerns with regards to South Korea's mandatory contact tracing, with much attention focused on the public disclosure of the movements of an infected patient. Most of the media and policy attention on privacy concerns have been on public disclosure of the infected person's movements, resulting in the country's National Human Rights Commission's action and the consequent restriction on the scope of information disclosed (Zastrow, 2020). For instance, disclosure of sensitive personal data such a patient's medical conditions, travel history, sexual orientation and private relations have attracted much controversy and debate (Oh, Chang & Jeong, 2020).

To be specific, what appears to have been critical to contact tracing and subsequent targeted testing, is the acquisition by the government of the location data of infected persons and others in close contact, rather than the disclosure thereafter of sensitive personal data (medical conditions, travel history, sexual orientation). (Chan, 2020). Although public disclosure of the patients' movements is supported by 90.3% of the public, only 59% of the respondents actually use the information (Cho, 2020). Nevertheless, despite these concerns, an opinion poll showed that residents approve of the contact tracing system – 90.3% of respondents felt that both acquisition and disclosure of personal information of confirmed patients was appropriate (Cho, 2020).

Given the unprecedented magnitude of the pandemic, there have been theoretical discussions even in other countries that are considering emulating South Korea's contact tracing efforts despite these privacy concerns (Lima and Manancourt, 2020). Such proposals have come from consumer rights advocates (Brookman, personal communication),[15] privacy advocates (Cegłowski, 2020), and even privacy advocates based in

15 Justin Brookman, director of consumer privacy and technology policy for Consumer Reports, interviewed in Lima, supra.

Europe where the General Data Protection Regulation prevails (Schrems, personal communication).[16] The Congressional Research Services, a public policy think tank of the United States Congress, has engaged in legal discussions over the use of mandatory, non-judicial location tracking for COVID-19 mitigation purposes, and pointed out the potential significance of the "special needs" doctrine or the "administrative search" doctrine as a possible constitutional justification (Foster, 2020). Other commentators also agree that the "administrative search" doctrine may justify mandatory location tracking for COVID-19 purposes (Rozenshtein, 2020).

At the same time, a medical doctor interviewed for the study acknowledged that as COVID-19 persists, continued use of personal data is going to be "problematic". He envisioned that in future, the use of personal data for contact tracing could be evaluated on a case-by-case basis. He elaborated that when the outbreak first started, authorities were "desperate to find a way to contain the disease and we were willing to try anything, but once the urgency subsides, people will question if their data is being used for the right purpose or not".

Also, the Korean law was being used in a manner not contemplated in the COVID-19 setting. Originally, the mandatory tracking was to track ascertained patients albeit against their will. But the Korean health authorities used it to identify and notify potential contacts also against their will. It is from this use that a large number of people who were within several kilometers' radius were rounded up to be notified arguably for their own benefit but only at the expense of their private location being submitted to the government (Scott & Park, 2021)

Originally, the mandatory tracking was to track ascertained patients albeit against their will. But the Korean health authorities used it to identify and notify potential contacts also against their will.

In summary, South Korea, with its unique experience of the MERS outbreak punctuated by the "dishonest patients" problem mucking up the contact tracing efforts, instituted the world's only sustained mandatory contact tracing law, which proved to be very effective in activating a massive testing system closely tailored to the subsections of the population with higher risk of exposure. These laws were accepted by the Korean public although privacy concerns remain as to the future use of the data thus accumulated, the overbreadth of the information collected such as credit card records, and finally the use of the law for location-tracking not just patients but location-tracking an overbroad section of the population for simple notification purposes.

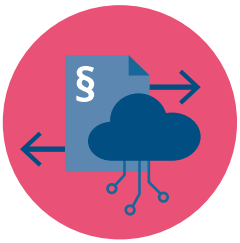
16 Max Schrems, interviewed in Lima, supra.

The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum. On one hand, **the government and industry players desire to exploit the potential of digitalisation and big data for public administration and economic growth**, but in doing so need to consider carefully how to sufficiently protect citizens' data privacy, and what that means in practice, **be it data anonymisation versus pseudonymisation; citizen data 'ownership' or citizen data 'protection'**. It has also underscored the importance of mutual trust between government, industry and citizenry, and how sour relations can impede not only the speed of data innovations, but their eventual, long-term economic and social efficacy as well as sustainability.

The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum.

Legal Regulations

While the Korean state has enacted comprehensive regulations which govern personal data both generally and in specific sectors, the 2020 amendments to the Three Laws of Data eased previous constraints considerably, leading to doubts about the coherence of the laws. One of the key issues that the 2020 amendments brought up was the introduction of the concept of 'pseudonymised data', which came alongside a broadened scope for such data to be processed without the consent of data subjects. Regulations including PIPA and the Credit Information Act then used pseudonymisation as the main basis for allowing exceptional further processing without consent. In other words, unlike the GDPR where certain data protection rights were derogated only in context of socially beneficial processing, Korean regulations derogated the same rights outside the ARS context simply for pseudonymizing the data.



Yet, experts observe that this is inadequate both in principle and in practice – it removes the grand trade-off between relinquishment of data subjects' rights and social benefit arising out of ARS processing. It also hurts both innovation and privacy as pseudonymisation, a technologically privacy-enhancing measure so much so that it strengthens data controllers' claims to non-consensual ARS use, has now become legally a right-depriving process, and a series of legal hurdles were gratuitously created to make pseudonymisation more cumbersome to do.

The regulations also outline the role of third-party data stewards including "data linkage agencies" and "credit information businesses" which are charged with overseeing the processes of data linkage and transferring data related to credit information for portability purposes, respectively. This creates a concentration of personal data in the hands of these data stewards. As observed previously, there are implications for cybersecurity as well as innovation capacity. **The concentration of data in a few entities leads to potential security vulnerabilities, and the power that these entities hold may inhibit innovation by making third parties privy to research agendas and reducing market competition in the credit and finance industries.**

Several concerns about the amended regulations have been raised in this report, but underlying the various technical contentions is a common issue that lies in the social attitudes towards data and relationships between different stakeholders in the country. **There has been a climate of reserve at best and fear at worst in the country.** This stems from the historical use of both data and laws. On one hand, **data punctuated with resident registration numbers have been subject to massive data breaches to the growing discontent of privacy-minded civil society**. On the other hand, **PIPA and other regulations such as defamation laws were used to protect vested political interests while lowering people's trust in big data controllers such as governments**. At the same time, incidents where regulations have been used to protect individual reputations, but not public interest or justice, have set a precedent for a popular focus on individual control and consent in data cultures. In turn, this may have led to the prioritization of pseudonymisation over public interest as a basis for non-consensual processing on the part of policymakers, and a general distrust towards processes like data linkage and any kind of non-consensual data processing on the part of data subjects and civil society. The amendments have further consolidated the amount of control data subjects have over their own data.

At present, a confrontational and mutually suspicious relationship between civil society, the state, and other data controllers has thus arisen which inhibits the formation of regulations that strike an optimal balance between facilitating data processing for innovation and public good, and protecting the rights and agency of data subjects. **The challenge ahead is for government and industry to engage the citizenry to communicate clarity on trade-offs required, which will be beneficial in trust-building, and to encourage citizens to believe in the social benefits accrued.** One mode of building trust is for the results of innovation research based on non-consensual data use, to be justified through the public publication of research results.

Part of this work also involves teasing apart legal quandaries and loopholes to ensure clarity, transparency and fairness among all involved. For instance, it is especially necessary to specify if data protection implies an approach to data that is based on ownership or privacy, both of which produce different outcomes.

Data Innovations in the Time of COVID-19

The case study of the COVID-19 pandemic in South Korea illustrates an extent of support for non-consensual data processing for the common good of public health. Contact tracing has been the most significant and scrutinized example of the use of data in efforts to respond to the pandemic. Despite the measure of advocacy for more stringent data protection laws and against the perceived relaxation of policies with the 2020 amendments, there seems to be less local resistance against the extensive surveillance that in many other countries would be considered excessively invasive. This would suggest that the majority of citizens consider public interest a significant reason for data processing, even if it is extensive and non-consensual.

Pushback against mandatory location tracking, such as from data privacy advocates, remains fairly muted, especially as such tracking remains legal under South Korean law (Open Net Association, 2020). Since PIPA allows non-consensual processing specifically authorized in other laws, such mandatory location tracking is technically permissible. However, more research is needed on why even the citizens who support strong data protection laws are not pushing back on invasive disease

surveillance. One speculation has to do with South Koreans' collectivist orientation and perception of communal risk: In risky situations such as the COVID-19 pandemic, South Koreans – at least compared to individuals in countries like the US, may have a heightened perception of social benefits borne from location tracking measures, and lowered concerns over personal data privacy (Kim & Kwan, 2021). Further research is in need to find out whether, in the calculus of balancing between public interest and privacy, it is the strong perception of public interest or the less concern with the privacy that may have allowed the uniquely mandatory contact tracing of Korea. One of the reasons that the US, the early vortex of COVID-19 outbreak, did not even consider mandatory contact tracking is because racial minorities' deep seated distrust of the police and law enforcement on surveillance. Therefore, **if it is people's trust of surveillance authorities that underlies Korea's successful contact tracing efforts, we will know what other countries must do to replicate the success.**

In risky situations such as the COVID-19 pandemic, South Koreans – at least compared to individuals in countries like the US, may have a heightened perception of social benefits borne from location tracking measures, and lowered concerns over personal data privacy.

At the same time, however, the state of public crisis should not excuse the establishment of unbridled state power to collect and personal data exceeding what is necessary, especially since this may set a precedent for data cultures beyond specific emergencies. **It is thus significant that guidelines or policies be set in place restricting the breadth of these powers to ensure that personal data is controlled and processed by impartial entities, and that non-consensual processing is limited to instances that are justifiable for public benefit.** The system of contact tracing, in particular, suffers from grave privacy problems which need to be addressed such as the broad scope of information that is collected and disseminated, including credit card records and medical records, and the fact that data is collected through the police. Also, mandatory contact tracing is used not just for tracing the itineraries of confirmed patients but for determining the locations of an indiscriminate number of people just to identify who to notify, and such use was not even contemplated by the legislators of the MERS-triggered law 5 years ago. Effective mandatory contact tracing was allowed by the broad trust that people gave to the health authorities.

Cautious discussion still needs to be held in in order to tease apart legal and regulatory quandaries (e.g., PIPA vs. GDPR), to ensure that citizen rights are sufficiently preserved in the course of innovative pursuits. Such discussions should also be carried out by country, not least because different contexts would present differences in perception of data innovation, how liberal or restrictive data privacy regulations are and should be, and sensitivity to data breaches. The COVID-19 pandemic may have necessitated a shift in the balance in the case of South Korea's contact tracing system, but looking forward, the post-COVID era will necessitate serious discussion on whether or not rights can be compromised towards publicly desirable ends, and what that means in practice – and in writing.

REFERENCES

A **Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (Network Act). Act No. 16021.** (2020).

Altshuler, T. S., & Hershkowitz, R. A. (2020, July 6). How Israel's COVID-19 mass surveillance operation works. *Brookings Tech Stream*. Retrieved from https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/.

B **Bae, H.s-J.** (2018, February 9). Korea to build database for medical big data. *The Korea Herald*. Retrieved from http://www.theinvestor.co.kr/view.php?ud=20180209000809.

Bundesdatenschutzgesetz (BDSG). (2019). Bundesministerium der Justiz und für Verbraucherschutz.

C **Cegłowski, M.** (2020, March 23). *We need a massive surveillance program*. Idle Words. Blog post. Retrieved from https://idlewords.com/2020/03/we_need_a_massive_surveillance_program.htm.

Chan, H. (2020, March 26). Pervasive personal data collection at the heart of South Korea's COVID-19 success may not translate. *Thomson Reuters.* Retrieved from https://blogs.thomsonreuters.com/answerson/south-korea-covid-19-data-privacy.

Charles Katz v. United States (1967). 389 U. S. 347.

Cho, S. (2020, May 18). 90% of users of patients' itineraries find personal data disclosure "appropriate" (확진자 동선지도 이용자 90% "개인정보 공개 적절했다"). *Yonhap News Agency*. Retrieved from https://www.yna.co.kr/view/AKR20200518072400017.

Choi, S.-J. (2020, November 9). Data Protection must be balanced with human rights and public interest. *Korean Bar Association.* Retrieved from http://news.koreanbar.or.kr/news/articleView.html?idxno=22418.

Credit Information Use and Protection Act 1995. Act No. 16188 (2020).

E **European Data Protection Supervisor** (2020, January 6). A Preliminary Opinion on Data Protection and Scientific Research. Retrieved from https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf.

F **Foster, M. A.** (2020). *COVID-19, Digital Surveillance, and Privacy: Fourth Amendment Considerations.* Congressional Research Services. Retrieved from https://crsreports.congress.gov/product/pdf/LSB/LSB10449.

G **Government of the Republic of Korea** (n.d.). *100 policy tasks*. Five-year plan of the Moon Jae-In Administration.

H **Haggard, S. and You, J.-S.** (2014). Freedom of expression in South Korea. Journal of Contemporary Asia, 45(1), pp. 167–179.

Hintze, M. and El Emam, K. (2019, January 29). *Does anonymization or deidentification require consent under GDPR?* IAPP. Retrieved from https://iapp.org/.news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/.

I **Information Commissioner's Office** (n.d.). What are the conditions for processing? *Information Commissioner's Office*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/.

J **Jun, W.** (2020). A Study on the Current Status and Improvement of the Digital Divide among Older People in Korea. *International Journal of Environmental Research and Public Health*, 17(11), 3917–3930. https://doi.org/10.3390/ijerph17113917.

K **Kim, D.** (2020, January 15). 'My Data' Changes Financial Topology – Customizing all my financial transactions (내 모든 금융거래 분석해 맞춤 서비스…'마이데이터'가 금융지형 바꾼다). *INews24*. Retrieved from http://www.inews24.com/view/1235990.

Kim, D.-H. (7 January 2020). Moon puts top priority on innovation to boost growth. *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20200107006600320.

Kim, H. (2021, 15 January). Kakao Map faces user data leak dispute. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20210115000801.

Kim, H., Kim, S. Y., & Joly, Y. (2018). South Korea: In the midst of a privacy reform centered on data sharing. *Human Genetics*, 137, pp. 637–635.

Kim, J.-H. (2017, November 9). 12 civil society organizations file criminal complaints against agencies and companies for unauthorized linkage of databases. *Kyunghyang Shinmun*. Retrieved from http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201711091626001.

Kim, J.-O. (2014, June 9). MERS massacre born of lies. *CBS No Cut News*. Retrieved from https://www.nocutnews.co.kr/news/4425249.

Kim, J. (2020, July 14). K-New Deal: South Korea to invest $133bn in digital, green sectors. *Nikkei Asia*. Retrieved from https://asia.nikkei.com/Economy/K-New-Deal-South-Korea-to-invest-133bn-in-digital-green-sectors.

Kim, J., & Kwan, M. P. (2021). An Examination of People's Privacy Concerns, Perceptions of Social Benefits, and Acceptance of COVID-19 Mitigation Measures That Harness Location Information: A Comparative Study of the US and South Korea. *ISPRS International Journal of Geo-Information*, 10(1), 25. https://doi.org/10.3390/ijgi10010025.

Kim, Y.-C. (2020, September 6). Regulator set to announce winners of MyData business. *The Korea Times*. Retrieved from http://www.koreatimes.co.kr/www/nation/2020/09/367_295375.html.

Koo, Y.-H. (2015, June 15). Seven Unforgettable MERS Patients. *CBS No Cut News*. Retrieved from https://www.nocutnews.co.kr/news/4428522.

Korea Information Society Development Institute (2020). 2020 ICT Industry Outlook of Korea. Retrieved from http://www.kisdi.re.kr/kisdi/common/download?flag=mobile&type=D&file=GPK_RND_DATA%7C34050%7C2#:~:text=Strengths%20and%20weaknesses%20in%20Korea's,highlighted%20to%20seek%20improvement%20opportunities.&text=ICT%20exports%20in%202020%20are,year%20to%20USD%20188.5%20billion.

Lee. D., Park, M., Chang, S., & Ko, H. (2019). Protecting and utilizing health and medical big data: Policy perspectives from Korea. *Healthcare Informatics Research*, 25(4), 239–247. https://doi.org/10.4258/hir.2019.25.4.239.

L

Lee, H.-J. (2020, June 3). Over 100 companies express interest in MyData services. *Korea JoongAng Daily*. Retrieved from https://koreajoongangdaily.joins.com/2020/06/04/business/finance/mydata-FSC-innovation/20200604023525477.html?detailWord=.

Lee, M. (2019). *Data protection in the age of big data in the Republic of Korea*. Global Information Society Watch 2019: Artificial intelligence: Human rights, social justice and development. Retrieved from https://giswatch.org/node/6187.

Lee, S.-G. (2019, February 25). Court Judgments and other Big Data Essential for AI Legal Services. *Korea Legal Times.* Retrieved from https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=150966.

Lee, S. M., & Park, C. M. (2019). Application of artificial intelligence in lung cancer screening. *Journal of the Korean Society of Radiology*, 80(5), 872–879. https://doi.org/10.3348/jksr.2019.80.5.872.

Lee, W. (2021, January 13). *South Korean AI developer shuts down chatbot following privacy violation probe*. mLex. Retrieved from https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-korean-ai-developer-shuts-down-chatbot-following-privacy-violation-probe.

Lim, D. (2018, August 20). Local governments have disclosed public data for 5 years. Need to increase usage. *ETNews*. Retrieved from https://www.etnews.com/20180820000187.

Lima, C. & Manancourt, V. (2020, April 5). Privacy agenda threatened in West's virus fight. *Politico*. Retrieved from https://www.politico.eu/article/privacy-agenda-threatened-in-wests-virus-fight/.

National Information Society Agency (2018). *National Informatization White Paper*. National Information Society Agency.

N **Newsis** (2021, February 9). Civil society sue SKT calling for stop on pseudonymisation. *Newsis*. Retrieved from https://newsis.com/view/?id=NISX20210209_0001335395&cid=13001.

Oh, B.-I., Chang, Y., & Jeong, S. H. (2020). COVID-19 and the right to privacy: *An analysis of South Korean Experiences*. Association for Progressive Communications. Retrieved from https://www.apc.org/sites/default/files/Covid_19_and_the_right_to_Privacy_an_analysis_of_South_Korean_Experiences.pdf.

O **Personal Information Protection Act 2011. Act no. 16930** (2020).

Park, Kyung Sin (2014). *Paradox of Trust: Korean Resident Registration Numbers*. Open Net Korea. Retrieved from http://opennetkorea.org/en/wp/920.

P **Park, Kyung Sin** (2017). *Criminal Defamation and Insult Prosecutions in South Korea*. Open Net Korea. Retrieved from http://opennetkorea.org/en/wp/2127.

Park, Kyung Sin (2021). *March 2021 Letter to European Commission and European Data Protection Supervisor on Korea's GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions.* Retrieved from http://opennetkorea.org/en/wp/3239.

Park, S.-U. and Park, M.-S. (2019). Toward a Policy for the Big Data-Based Social Problem-Solving Ecosystem: the Korean Context. *Asian Journal of Innovation and Policy.* 8(1), pp. 58–72.

Park, Kyung Sin (2020). *Korea's COVID19 Success and Mandatory Phone Tracking. Open Net Korea*. Retrieved from http://opennetkorea.org/en/wp/3142 and also a presentation made at Social Science Research Council(SSRC)'s Public Health, Surveillance, and Human Rights Network on July 21, 2020 (the completed paper of the PHSHR network available at https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/).

Park, Kyung Sin (2021). Data as public goods or private properties?: A way out of conflict between data protection and free speech, UC Irvine *Journal of International, Transnational, and Comparative Law,* 6 (77), available at https://scholarship.law.uci.edu/ucijil/vol6/iss1/5.

Rosenberg, E. B. (2019, January 18). *I-Korea 4.0: Moon Jae-In's strategy to bring South Korea into a new digital era*. LinkedIn. Retrieved from https://www.linkedin.com/pulse/i-korea-40-moon-jae-ins-strategy-bring-south-korea-new-rosenberg.

R **Rozenshtein, A. Z.** (2020). *Disease Surveillance and the Fourth Amendment.* Lawfare. Retrieved from https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment.

Scott, M. & Park, J. M. (2021, April 19). South Korea's Covid-19 success story started with failure: The inside account of how one country built a system to defeat the pandemic. *Vox*. Retrieved from https://www.vox.com/22380161/south-korea-covid-19-coronavirus-pandemic-contact-tracing-testing.

S

Servick, K. (2020, March 22). Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? *Science*. Retrieved from https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price.

Seo, J.-W., & Lee, E.-J. (2019, May 22). S. Korea to build medical big data highway to foster bio health sector. *Pulse by Maell Business News Korea.* Retrieved from https://pulsenews.co.kr/view.php?sc=30800025&year=2019&no=338336.

Sohn, J. A. (2017). President emphasizes 'people-centered' fourth industrial revolution'. *Korea.net.* Retrieved from https://www.korea.net/NewsFocus/policies/view?articleId=149973.

Sung, J.-W. (2020, September 2). Big Brother wants to know what's for lunch. *Korea JoongAng Daily*. Retrieved from https://koreajoongangdaily.joins.com/2020/09/02/business/finance/data-credit-information-customer-data/20200902160257670.html?detailWord=.

Sweeney, L, & Yoo J. S. (2015). De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data. *Technology Science.* Retrieved from https://techscience.org/a/2015092901.

T **The Economist Intelligence Unit** (2016). *Connecting Capabilities: The Asian Digital Transformation Index.* The Economist Intelligence Unit. Retrieved from http://connectedfuture.economist.com/connecting-capabilities/article/connecting-capabilities.

The Korea Herald (2014, March 24). [Editorial] 'Galapagos regulation': Korea's online payment system needs reform. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20140325000577.

Y **Yonhap News Agency** (2020, March 5). Digital divide still high in S. Korea. *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20200305004400320.

Yang, W.-M. (2019, July 26). Prosecutors exonerate use of deidentified data. Will it open floodgate of data usage? *footnote: Boan News*. Retrieved from https://www.boannews.com/media/view.asp?idx=81801&kind=2.

Yoon, W. S. (2020, August 9). 모자이크 없이 경찰 강압수사 영상 제보한 변호사 기소의견 송치. Retrieved from https://www.yna.co.kr/view/AKR20200908053100004.

Z **Zastrow, M.** (2020, March 18). South Korea is reporting intimate details of COVID-19 cases: has it helped?. *Nature*. Retrieved from https://www.nature.com/articles/d41586-020-00740-y/.

Sample of Questions

Semi-structured interviews were conducted with questions broadly aligned with three themes:

1. How the regulation of data affects innovative capacities
2. Data cultures, or perceptions around data and innovation
3. How data creates value or values

A sample of questions for each theme follows:

Regulation	• To what extent do you think the laws and regulations around data protection have been helping or hindering the innovation capabilities of firms and organisations? • Do you see the legal landscape, as in the laws and regulations in specific, or the legal framework, changing in the next few years? • How can the current laws and regulations, including the legal framework, be improved so that the innovation capabilities of organisations can be further enhanced?
Data cultures	• How is personal data seen in Korea? For example, do people see it as something that they need to protect? Or as byproducts of economic transactions? • How might perceptions of personal data and privacy have an impact on innovation? For example, what types of data would be considered taboo to share, and in what contexts?
Data and value creation	• What do you think is the value that organisations bring when they are successful in managing their data, including analysing, storing, protecting, and sharing their data? • How do you think frameworks like the GDPR affect domestic and trans-border operations, and to what extent do you think a similar framework would be feasible in Korea?

Methodology

8 interviews

This project adopted a case study approach, with data collected from semi-structured expert interviews and published documents. A total of eight interviews were conducted with various experts, ranging from academics, lawyers and representatives from internet companies. A content analysis on twenty selected documents such as press releases and public consultation papers was also conducted, where the documents were coded according to themes such as value associated with data, principles of data governance and partnerships in data sharing.

20 relevant documents

AUTHORS

Kyung Sin Park is a Professor at the Korea University School of Law, and co-founder and Executive Director of Open Net Korea (www.opennetkorea.org), a not-for-profit organization that aims to provide a platform for discussion and collaboration to explore effective policies and solutions to facilitate freedom and openness of South Korea's internet. He has written academically and been active in areas such as net neutrality, web accessibility, digital innovation, and open data.

Dr Natalie Pang is a scholar of digital humanities, specializing in socio-technical studies of technology including social media and civil society and the convergence of data and AI in urban cities.

We would like to thank all expert interviewees who have been generous in sharing their time and insights on the topic. All interviewees and their affiliations have been anonymised, as guided by the approved ethical guidelines of this project.

Editors
Christian Echle
Director Regional Programme Political Dialoge Asia
christian.echle@kas.de

Katharina Naumann
Programme Manager for Digitalisation
katharina.naumann@kas.de

Konrad-Adenauer-Stiftung e. V.
Regional Programme Political Dialogue Asia
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
www.kas.de/singapore

Imprint

Published by:
Konrad Adenauer Stiftung Regional Programme
Political Dialogue Asia, Singapore, 2021

Design and typesetting: yellow too Pasiek Horntrich GbR

Printed with financial support from the German Federal Government.

ISBN 978-3-95721-796-7

Data fuels digital change. The ability to collect, process, and make available ever-increasing amounts of data is a key to innovation and growth.

This report is one of the series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates about data governance and data protection. The study was carried out in collaboration with the National University of Singapore (NUS). We selected Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health and smart cities to understand how innovation is driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

This report examines the key developments in data policy and innovation in South Korea, focusing on the domains of regulations, namely the "Three Laws of Data", and e-health during the COVID-19 pandemic period. The case of South Korea shows the importance of careful consideration of what it means to balance data innovation with privacy, and the trade-offs on either side of the spectrum.

Konrad-Adenauer-Stiftung e. V.

DATA AND INNOVATION IN ASIA-PACIFIC