CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

FEBRUARY 2024

Korea's Path to Digital Leadership

How Seoul Can Lead on Standards and Standardization

Evan A. Feigenbaum and Michael R. Nelson, editors
Dasom Lee | Byoung-il Oh | Kenji Kushida | Elina Noor

Korea's Path to Digital Leadership

How Seoul Can Lead on Standards and Standardization

Evan A. Feigenbaum and Michael R. Nelson, editors
Dasom Lee | Byoung-il Oh | Kenji Kushida | Elina Noor

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Project Participants

The volume's editors are grateful to the participants in a virtual workshop on "Korea, Standards, and Standardization," and they are especially appreciative of those who offered helpful comments on chapter drafts. They also express thanks to the Korea Foundation for its generous support of this project and to Carnegie's Alex Taylor and Sarah Camacho for their support of this volume.

D. Linda Garcia
Communication, Culture & Technology Program, Georgetown University

Paul Hofheinz
Lisbon Council

Mallory Knodel
Center for Democracy & Technology

Robert Pepper
Meta

Jun Takei
Intel Corporation

Irving Wladawsky-Berger
Sloan School of Management, Massachusetts Institute of Technology

Naomi Wilson
Information Technology Industry Council

Summary

Strategic competition among big powers, especially between the United States and China, is leading to the securitization of economies and technologies. Increasingly, Washington and, to a lesser extent, Brussels view Chinese dominance of commercial technologies as a national security threat. They therefore aim to exclude Chinese systems from their economies and leverage intergovernmental and private sector bodies to preclude Beijing and Chinese companies from setting global standards for technologies and business processes. That has led many policymakers to refract global standard setting through the prism of competition between China and its strategic rivals, with commercial and technological competition framed in predominantly geopolitical terms.

But the United States, China, and Europe are not the only players in standards and standardization. A host of other players have joined them, not least in setting standards for the emerging digital economy. And these other players do not necessarily share their securitized approach to technology governance.

In many cases, national regulators and local firms in these other countries are setting homegrown standards for their markets while resisting pressure to adopt or assimilate either Western or Chinese standards. In some cases, these countries are themselves becoming pacesetters, with the potential to export and scale homegrown standards as their companies' share of global business expands and their role as technological innovators grows.

Instead of viewing standards and standardization merely as arenas for Western strategic competition with Beijing, it is essential to look at how these additional and increasingly significant players are evolving into de facto standard setters.

This volume digs into South Korea's experiences with standards and standardization in the digital arena and draws attention to Korea's distinctive digital policy. It then compares Korea's experiences to those of the United States and other Asian players, notably Malaysia and Japan. It is the third in a series of volumes by the Carnegie Endowment for International Peace on Korea as a technological and digital pacesetter.

INTRODUCTION

Korea, Standard Setting, and the Digital Transformation

Evan A. Feigenbaum and Michael R. Nelson

Strategic competition among big powers, especially between the United States and China, is leading to the securitization of economies and technologies. Increasingly, Washington and, to a lesser extent, Brussels view Chinese dominance of commercial technologies as a national security threat. They therefore aim to exclude Chinese systems from their economies and leverage intergovernmental and private sector bodies to preclude Beijing and Chinese companies from setting global standards for technologies and business processes. That has led many policymakers to refract global standard setting through the prism of competition between China and its strategic rivals, with commercial and technological competition framed in predominantly geopolitical terms.

But the United States, China, and Europe are not the only players in standards and standardization. A host of other players have joined them, not least in setting standards for the emerging digital economy. And these other players do not necessarily share their securitized approach to technology governance.

There has been a proliferation of models for technology governance, as these other countries develop their own experiences and practices. In many cases, national regulators and local firms are setting homegrown standards for their markets while resisting pressure to adopt or assimilate either Western or Chinese standards. In some areas, these other countries are themselves becoming pacesetters, with the potential to export and scale homegrown standards as their companies' share of global business expands and their role as technological innovators grows.

Instead of viewing standards and standardization merely as arenas for Western strategic competition with Beijing, it is essential to look at how these additional and increasingly significant players are evolving into de facto standard setters.

South Korea (hereafter Korea) is both a critical and understudied player in the standards and standardization game. With world-class, globally competitive companies and a nearly $1.7 trillion economy—the thirteenth largest in the world and the fourth largest in Asia—Korea has shown a willingness to develop homegrown standards.[1]

This volume digs into these Korean experiences and then compares them to those of other Asian players, notably Malaysia and Japan. It is the third in a series of volumes by the Carnegie Endowment for International Peace on Korea as a technological and digital pacesetter.

The first of these Carnegie volumes, *The Korean Way With Data,* illustrated how Seoul has tried to craft coherent and consistent policies in three important areas related to data: (1) online authentication and data access control, (2) cyber defense and data resilience, and (3) data localization.[2]

The second volume, *Data Governance, Asian Alternatives*, rejected the notion that a stark contest between democracy and autocracy will shape the governance of technology and data.[3] It showed how two Asian democracies, India and Korea, are carving out distinctive paths on data policy, not just following Western or Chinese models.

The purpose of this third volume, *Korea's Path to Digital Leadership*, is to explore how Korea is adopting homegrown standards, creating norms and business processes, and setting policies that will shape how the internet, online applications, and cloud computing grow and evolve, both in Korea and around the world. The volume then compares what is happening in Korea with developments in Japan, Malaysia, and the United States.

Korea's Progress

Michael R. Nelson opens the volume by asking several framing questions about digital leadership. He urges leaders to push for consensus within governments and industry and describes eleven particularly thorny challenges that many governments—in developed and developing countries—are trying to address:

1. Connecting the unconnected
2. Broadband competition
3. Encryption
4. Cybersecurity of government systems
5. Cybersecurity of nongovernment systems

6. Digital identity
7. Content moderation
8. Data localization
9. Data architecture
10. Data protection
11. Online copyright

These eleven categories provide the policy framework for report cards to grade various countries' progress in digital policy in the remaining chapters.

Two chapters from Korean authors then comprise the core of the volume. They evaluate the strengths and weaknesses of Seoul's national digital policies.

First, Dasom Lee's chapter dives deeply into four case studies, showing how government agencies in Seoul and Korean corporations play an increasingly important role in international standard setting and the adoption of standards. Lee arrives at four key conclusions.

- **Heightened attention to standards bodies**: Over the past two or three decades, as Korean information and communications technology (ICT) companies have grown to become world leaders, they have devoted much more attention to international standards bodies.
- **Growing focus on setting specific standards**: In addition to sending more employees to staff international standards bodies, these Korean firms also have devoted much more attention to shaping which standards are adopted.
- **Greater involvement of the private sector**: While government agencies have been the most important players in standards development in Korea in the past and continue to serve this role in many sectors, in a growing range of areas Korean firms and CEOs are having a direct impact in the standards arena.
- **Increased emphasis on profiting from new standards**: There are many examples of past Korean efforts to use national standards to protect home markets and favor domestic companies. More recently, Korean companies have pushed for an approach that leverages the development of international standards to ensure that they are among the first to adopt and profit from new standards and business processes.

The second Korea-focused chapter, by Byoung-il Oh, offers an extensive report card to help grade Korea's progress. His primary focus is on two of the ten categories—data protection and data architecture—areas where Oh has provided many years of insights and leadership.

He uses these subjects as proxies for gauging Korean standard setting in a range of areas: encryption, cybersecurity of government systems, digital identity, and content moderation. He adds another category, the regulation of artificial intelligence, but he assigns both Korean government and industry actors a grade of C.

When Oh's assessments of Korea's progress are combined with those of the Korean contributors to Carnegie's two previous volumes on Korean digital policy, their contributions collectively form a combined report card (see table 1).

Table 1. Report Card on Digital Leadership in Korea

Key Digital Issues	Letter Grade	Notes
Connecting the unconnected	A	
Broadband competition	C	Grade is falling.[4]
Encryption	B	
Cybersecurity of government systems	F	
Cybersecurity of nongovernment systems	C	Grade is improving.[5]
Digital identity	C	Grade for the past twenty-plus years, with recent improvements.[6]
Content moderation	C	
Data localization	B[7]	
Data architecture	B	
Data protection	B	
Regulation of artificial intelligence	C	

Note: A = superior, B = above average, C = average, F = failing, I = incomplete. The grades only indicate how well or poorly the government is doing in various areas; they cannot be used to compare a country's performance with that of other countries.

Korea in Comparative Context

The next three chapters compare Korea's experiences to those of three other countries: Malaysia, Japan, and the United States.

The chapter on Malaysia, from Carnegie scholar Elina Noor, examines a country whose experiences with standard setting are quite analogous to Korea's experiences. According to the International Telecommunication Union's latest ICT development index, Malaysia is somewhat more advanced than Korea in several aspects of digital development.[8] In addition, Malaysia's population is roughly twice that of Korea. Noor concisely justifies the grades she has assigned in each of the following categories, and she adds a twelfth category, digital inclusion (see table 2).

Table 2. Report Card on Digital Leadership in Malaysia

Key Digital Issues	Letter Grade
Connecting the unconnected	A
Broadband competition	B
Encryption	C
Cybersecurity of government systems	F
Cybersecurity of nongovernment systems	C/F
Digital identity	I
Content moderation	C
Data localization	B
Data architecture	C/I
Data protection	I
Online copyright	B
Digital inclusion	C

The chapter on Japan from Carnegie's Kenji Kushida explores how the government in Tokyo and the Japanese private sector are embracing various aspects of the digital transformation while the country is lagging considerably as an international standard setter. Kushida notes prior Japanese failures when setting its own information technology–related standards, arguing that when Tokyo sought to do so in some areas, this had the perverse effect of isolating Japan's domestic market from global competition. Japanese companies ended up being less competitive in global markets, so Japan today aims to correct these failures by assimilating

international standards rather than setting its own in ways that might isolate the country's firms and attenuate their competitiveness. Kushida grades Japan in nine categories (see table 3).

Table 3. Report Card on Digital Leadership in Japan

Key Digital Issues	Letter Grade	Notes
Connecting the unconnected	A	
Broadband competition	A	
Encryption	I	
Cybersecurity of government systems	C	Improving overall, with an A in some areas and an F in others.
Cybersecurity of nongovernment systems	C	An A in some areas and an F in others.
Digital identity	B	
Content moderation	C	
Data localization	A	

The next chapter, by Michael R. Nelson, covers American digital policy, an especially difficult task for at least two reasons. First, there are many U.S. players involved, including the courts and state legislatures. Second, within each policy category, there are problems that are being addressed but not always addressed very well. Worse, over the last thirty years, successive administrations have varied significantly in their priorities.

Nelson is, ultimately, an easier grader than some of the other authors (particularly Oh). This is one reason why these report cards can only be used to identify strengths and weaknesses on digital policy within each country but cannot be used to conclude that one country is doing better than another. Though other digital policy experts might use different metrics, Nelson grades the United States this way (see table 4).

Table 4. Report Card on Digital Leadership in the United States

Key Digital Issues	Letter Grade	Notes
Connecting the unconnected	A	
Broadband competition	B	
Encryption	C	
Cybersecurity of government systems	B	
Cybersecurity of nongovernment systems	A	
Digital identity	C	
Content moderation	C	
Data localization	A	Grade is falling.
Data architecture	B	
Data protection	I	
Online copyright	C	

Digital Leadership Matters

Ultimately, digital policy and standards are shaping both business and warfare in increasingly unpredictable, exciting, and international ways. So it is clear that nations will, and should, seek to adopt policies and encourage standards that yield world-leading technology companies; foster a fiercely competitive race between those companies to develop the most innovative products and services; give those companies an advantage in global markets; spur the development of a large and talented tech workforce; and empower users and companies by collecting, protecting, and sharing the data needed for exciting new tools, including big data and machine-learning applications.

Those that succeed will be the winners in the global economy and on the battlefield—as they seek to attain peace through prosperity and deterrence through digital power. This Carnegie volume will hopefully help Korea and other countries achieve these goals.

In most countries, the largest barriers to progress in digital policy are political inertia, fear of the future, and bureaucratic fights among government agencies. This volume aims to bring attention to Korea's distinctive experiences on digital policy, but its broader lessons in digital leadership can show how to ensure that relevant actions lead to effective implementation.

CHAPTER 1

Standards, Standardization, and Digital Leadership: Thorny Questions in Tech Policy

Michael R. Nelson

Today, the news is full of stories about breakthroughs in artificial intelligence (AI) and how governments are struggling to make sense of the powerful tools it enables. While Brussels and Washington are drafting laws to fix AI, they are failing to address far more fundamental policy issues that will shape the digital transformation we are living through. Some countries, including South Korea and India, are taking a more comprehensive approach to digital policy making, which could (if done right) better position them to realize the full benefits of emerging technologies (whatever they may be).

I have been working on digital policy for more than thirty-five years. And during that time, whether I was in government, the private sector, or academia, I have been guided by a mantra we used when I worked with former U.S. vice president Al Gore in the White House in the 1990s: "First, do no harm." That is the Hippocratic Oath, the famous oath that doctors take, but we applied it to the internet as well. Since then, I have been trying to stop stupid stuff that could hinder the development of the internet and limit its potential.

Fortunately, I was not alone. A lot of people—particularly in the technical community—worked hard to make sure innovators and internet users had lots of room to find new ways to use the net, the web, and the cloud. We faced a lot of critical decisions about technology standards, online censorship, privacy and cybersecurity, e-government and e-commerce, and more. And, at least in some countries—like India, Japan, South Korea, and the United States—most of the time policymakers made the right choices. That enabled the internet to grow from fewer than a million users in the early 1990s to more than half the world's population today. In the United States, these policy choices also enabled the growth of the first trillion-dollar companies. And they enabled the growth of e-business, videoconferencing,

global digital libraries, and access to almost unlimited amounts of music, movies, and culture. Those applications are now providing the data that powers exciting new big data and AI applications.

But today, unfortunately, a lot of people in government, in the corporate sector, and in advocacy groups are promoting proposals that would limit what the internet and the cloud could become. Often, they are doing it for good reasons (like protecting children online or tracking down terrorists). In other cases, CEOs and politicians are trying to limit what we can do with the internet for selfish, profit-driven reasons. They propose simple-sounding laws or regulations that could have all sorts of complex, unintended, and harmful effects.

While most of the news coverage about governments trying to shape how digital technologies can be used focuses on law, regulation, and court cases, this is only part of the picture. For more than thirty years, groups like the Internet Engineering Task Force, the World Wide Web Consortium, and the Institute of Electrical and Electronics Engineers have been writing technical standards that enable devices, networks, and applications to work and work together. As new problems and new opportunities develop, these groups and their members hash out new standards. Sometimes, they restrict what is possible online. More often, they allow developers and users to build safer, more secure, more powerful, and more interoperable systems and applications.

Governments and intergovernmental organizations (such as the United Nations' International Telecommunication Union) can shape these standards and decide which ones are widely adopted by influencing government procurement decisions and by adopting legislation calling upon tech companies to fix problems policymakers (and their constituents) are concerned about (such as online privacy). To distinguish these efforts from standards-setting, I refer to this process as "standardization," following the lead of Carl Cargill, who has been studying and shaping how standards are made and which ones are adopted for more than thirty years.[9] Too often, government officials say they want one single standard to solve a potential problem posed by digital technologies. Such an approach often restricts innovation that might lead to better solutions in the future. Worse, by endorsing one approach over others, imposing a single standard can often favor one company (or a handful of companies) over others, dramatically limiting competition in the market. When politicians refer to "standards," they often would be better off using the term "standardization." Usually, they are not trying to design technology. Instead, they often really want a consensus (sometimes informal) about what responsible companies and users should do with a given tool or technology. The end users should be empowered to take different approaches (and rely on different products and services, which are built around different standards) to satisfy government-suggested goals.

A very successful example that has had a huge impact around the world is the U.S. National Institute of Standards and Technology's Cybersecurity Framework.[10] It does not impose a single set of standards for building more secure systems. Instead, it outlines a wide range of issues and technical problems that information technology (IT) companies—and the

companies that buy and use their products and services—need to address. Then, it provides pointers to information and groups that could help them do so. In that way, the framework provides a great deal of flexibility to tailor solutions to the constraints and needs of each organization.

It is important to realize that standardization is not just about technology standards. It also describes business processes and norms that shape how organizations operate and how their employees work. For instance, the framework stresses the need to have policies and procedures in place in order to quickly and effectively respond to cyber attacks.

Smart governments understand the full range of tools they have for shaping and accelerating the digital transformation—and avoiding negative, unintended consequences when adopting new, imperfect technologies. These tools include not just legislation and regulation but also government procurement decisions, the "bully pulpit" (political leaders and their staff speaking loudly and clearly about policy problems that need to be addressed), funding research and testbeds to find and demonstrate new tools and techniques, and norms on how new technologies should be designed and used.

In a handful of countries, some politicians understand at a deep level the opportunities and at least some of the serious problems posed by emerging digital technologies. And in an even smaller number of countries, such leaders put forward effective, coordinated approaches to address the promise and the perils technologies pose. Their secret? Something I call "digital leadership."

In contrast, in too many countries, politicians pretend that technology can do the impossible. They think they just need to tell the techies and the entrepreneurs to "nerd harder." For instance, it makes no sense for data protection authorities to tell companies to limit how much data they collect and how long they keep it for and, at the same time, punish those companies when they retain data that law enforcement agencies demand. Nor is it logical to urge small businesses to use state-of-the-art cloud-based services so they can better compete for global markets—and then limit cross-border data flows. Leaders have to choose which policy goals to pursue.

Digital leadership usually comes from presidents or prime ministers who can put the needs of their countries' citizens above the narrower needs of individual agencies or pressure groups. That will often help with finding new approaches, better models, and effective metaphors. Most importantly, it will require political leaders who face up to the real choices that must be made. In India, Prime Minister Narendra Modi has invested his personal time and energy to promote solutions to thorny problems like digital authentication and data protection. Even before his election in 2017, former president Moon Jae-in of South Korea had identified digital policy as a key area. During the campaign he made digital authentication a campaign issue,[11] and he made good progress during his presidency.

There are dozens of digital issues and hundreds of proposals (good and bad) that policymakers have offered. But here I outline the few thorny questions that stand out as most important and most contentious and, in some cases, suggest new approaches. Most importantly, I will briefly explain what could happen if we make the wrong choices. Each of these topics is an urgent problem that requires deep analysis, new thinking, and rapid (but well-considered) action. In later chapters, contributors will assess how countries like South Korea, Malaysia, Japan, and the United States are doing and how much "digital leadership" they have demonstrated in each area. By comparing and contrasting these countries' successes (and failures), we hope to inform digital policy makers in other countries as well.

So, what are the thorniest questions and why are they so hard to answer?

1. Connecting the unconnected
2. Broadband competition
3. Encryption
4. Cybersecurity of government systems
5. Cybersecurity of nongovernment systems
6. Digital identity
7. Content moderation
8. Data localization
9. Data architecture
10. Data protection
11. Online copyright

Connecting the Unconnected

With hundreds of millions of new people working or learning from home due to the coronavirus, internet traffic surged by 30 percent, 40 percent, or even more in some markets.[12] In the United States and many other countries, internet service providers (ISPs) have been able to meet the increase in demand. But, in some countries, primarily those where incumbent telecommunication companies are still heavily regulated like the monopolies they used to be, investment has lagged, and customers in less densely populated areas have lacked the bandwidth needed for video conferencing or streaming services. Or their options have been too expensive.

Depending upon the choices governments make, I see three possible outcomes:

1. Provide subsidies to a handful of big, incumbent phone companies and cable companies.

2. Target subsidies to poor or rural internet users who currently cannot access the benefits of the internet and the cloud.

3. Continue to try a different approach every few years, resulting in perverse incentives, market distortions, and discouragement for innovators and investors who might have a better way to connect the unconnected.

Broadband Competition

One of the most effective ways for governments to promote better, more widespread, more reliable, and more affordable broadband access (both wired and wireless) is by enabling the development of more competition in the telecommunications sector. Unfortunately, some of the government subsidy programs that have helped make the internet more affordable favored only a portion of ISPs. That has often made it harder for new competitors with new technologies (such as satellite internet companies) to compete against subsidized incumbents.

A few countries, such as South Korea, have gone so far as to enact regulations that mandate that smaller network providers pay the dominant telecommunication companies an interconnection fee (set by the government) for each megabyte of data they send to customers of the incumbents.[13] The European Union first considered such an approach more than ten years ago. It was rejected wholeheartedly by national telecommunication regulators in Europe. Despite that (and the obvious failure of the South Korean policy), Thierry Breton, the European commissioner for internal market (and a former CEO of the French telecom company Orange), has been pushing hard for a similar "sender pays" model.[14] This policy would upend the business model of the internet that has served users around the world—and enabled its explosive growth—for more than twenty-five years. Not surprisingly, a large cross section of tech companies (in Europe, Korea, and elsewhere) oppose this government-mandated subsidy system.[15]

Encryption

One of the hardest digital issues I have ever worked on is controls on encryption. This was the first issue Gore assigned to a small team of us when I showed up to work at the White House in January 1993. Thirty years later, policymakers are still struggling to address it.

For more than twenty years, policymakers have faced three options (and most have chosen the third):

1. Promote end-to-end encryption for all data everywhere.

2. Limit encryption so law enforcement and other government agencies can track users' activities online.

3. Pursue both goals at the same time and keep arguing.

What happens if they do not choose? If individuals and companies cannot trust that their data is fully protected, they will be unlikely to fully trust (and thus adopt) new cloud and Internet of Things applications. We may never know what opportunities we would miss. But we do know that hackers would prosper. A paper from the Carnegie Encryption Working Group highlights why this is so important.[16]

Cybersecurity of Government Systems

The challenges of securing government systems are widely known: rapidly evolving technology, lack of adequate funding to hire the best IT talent and build state-of-the-art systems, difficulties in getting different parts of government to cooperate, and, of course, bureaucratic turf fights about who will be in charge and how much power and budget they will have. But at least there is broad consensus on what needs to be done—and, in most countries, there is growing alarm about how vulnerable governments' IT systems can be. This is clearly an area where top-level leadership (and pressure) from the office of the president or prime minister can make a difference.

Cybersecurity of Nongovernment Systems

In many developed countries, the situation is different (and worse) for IT systems in most commercial and nonprofit organizations. That is less true in banking and financial services, which are recognized as a model for other sectors—yet major data breaches and scams, affecting millions of bank and credit card customers at a time, still occur often. One way that digital leadership from presidents and prime ministers could make a difference regards surveillance. Ideally, cyber defenses would get better and better—and do so faster than the skills of malicious hackers and nation-states' cyber warriors. Unfortunately, intelligence agencies find it easier to exploit vulnerable, buggy systems. The U.K. government has even gone as far as to recently propose legislation to limit how and when IT companies can fix vulnerabilities that are found.[17] Such limits provide de facto "back doors" for surveillance by intelligence agencies and law enforcement. In a royal form of digital leadership, King Charles III endorsed the legislation in his 2023 King's Speech. Unfortunately, in many countries the debates between supporters of making surveillance easier and advocates for better cybersecurity are happening out of the public eye.

Digital Identity

Many countries are promoting digital identity systems to enable e-government services, support online banking, prevent online fraud, and protect against cyber attacks. Estonia and India have been leaders in implementing and promoting their online authentication systems. But will users trust such services if privacy is not built in?

I think there are four possible outcomes:

1. Digital identity systems are designed to ensure the privacy of users.

2. Government-controlled digital identity systems allow governments to monitor most transactions online.

3. Digital identity will be designed by corporations that want to monitor transactions online.

4. There will be competing systems that cannot interoperate and that have different standards and procedures, leading to confusion, lack of trust, and limited adoption.

Content Moderation (and/or Censorship)

Everyone agrees that the internet has had a profound impact on the more than 1 billion people around the world who use it regularly. Certainly, one of the most powerful ways it has changed our lives is by enabling us to access—and contribute to—the ever-expanding corpus of new content and online services. Unfortunately, some of that content is unwanted, misleading, manipulative, and even dangerous or deadly. Governments have focused much of their attention on social media companies and news media websites, but dealing with unwanted or harmful content extends to other types of online services (such as gaming and messaging services, among others).

This issue is global, although much of the news reporting focuses on legislation and regulation in the European Union (particularly the Digital Services Act), the United States (and the debate over Section 230 of the Communications Decency Act), India, and China. In the United States, the issue has been particularly emotional and complex because of the inherent conflict between the free speech protections in the First Amendment and the desire of policymakers and their constituents (especially parents) to limit the spread of harmful content. One result has been dozens of high-profile congressional hearings with tech CEOs and representatives of various advocacy groups. At the same time, until legislatures and parliaments act, battles are being fought out in the courts—at the state, provincial, and federal levels.

There will never be a globally agreed-upon set of criteria for what is "acceptable speech" and what online platforms should block. Cultures vary too much, and so do governments. However, it is possible that individual internet users could be provided with better tools and information to tailor or filter the services they and their families use—and new companies might find ways to better meet the desire of consumers to get the content and services they want. There is clearly a market demand.

Data Localization and the Splinternet

The magic of the internet has been its global, interoperable nature. A small startup in one country with a new idea can build a web application, and within months millions of people in almost every country can be using it.

However, in recent years more governments have sought to limit how and when foreign platforms and online service providers collect data about their citizens. In some cases, the services are simply blocked, but in other cases governments choose to allow access to the websites while insisting that user data is not exported.

These concerns extend well beyond consumer websites to include business-to-business online services as well as data routinely collected by transnational companies (about their employees as well as their customers). As the Internet of Things and cloud computing expand into every sector of the economy, the amount of data, the velocity with which data move across borders, and the number of ways in which they are used will increase dramatically.

The G7 countries have committed at the highest level to "data free flow with trust"[18]—but each country is struggling to explain what that really means and what limits on that ideal make sense. Other countries, such as India, are drafting data protection legislation and regulations that could change policy in very significant ways. In India and other countries eager to compete globally, policymakers need to consider consumer privacy, protection of confidential corporate information, national security, competition, trade agreements, the need to enable local IT companies to serve the global market, and much more. Too often, the result has been ambiguous and conflicting policy requirements promoted by different agencies and ministries to meet the often conflicting needs of different stakeholders.

The possible outcomes are in stark contrast:

1. Maintain the global internet where every app works everywhere.

2. Fragment the internet. Follow China's or India's model and block hundreds of foreign apps and websites. Limit the use of global cloud-based services in many sectors. The end result would be so-called national "splinternets" rather than a single, global internet.

Data Architecture

One of the most overlooked (and yet essential) standards and policy issues involves data governance. How can governments design systems, promote business practices, and craft policies that lead to the development of interconnected databases that can be tapped to solve both government and business problems—while providing the data protection that citizens expect?[19] Estonia was a pioneer in doing this for government data. India's answer to this challenge, the India Stack, is much more ambitious because of its much greater scale.[20] The India Stack incorporates a proposed Data Empowerment and Protection Architecture, intended to provide access to both government and commercial data. If the Indian government can succeed (even partially), it will stimulate a wide range of new applications from Indian companies and their partners, especially in the area of big data and machine learning.

Data Protection

In most countries, data protection and content moderation are the two most emotional digital policy challenges. The coronavirus crisis showed why. People like privacy. But China, Israel, South Korea, Taiwan, and other countries showed how cell phone location data could be used to track and slow the spread of the coronavirus. Somehow, we need to recognize that more and more sensitive data are going to be collected—and that such data are needed to address a growing number of societal problems. Using the cloud, the Internet of Things, and machine learning to collect and analyze terabytes of data can generate jobs and save lives—if we find ways to revamp privacy laws and business practices.

The choices:

1. Enforce stricter limits on what data can be collected and why.

2. Allow more businesses and governments to find ways to scoop up, combine, and abuse the data being generated about us.

3. Create new transparency requirements (in law and in contracts) that tell smartphone and app users exactly what data are being collected, why, and how they will be protected. New approaches and business models like data unions, data cooperatives, and data spaces could enable more data collection for more uses with enhanced privacy.

Online Copyright

Since the start of the coronavirus crisis, the shift for workers in developed countries to "living online"—virtual doctor's visits, shopping online, connecting with friends—has been easier than most people imagined. But, in some cases, old laws are getting in the way of

new approaches. Copyright provides one obvious example. I should be able to play a video I own with my friends using a videoconferencing platform without paying twice. Zoom is not a radio station or a TV station, so Zoom users should not have to pay the same copyright fees that traditional entertainment networks do.[21] When it comes to online copyright, the current model and mindset need to change. Somehow, government policy needs to draw a clearer line between private and public—and between abuse and the fair use of copyrighted material. But these tough choices should be made by legislatures, not by courts, where a series of different judges make different interpretations of how copyright applies in the virtual world.[22]

Possible outcomes:

1. Every use of copyrighted material will be monitored, and fair use will almost disappear.

2. More and more content online will be public domain (like Wikipedia).

3. More and more owners of copyrighted material will find new business models that do not require copyright filters, watermarking, or other copyright markers.

Conclusion

I am a pathological optimist—or perhaps just a delusional utopian—when it comes to technology. But, after spending more than thirty-five years in Washington, DC, I know how politics and self-interest can get in the way of progress. My hope is that at least a few countries will have political leaders who will provide the digital leadership needed to find real and effective answers to the thorny questions examined above and that other countries will pay attention and do the same. The leadership of smaller countries, like Estonia, Israel, and Singapore, have a lot to teach us. Other countries, including Japan and India, have leaders trying to lead by example at the G7 and the G20. But we do not have the luxury of time.

My dream is that politicians everywhere will adopt former president Bill Clinton's White House mantra and strive to "First, do no harm." And I hope they will realize that the four keys to effective digital policy are competition, innovation, transparency, and empathy. Call them the CITE goals. Then leaders will be able to craft clear, consistent policies that their citizens need—policies that give users informed choices and encourage companies to think of customers first. Let us hope government can shape technologies and policies to meet these goals. Let us design a cyber civilization that will work for our children and their children.

CHAPTER 2

The Role of South Korea's Private Sector in Setting Technology Standards

Dasom Lee

South Korea has been a leader in technology innovation for more than two decades, particularly in the areas of telecommunications, consumer electronics, and automobiles. Over that period, the country's participation in international technology standardization processes has grown. Many Korean organizations and corporate leaders joined and now actively participate in the International Electrotechnical Commission, the International Organization for Standardization (ISO), and the United Nations' International Telecommunication Union (ITU).

Considering Korea's importance in global digital development, the country's private sector should consider ways to increase its impact on technology standard-setting processes. This chapter uses case studies to examine the two primary ways by which Korean companies engage in setting international technology standards: 1) by industry and corporate leaders taking on positions of influence and 2) by participating in standard-setting workshops and seminars with other stakeholders. Both of these approaches allow private corporate actors to represent their industries and their companies' interests as well as communicate the latest trends related to technology development and the market.

Technology Standard Setting and South Korea

Technology Standard Setting

International standard-setting processes involve a number of stakeholders, including national governments, international organizations, private sector organizations, development aid agencies, and consumers. The ISO, composed of 167 national standards bodies, is the

leading international standards organization.[23] Its General Assembly has the authority to enact standards based on reports written by the ISO Council.

There are a number of different types of standards, including those related to categorization, infrastructural development and maintenance, and innovation. Standards also address a range of issues, such as road safety, medical packaging, and environmental protection.[24]

Standards have played a major role in shaping the development of emerging technologies.[25] These standards not only define technologies; they also shape how they are used. For instance, the World Bank defines technology standards for identity systems as those that relate to "the hardware, software, and platform involved in most technical aspects of the identity lifecycle, including creating and proofing identities, issuing credentials, authentication of identities, and the interoperability with other databases."[26]

Technology standards differ from business norms and practices because they are considered to be international regulations that must be met in order to sell and distribute goods around the world in a safe and responsible manner. They offer significant advantages by facilitating coordination among interested parties as they establish broad agreement on specific technologies. Particularly in the digital arena, the increasing pace of innovation has triggered more technology standard-setting activities.[27]

Korea's Role in New and Emerging Technologies

Korea is considered one of the world's most innovative nations.[28] The Bloomberg Innovation Index has ranked Korea as the most innovative country for seven out of the nine years that the index has been published.[29] The World Intellectual Property Organization's Global Innovation Index 2022 ranked the country sixth in the world and first in Southeast Asia, East Asia, and Oceania.[30] In the latter index, Korea ranked particularly high in human capital and research (ranked first) and knowledge and creative outputs (ranked fourth). The Korean city Daejeon is one of the world's top three most research-intensive science and technology clusters.[31] Similarly, the Organisation for Economic Co-operation and Development (OECD) has described Korea as a "global powerhouse in science and technology," and it has one of the world's most advanced digital economies. The country has been named as one of the leaders in the information and communication technology (ICT) sector due to its high broadband penetration, fiber-optic connections, and 5G commercial subscriptions.[32] Furthermore, Korea has used these ICT connections to implement infrastructural innovations such as collecting traffic data and building smart cities.[33]

The South Korean Ministry of Science and ICT announced in September 2022 that the country's future technological developments will focus on six areas: artificial intelligence (AI), AI semiconductors, 5G and 6G communication, quantum, metaverse, and cybersecurity. The ministry also said that there will be continued partnerships between the public sector and the private sector to support and harness human capital in the era of digitalization.[34]

Standard Setting in Korea

Although Korea is home to many top technology companies, it has only recently emerged as a leader in the development of global technology standards. For decades, the United States, Japan, and several European countries have played more high-profile roles in standard setting—a trend that is changing. In 2023, for example, Sung Hwan Cho, the president of Hyundai Mobis, was elected president of the ISO. Cho will serve as the first Korean president of the ISO in 2024–2025.[35]

Both the Korean government and the private sector could help establish or revise the country's industry standards. Relevant government organizations, such as the Korean Agency for Technology and Standards (KATS),[36] could initiate the process for Korea to adhere to international standards for new and emerging technologies. KATS could hire associations or research institutes to draft standards for specific technologies and/or industries. Relevant stakeholders could propose the establishment or revision of standards at any time.[37]

Once the initiation process starts, relevant government ministries and administration teams could evaluate the standards to determine whether there are any discrepancies in the application and use of the proposed standards. Additionally, a public hearing could be organized to discuss all stakeholders' opinions. If any stakeholder requested a public hearing in writing, the president of KATS would be required to hold such a hearing. Here, the relevant stakeholders include research institutes, teaching institutes, technology producers, government actors, international stakeholders, and consumers.[38]

For technology-specific standard setting, the Industrial Standard Review Committee[39] must submit proposed standards to the relevant technical review committee,[40] which is composed of experts in each field. If it is deemed necessary, the standard proposal may be submitted to the specialized committee for further evaluation.[41]

Case Studies

Although the technology standard-setting process in Korea is largely led by the government, the private sector plays an important role by participating in workshops and being involved in international processes. The four case studies in this section showcase how private Korean companies have been involved in technology standard-setting processes. They include one consumer-oriented technology, namely the 5G mobile network, and three infrastructural technologies: smart meters, smart grids, and automated vehicles.

5G: A Consumer-Oriented Technology Case Study

Consumer-oriented technologies are directly marketed toward and used by consumers rather than businesses or governments. Consequently, they directly reflect consumers' needs and wants and, compared to infrastructural technologies, are more sensitive to market demands. Because the transition toward digitalization has rapidly accelerated, especially after the COVID-19 pandemic,[42] consumers may not have a deep understanding of consumer-oriented technologies. It is therefore critical that technology standards protect consumers' safety and privacy and address other related societal concerns.

Enabled by its superfast broadband internet infrastructure and high smartphone penetration, Korea was the first country to adopt 5G, in April 2019, making 5G an ideal case study for this chapter. 5G is particularly relevant in showcasing Korea's importance in the global standard-setting scene because it, along with China, has been leading the standard-setting efforts for 5G. In 2013, Yoon Jong-iok, then vice minister of the Ministry of Science and ICT, stated that Korea and China were poised to lead the global research and development (R&D) effort to standardize 5G networks because of their large, fresh market opportunities as well as their dense populations in cities.[43] Indeed, the Korea Information Society Development Institute found that Korea's investment in R&D for ICT was ranked first among the largest twenty-four OECD countries in 2019.[44]

Even before 5G networks were introduced, Korea was leading the mobile telecommunications network race. One of the most notable inventions was WiBro, created by Samsung Electronics and the Electronics and Telecommunications Research Institute (ETRI) in 2004. With a speed of 50 megabits per second, it was faster than 3G mobile networks and was considered the technology that would shape the future of communications. In 2006, WiBro was commercialized by KT and SK Telecom, the two largest telecommunications service providers in Korea. That was five years before LTE was developed in 2011. But WiBro was eventually deemed unsuccessful for three reasons: there were few services on the internet that required such speeds at that time, there was a limited number of WiBro devices, and coverage was incomplete.[45]

Since then, private companies in Korea have continued to play active roles in the development and commercialization of new communications technologies. The most contemporary telecommunications service is 5G, which is used by half of all Koreans and accounts for 33 percent of mobile communication subscriptions and 72 percent of overall online traffic.[46] 5G uses 3.5 gigahertz band for consumer use and 28 gigahertz band for industry use, such as in factories, government agencies, hospitals, and schools. It follows the international standards established by the ITU and the Third Generation Partnership Project (3GPP).[47] The ITU introduces service scenarios and requirements, and the 3GPP meets those requirements through technology and infrastructural developments.

In Korea, a number of organizations have been involved in the development of 5G standards, including government actors (for instance, the Ministry of Science and ICT, the National Radio Research Agency, and the Korea Institute of S&T Evaluation and Planning) and research organizations (for instance, the Telecommunications Technology Association, the Korea Radio Promotion Association, and the 5G Forum Korea). These organizations collaborate with international standards organizations to promote global standards harmonization, technology testing, and maintenance, as well as to address international standards within the Korean market.[48]

Critical to the standard-setting process is the way that private companies select standards to adopt and promote. A 2020 report by Strategy Analytics documented corporations' contributions to 5G standardization through the 3GPP.[49] The report focused on various metrics: the number of 5G-related papers, such as submitted papers and approved/agreed papers; chairman positions for all technical specification groups and working groups; and rapporteurs of 5G-related work items and study items for all such groups. It ranked China's Huawei as the company with the most contributions to 5G standardization, while the two Korean companies included were ranked sixth (Samsung Electronics) and eleventh (LG Electronics). Similarly, IPLytics, a German think tank focused on intellectual property, showed that Huawei had the most patents related to the 5G technology in 2021, with Samsung Electronics (ranked second) and LG Electronics (ranked third) following closely behind.[50] In this way, these Korean companies have been playing leading roles not just nationally but also for international standard setting.

Smart Meters, Smart Grids, and Automated Vehicles: Infrastructure-Related Technology Case Studies

Infrastructural technologies, particularly those related to energy and transportation, impact all people, so standards for these technologies have a direct impact on people's safety and well-being. Through sensing, controlling, and networking, smart meters, smart grids, and automated vehicles—the focus of this chapter—communicate not only with consumers but also with each other to provide the most efficient and interoperable environment.[51]

Korea has been leading in some ways and lagging in other ways in the global race for these infrastructural technologies. For smart meters and smart grids, Korea joined the international effort to digitize energy systems early by establishing and developing test beds. (Here, digitization of energy systems refers to using smart technologies such as smart meters and smart grids to maintain, manage, and control supply and demand of energy.) In 2009, the town of Gujwa-eup in Jeju Province became one of the test beds for smart grids.[52] Jeju also hosts a number of self-driving mobility tests. However, because of delays in development of level 3 automated vehicle technology, so far, the results from the test beds have been preliminary.[53]

For automated vehicles, North American and European countries have mostly been at the forefront of creating technology standards, and Korea is only now trying to join as one of the first countries to commercialize level 3 automated vehicle technologies.[54] These infrastructural technologies are good case studies that exhibit the complex role that Korea plays in the global effort to set standards for new and emerging technologies.

Smart Meters and Smart Grids

Smart meters are the interfaces between the electrical grid and a building or a unit; they allow recording and potential monitoring of electricity consumption. Smart grids are electricity networks that use digital technologies to monitor and control the use of electricity and manage its transportation. Both smart meters and smart grids collect data regularly via wireless or wired communication technologies.[55]

The installation of smart meters and smart grids has skyrocketed globally in the past ten years or so, with some countries such as France and Norway making their installation mandatory.[56] Some experimental projects—such as the GridWise Olympic Peninsula Project, the AEP Ohio gridSMART Demonstration Project, and the Pacific Northwest Smart Grid Demonstration Project, all in the United States—have shown the potential benefits of smart meters.[57] These benefits include more efficient or real-time communication between producers and consumers, better and more sustainable grid management, and more consumer control.

Korea has developed its own systems and structures for smart grids and meters that are quite different from other countries'. For Korean apartment blocks, among the most common dwelling arrangements in the country, one smart meter is installed per block that consists of multiple households rather than one smart meter per household.

There are several potential issues around smart grids and smart meters that need to be addressed through standards, particularly privacy and data security. Because smart meters collect data several times an hour to gauge the electricity consumption of each household (or, in Korea's case, each apartment block), they can reveal personally identifying information, such as whether someone is present and their lifestyle, habits, and employment status. One study revealed that, using smart meters, researchers could identify the TV channel that residents were watching.[58] Disclosure or misuse of such information could be a severe privacy and security issue. Smart grids also pose potential security challenges such as hacking and use of malware.

In Korea, forums that involve stakeholder organizations have played a big role for standard setting, including for smart meters and grids. When smart meters were first introduced in the country in the early 2010s, government bodies formed to standardize the technology. The Smart Grid Standardization Forum was one such attempt. It was organized in Jeju in 2010 and convened government bodies such as the Korea Electric Power Corporation

(KEPCO) and Korea Power Exchange; private companies such as SK Telecom, LG Energy Solution, and LS Electric; and scholars.[59] The forum remains active and provides a space for various Korean stakeholders—as well as international standardization players such as the International Electrotechnical Commission, the ISO, the European Telecommunications Standards Institute, and the European Committee for Standardization—to discuss potential social and technological challenges of smart meters and grids.

Some key figures from the private sector have also emerged. The most notable person is Ja-Kyun Koo, the chair of LS Electric and of the Korea Smart Grid Association. That association has been a leader in establishing relevant technology standards for smart meters in Korea and has been involved in developing and establishing various sub-standards regarding national and international smart grid standardization.[60]

Despite Korea's early development of test beds for smart meters and grids, the results have been disappointing. The smart grid project in Jeju was abandoned around 2013 after the organizers realized that without different electricity pricing schemes, the environmental impact would be minimal.[61] Indeed, it has been difficult for private organizations to be readily involved in standardization processes for these technologies because Korea's energy industry is managed by a government agency, KEPCO. The failed Jeju model raised doubts about smart meter technology in Korea; instead of being a global leader for the technology, Korea has taken a step backward.[62]

Automated Vehicles

Another case study involves automated vehicles, also known as autonomous vehicles or self-driving cars. SAE International, a nongovernmental professional association, provides a useful taxonomy to describe the levels of automation and the extent to which automation can change the driving environment and driver behavior.[63] To briefly describe, level 0 refers to vehicles that have no automation technologies, and level 5 refers to vehicles that are fully automated and do not require any human driver interaction. Most technologies that are currently being developed and tested are level 3. Some companies, such as Tesla and Google, are testing level 4 technologies, in which fully automated driving is possible in some situations or environments. SAE International's taxonomy for automated vehicles encompasses several components, including sensors, controls, communication, GPS and mapping, safety, cybersecurity, software platform, infrastructure, and performance.

The ISO is another major actor in international standard-setting processes for automated vehicles. It has developed and published documents on intelligent transport systems' standards for braking, data sharing, and governance principles, among other topics.[64]

The Korean government has been ambitious in its commercialization of automated vehicles. It published a document in 2019 that stated it plans to build the infrastructural and institutional requirements for level 4 automation by 2024 and introduce level 4 automation on major roads by 2027.[65] Considering the global ups and downs in the development of

the technology, this goal could be unrealistic: a recent study found that most people in the industry do not expect to see level 4 vehicles commercially deployed before 2030.[66] However, the document showcases the Korean government's interest in automated vehicles.

Despite this interest, the country has been somewhat lagging on developing standards for automated vehicles. It was California and the Netherlands, for example, that first started testing remote-controlled automated vehicles on public roads. (That technology is not yet allowed to be tested on public roads in Korea.) Many existing standards on the vehicles, such as the level of automation, were developed in countries in North America and Europe.

However, Korean automotive corporations are becoming more daring. For example, Hyundai announced that it would launch level 3 autonomous driving technology some time in 2024.[67] This release would make Hyundai one of the first—if not the first—company to commercialize level 3 automated vehicles to the public. The Korean private sector is therefore expected to play a more global role in this sphere, especially with Hyundai Mobis's Cho becoming the president of the ISO in 2024. In addition, Hyundai Mobis organized an international forum in 2022 with Cho to discuss international automated vehicle standard-setting progress.[68] This event was followed by a workshop in March 2023, which included researchers from several private companies such as Hyundai Mobis, LG Electronics, KT Corporation, Samsung Electronics, and LG Innotek. During the workshop, private sector personnel discussed standards on scenario and data collection, standards for automated vehicle parts, and ideas to support and lead international automated vehicle standards.[69]

The Korean government is also becoming more engaged. KATS hosted an international conference in 2021 to discuss standards for levels of automation for automated vehicles.[70] Furthermore, the Ministry of Land, Infrastructure and Transport has been involved in revising regulations to meet international automated vehicle standards, such as their speed while being tested on public roads, disengagement issues, and alarm systems.[71] ETRI is another main player; it has also been involved in international levels of automation standard setting via SAE International.[72]

Main Takeaways From the Case Studies

Considering the processes of technology standards, it is inevitable that the Korean government will lead. Nevertheless, private companies have not been taking a back seat. The case studies reveal that the private sector has been involved in standard-setting processes in two main ways. The most obvious way is for an industry leader to assume a position that allows some influence over the standards. Cho is the most prominent example. But his term will only last two years starting in 2024. The second way is to have dozens of mid-level technical

experts deeply engaged in writing standards. In the long run, this strategy will have more impact than one top executive devoting a few hours a week to managing a standards organization.

Technology Adoption

Although Korean companies are engaged in setting international technology standards, they play a larger role in promoting the adoption of these standards—particularly by incorporating the standards into new products and services. They often shape the strategies of tech companies and early adopters around the world, which in turn drives development of new standards and highlights issues that need to be addressed.

However, some standards that are adopted and promoted by Korean companies do not succeed. There are often two, three, or more technologies competing during the deployment and adoption phases. In many cases, this is a market-driven process in which private companies take the lead.

Mobile transaction technology is one helpful case study to showcase the factors that can influence technology standard adoption. In early 2015, Samsung acquired LoopPay, which provided an alternative to Apple Pay for non–Apple phone users in the United States.[73] Later that year, using LoopPay technology, Samsung introduced Samsung Pay, which allowed Samsung phone users to purchase goods using debit or credit cards saved on their phones. Since then, Samsung Pay has been enhanced so that it is used for personal identification, digital identification, block chain accounts, student cards, digital car keys, movie tickets, and airplane tickets. In Korea, Samsung Pay is one of the leading mobile payment service providers, ranked third after Naver Pay and Kakao Pay.[74] Although Naver Pay and Kakao Pay have larger market shares, they are different from Samsung Pay because they are software-based companies that use QR codes for payments, whereas Samsung uses its smartphone technology for mobile transactions.

Samsung Pay was successful from the beginning in Korea. Apple Pay, despite being introduced a year before Samsung Pay in the United States, could not be used in Korea until 2023. That is mainly because Apple Pay failed to use near field communication (NFC) technology. In Korea, most mobile payment transactions use magnetic secure transmission (MST) technology. Samsung smartphones have both NFC and MST technologies embedded, but Apple smartphones only support MST. After Apple Pay was introduced in Korea, store owners were required to purchase MST payment devices that cost approximately $120 to $150 to support Apple Pay. Consequently, some small shop owners pushed back against using Apple Pay.[75]

Two questions are then raised: First, why did Apple not adopt MST and NFC like Samsung did? Second, what made Korea's mobile transaction market adopt MST? The answer to the first question is simple: Samsung acquired LoopPay, which invented MST, so Apple did not have access to MST technology.

The answer to the second question is more complex. MST technology, in which a card's magnetic strip is swiped to make a digital payment, has been the foundational technology of credit and debit card purchases in Korea. Because most stores already had a payment device that supported MST, the transition to MST that Samsung Pay adopted was seamless. Around the mid-2010s, there were changes from MST to integrated circuit (IC) cards, which demanded new card readers for many shops. This switch raised the question of whether the new card readers should also have NFC reading functionality. However, due to concerns around cost and accessibility, this idea was shut down, and only IC readers were adopted.[76] The question of added cost regarding the adoption of NFC is still being discussed in Korea. For vendors to be able to use NFC, they must purchase a different card reader. Furthermore, the media reported that Apple Pay's transaction fees are quite high at 0.15 percent per transaction (five times what is charged in China), compared to Samsung, which has no transaction fees.[77]

This competition between MST and NFC was not seen in the United States. Based in the United States, Apple has always been a dominant smartphone brand there. From the beginning, Apple involved a large number of banks in the introduction and rollout of Apple Pay.[78] This contrasts with Korea, where users must have a Hyundai credit card to use Apple Pay.[79]

It was the market that determined the adoption of MST in Korea, and the involved companies played a significant role in the deployment, distribution, and use of the technology. NFC's omission from card readers was not related to technology standards, since the technology standards for NFC had been published in 2003. Instead, it was market adoption that led to wider use of MST transactions.[80] The use of Apple Pay has also been stymied by transaction fees and technology inaccessibility. This case study denotes the importance of socioeconomic factors that drive technology development, distribution, and adoption.

Strategic Leadership and the Korean Private IT Sector

Traditionally, in a market economy, companies' main role has been to produce goods for consumers and profit from sales of those goods. But today, companies are no longer expected to only produce profit—they should also contribute to society through ethical business practices.

The transnational companies that originated in Korea have promoted corporate social responsibility. For example, Samsung has identified "creating shared value" as one of its key concepts in its sustainability reports since 2013, indicating its dedication to environmental

and social sustainability.[81] The company highlights its environmental sustainability programs and employee benefits. Researchers showed that Hyundai has also worked to improve the quality of the lives of marginalized people.[82] For example, in 2023, Hyundai Motors and Kia Motors—which have the same mother company, Hyundai—donated approximately $158 million, surpassing the total donation amount of Samsung Electronics for the first time.[83]

Additionally, Korea has benefited from having millions of eager early adopters willing to experiment with new products and services, and Korean companies have developed techniques for learning from their customers. Tailoring products to customers' needs and concerns is one reason private companies in Korea have produced digital goods that have become wildly popular around the world.

There is an intimate relationship between corporate social responsibility and strategic leadership, defined as the use of assets to achieve organizational and individual goals.[84] For companies to understand the demands of the public and contribute to environmental and social sustainability, strategic leadership—or more specifically digital leadership—must be construed as a key pathway through which these goals can be achieved.[85] Digital leadership not only involves setting standards; it also includes norms of behavior, which affect corporate behavior, processes, culture, and organizational structure. Although their role within Korea is somewhat lacking in standard-setting processes, private companies have been leading and guiding the industry on corporate citizenship and corporate social responsibility.[86]

Conclusion

While the private sector in Korea has produced several international leaders who have taken a top-down approach to setting standards, Korea should also do more to build out bottom-up approaches that involve employees and the public in order for the country to exercise more influence within the international standard-setting community.

The following points may be further discussed to improve the democratic process of technology standard setting in Korea (and elsewhere):

- greater involvement of corporate researchers, developers, and engineers;
- greater involvement of corporate leaders in the international standard-setting scene;
- involvement of the public, especially for consumer-oriented technologies;
- greater transparency of technology standard-setting processes through reports and/or recordings of workshops; and

- opportunities for the public to learn more about standard-setting processes, especially regarding consumer-oriented technologies.

Because new and emerging technologies are now developing at a speed that it is difficult for regulators to match, private standard setting and voluntary standards have become increasingly important, and corporate actors often play a critical role.[87] A deeper discussion on voluntary technology assessments and private standards may be required to further promote the development of safe technologies.

CHAPTER 3

A Digital Policy Report Card for South Korea

Byoung-il Oh

For more than three decades, South Korea has made building its digital sector a high priority. The country is a world leader in semiconductor chip production and has one of the highest broadband penetration rates in the world. The online content available to Koreans is varied, and the country's content industry is competitive and thriving. The International Telecommunication Union's 2023 ICT Development Index ranked Korea eighteenth for digital development overall and twenty-second for connectivity.[88]

Significantly, these rankings were lower than those the country had scored in previous years.[89] Despite being a leader in the global digital economy, Korea is not advancing as rapidly as it had in the past. This is due in part to the government's inability to work effectively with industry leaders and the public to craft clear policies in several key areas. The bad news is that Korea has spent decades trying to sort out thorny issues like online authentication. The good news is that President Yoon Suk-yeol and his predecessor, Moon Jae-in, have been personally committed to improving how Korea addresses challenges like data protection and digital identity.

The performance of Korean digital policymakers over the last decade or so presents a mixed picture, and much more remains to be done. A consistent theme is that previous initiatives have often provided a clear vision, but implementation has been disappointing. This is due in part to a lack of broad buy-in from the industries and stakeholders involved.

Privacy, Data Protection, and Data Infrastructure Policies: Grade B

Korea's personal information protection laws are very strong, but the implementation and enforcement of these laws has been inconsistent. It was only in 2020 that the Personal Information Protection Commission (PIPC) was established as a practical supervisory body and the relevant laws were unified. Still, further personal information protection legislation was needed to respond to the development of new technologies. The government therefore advanced laws to more clearly establish the rights of data subjects related to the automated processing of personal data. But because of the government's desire to promote the use of personal information for the development of the big data industry, the rights of Korean data subjects are more limited than those provided by the EU's General Data Protection Regulation (GDPR), and many aspects of personal information protection still need to be strengthened in Korea.

Personal Information and Big Data

An expression often used to emphasize the importance of the data industry is, "Data is the new oil" of the twenty-first century. Personal information is one of the most important types of data. However, for all Korea-based companies—including social media platforms, financial institutions and small retailers—to use personal information, they must demonstrate a legitimate basis under the Personal Information Protection Act (PIPA). In the private sector, personal information is usually processed with the consent of the data subjects. Of course, it is not easy to obtain the consent of every user of an online service that might be accessed by tens of millions of people. And what constitutes consent can vary. The processing of personal information for big data analysis is often done for reasons different from the purpose for which the information was collected in the first place. Therefore, as a way to use personal information without data subjects' consent, Korea has promoted the concept of de-identification.

The De-identification of Personal Data

Since the early 2010s, government departments such as the Ministry of the Interior and Safety and the Korea Communications Commission (KCC) have begun to create guidelines that allow de-identified personal data to be processed without the consent of data subjects for the purpose of revitalizing the big data industry.

In June 2016, the government of president Park Geun-hye released the Guidelines for De-identification of Personal Data, which integrated separate sets of guidelines that had previously been published by different ministries.[90] The guidelines defined de-identification as "measures to make individuals unidentifiable by means of, for example, deleting or replacing all or some of the elements from [the] dataset." Any de-identified data that have undergone

appropriate de-identification in accordance with the guidelines are presumed to be nonpersonal data and thus can be used for big data analysis or provided to third parties without the consent of data subjects.

At the same time, the guidelines prohibited the public disclosure of de-identified data in principle, because there can be a high risk of re-identification. De-identified data must be accompanied by security measures, as there is a possibility of re-identification if de-identified data are leaked and combined with other data. However, despite the fact that de-identified data can be re-identified, the guidelines presume that such data are nonpersonal and therefore exempt from the application of the PIPA. Finally, the guidelines require the government to designate so-called specialized agencies that focus on data de-identification to support the combination of data sets held by different data controllers.

Civil society groups criticized the guidelines for violating the PIPA. The concept of de-identification had not been considered when the act was originally passed, and it was unclear whether de-identified data were personal information or not. Even if the data subject was identified during de-identification, the data controller was exempt from liability if the data subject was de-identified again.

In particular, when combining data sets, it is difficult to view such data as nonpersonal since this process requires a common identifier. Therefore, the combination of data sets through a specialized agency may violate the PIPA by providing personal information to a third party without the consent of data subjects. According to a 2017 parliamentary inspection of the administration, 340 million pieces of consumer data were combined from August 2016 to September 2017 under the de-identification guidelines. In November 2017, civic groups filed a complaint against specialized agencies and twenty companies for violating the PIPA.[91] Companies have since stopped processing personal data in accordance with the guidelines, though they have not officially been repealed.

Regulatory and Institutional Innovation Hackathon

Both Park and her successor, Moon, touted the Fourth Industrial Revolution and stressed the need to promote the big data industry. As a result, the government's approach to data protection policies did not change when Moon took office in May 2017; although the words used to describe the policy changed. Under Moon, there was more emphasis on consulting with stakeholders rather than merely pushing the government's policy.

In early 2018, the Presidential Committee on the Fourth Industrial Revolution held a series of events called the Regulatory and Institutional Innovation Hackathon to gather relevant stakeholders from the government, industry, civil society, and academia to discuss and seek consensus on key issues related to the digital revolution. Two stakeholder meetings were held at the second and third installments of the hackathon under the agenda of harmonizing the protection and use of personal information.

At the first meeting, the participants agreed to work toward establishing the legal concepts of personal information, pseudonymized information, and anonymized information to refer to personal data, rather than using the term de-identification. They said the term de-identification was ambiguous, because depending on the level of de-identification, the new data sets may still be personal information or they may be anonymized information processed to make it impossible to re-identify the data subjects. The participants agreed that anonymized information would not be subject to the PIPA and would be distinguished from personal information.

To clarify the concept of anonymized information, instead of defining this term in law, participants at the meeting discussed supplementing the concept of personal information by referring to recital 26 of the EU's GDPR, which distinguishes between truly anonymous data and data that has been de-identified but might still be traced to an individual.[92] (The GDPR recitals provide additional context to accompany the regulation's articles.) The group also decided to establish a legal basis for the definition and use of pseudonymized information. Finally, participants agreed to conduct additional discussions on major issues regarding the protection and use of personal information.

Although the participants of the first meeting reached an agreement on basic concepts, their conflicting agendas meant there was no consensus on the details. Thus, the issue of personal information was dealt with again at the second meeting, where participants discussed issues such as the use of pseudonymized information, the combination of data sets, and oversight mechanisms.

Civil society participants argued that the use of pseudonymized personal information for purposes other than those for which it was first collected, and providing it to a third party, would be a restriction of the data subject's rights. These participants also argued that the use of pseudonymized information for other purposes should be limited to academic research and statistical compilation with public-interest value that benefits society as a whole. Industry representatives, meanwhile, argued that such use of pseudonymized information should be broadly allowed for industrial and market research to develop the big data industry. In the end, the second meeting did not reach a consensus on these issues, and the final report included all of the different positions expressed.[93]

The So-Called Three Data Laws

After the hackathon, the Moon government proposed three new data protection laws to the National Assembly on November 15, 2018.[94] The laws consisted of amendments to the PIPA, to the Network Act, and to the Credit Information Act. One goal of the proposed amendments was to foster the growth of Korea's data industry. Various civil society groups criticized the government, calling the laws the "personal information theft acts."[95] The government promoted the amendments as having been based on the social consensus achieved in the hackathons, but civil society groups argued that the proposed legislation reflected corporate positions on issues that the hackathon participants could not agree on. Despite the opposition from civil society, the National Assembly passed the laws on January 9, 2020.

Although the laws were packaged as the three data acts, the provisions of the Network Act were ultimately incorporated into the corresponding provisions of the PIPA. Therefore, the main changes to Korean data protection law were the amendments to the PIPA and to the Credit Information Act. Two main aspects of the legislation stand out.

First, the laws introduced pseudonymized information as a legal concept. The amended PIPA defines "pseudonymization" as "a procedure to process personal information so that the information cannot uniquely identify an individual without additional information"—and therefore defines information that has been through this process as pseudonymized information.[96] A personal information controller may process pseudonymized information without the consent of data subjects for purposes such as statistical analysis, scientific research, and archiving that is in the public interest.

The laws allowed a specialized institution designated by the PIPC or the head of a related administrative agency to combine pseudonymized information from different personal information controllers. When processing such information, the controller must ensure that technical, organizational, and physical safety measures are followed. No one may process pseudonymized information for the purpose of identifying an individual, and violations of this rule are punishable with a fine.

Second, the laws integrated the authority to supervise personal information—a power previously held by the KCC and the Ministry of the Interior and Safety—into the PIPC, which became a central administrative agency. However, the provisions of the Credit Information Act relating to personal information were not incorporated into the PIPA, and so the supervision of such information in the financial sector—that is, personal credit information—remained under the purview of the Financial Services Commission. Provisions on the processing of pseudonymized information for scientific research purposes were also included in the Credit Information Act, but the specific wording used was slightly different from that in the PIPA, which may cause confusion.

The Scope of Scientific Research

At the hackathon, civil society and industry representatives expressed different opinions about the purpose and scope of the use of pseudonymized information. The government's use of the phrase "scientific research" in the PIPA amendment reflected the desires of industry advocates. The revised act defines scientific research as that which "applies scientific methods, such as technological development and demonstration, fundamental research, applied research, and privately funded research."[97] Research conducted for commercial purposes within a company also fits this definition, as long as it uses the scientific method. A document that accompanied the PIPA amendment states that pseudonymized information may be used for scientific research, "including industrial purposes such as the development of new technologies, products, and services based on data, statistics for commercial purposes such as market research, and archiving purposes in the public interest."[98]

Civil society groups argued that the new definition of scientific research would allow for the processing of pseudonymized information for purposes other than those permitted as long as the controllers claimed to be conducting research.[99] That is because research does not usually involve unscientific methods, so any research could be said to be scientific. Civil society representatives maintained that the use of personal information without the consent of data subjects should be limited to academic, rather than scientific, research. That is because processing personal information for any purpose other than the original intention limits the rights of data subjects, and to justify such a restriction, there must be a corresponding social value and public interest.[100] The previous wording of the PIPA had used the term "academic research" instead of "scientific research"—but did not define it.[101]

The definition of scientific research in the PIPA amendment was borrowed from the EU's GDPR. Although the GDPR itself does not define scientific research, recital 159 explains it by stating that "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."[102] The recital further states that such processing should take into account the EU's objective of strengthening its scientific and technological bases by creating a European Research Area in which researchers, scientific knowledge, and technology circulate freely.

The European Data Protection Board, which is responsible for ensuring consistent application of the GDPR, has not yet issued a specific opinion or guideline on scientific research. However, recital 159 makes it seem that scientific research under the GDPR is not limited to research conducted in a particular field or by a particular institution but comprises research that can contribute to a common intellectual community called the European Research Area. In reviewing the concept of scientific research under the GDPR in 2020, the European Data Protection Supervisor (EDPS) stated that "for a controller to simply claim to process data for the purposes of scientific research is not sufficient" and that "it is a common assumption that scientific research is beneficial to the whole of society and that scientific knowledge is a public good to be encouraged and supported."[103]

Some Korean civil society members are concerned that by pseudonymizing consumers' personal information, companies will be able to further process it for purposes unrelated to that for which it was originally collected, combine it with the personal information of other companies, and share it or sell it to other firms in the name of scientific research—without the consent of data subjects.

For example, personal information held by telecommunications companies is very valuable. These companies can pseudonymize consumers' personal information and use it for their own research purposes or provide it to other firms, such as insurance companies, for research purposes—normally for a fee. Having been pseudonymized, personal information can be shared or sold to numerous companies. It cannot be ruled out that users may be identified and impacted in unanticipated ways when their personal information is combined with other such information.

Strengthening the Powers of the PIPC

The PIPA was first enacted in 2011 to establish a general law applicable to all personal information controllers in the public and private sectors. Therefore, when the PIPA was passed, the relevant provisions of other laws that had previously governed personal information in specific areas, such as the Network Act and the Credit Information Act, should have been repealed. However, these existing laws were maintained because the ministries and bodies in question refused to relinquish their supervisory authority. This led to criticism, especially from stakeholders in academia and civil society who argued that overlapping or similar regulations existed in different personal information laws, causing confusion and increasing the burden of compliance for controllers.

In addition, while the PIPA established the PIPC as a presidential agency, the act only granted the commission certain powers, such as of the ability to deliberate and resolve matters concerning the interpretation and operation of personal information protection law. Meanwhile, the Ministry of the Interior and Safety remained the competent ministry and supervisory authority for the PIPA. Therefore, the provisions of the 2020 amendments to unify Korea's personal information protection laws and integrate the supervisory bodies into the PIPC were desirable steps that had been demanded by civil society and academia.

However, these amendments still have shortcomings. Most notably, because the provisions of the Credit Information Act relating to personal information were not integrated into the PIPA, the Financial Services Commission retains its supervisory authority over personal credit information. As a result, the goal of unifying the similar and overlapping provisions of related laws into the PIPA was only half realized. Overlapping regulations therefore still exist between the PIPA and the Credit Information Act, causing confusion. For example, the two acts refer to scientific research in different ways.

The delay in integrating Korea's personal information protection laws and oversight bodies for nearly a decade, until the PIPA was revised in 2020, was due to the selfishness of government departments that did not want to give up their authority. At the time of the hackathon in early 2018, participants from government ministries opposed even putting the supervisory system on the agenda for discussion. So why did the 2020 data laws partly succeed in integrating the existing legislation and the supervisory bodies?

The superficial intention of the 2020 amendments was to strengthen supervision of the use of personal information to pave the way for the introduction of pseudonymized information. Yet, the belated reconciliation of interdepartmental interests was probably also due to the fact that an independent supervisory authority was necessary to obtain an adequacy decision under the GDPR—essentially, a ruling from the European Commission that Korea provides an adequate level of protection for personal data transferred from the EU. The Korean government had formed an EU Adequacy Assessment Task Force in August 2015 and conducted adequacy negotiations with representatives of the EU. But in October 2016, the European Commission ruled that Korea's personal information supervisory body lacked

independence and authority. Eventually, after the independent and empowered PIPC was established in August 2020, the European Commission adopted an adequacy decision for Korea in December 2021.[104]

The Rights of Data Subjects

On September 28, 2021, the government proposed another PIPA amendment, known as the Second Amendment, to the National Assembly. The assembly approved the revised act on February 27, 2023.

Highlights of the Second Amendment

The Second Amendment included extensive provisions. Three major revisions are noteworthy.

First, the special PIPA provisions on the processing of personal information by providers of information and communications services, which had been borrowed from the Network Act, were repealed. Other relevant provisions of the act were revised so that they would apply equally to all personal information controllers, whether or not they are information and communications service providers.

Second, the legislation introduced rights for data subjects that need to be protected as new technologies such as artificial intelligence (AI) evolve. These are the right to request the transfer of personal information and the right to control over automated decisions. The former refers to a data subject's right to ask a personal information controller to hand over personal information about that data subject either to them, an institution that specializes in personal information management, or a person who can take appropriate security measures and meet relevant technical standards. The right to control over automated decisions guarantees that a data subject can reject a decision, or request an explanation of it, if the decision was made using a completely automated system, including AI, and has a significant impact on their rights or obligations.

Third, the amendment addressed previous shortcomings in the PIPA. The legislation established new provisions related to the installation and operation of mobile video information-processing devices, and it supplemented the rules for the overseas transfer of personal information. In addition, the Second Amendment changed the sanction method for PIPA violations from a criminal punishment to a fine—effectively, an economic sanction.

Shortcomings of the Second Amendment

It is true that the Second Amendment improved the PIPA in general, first, by resolving the problems of having special provisions that applied only to information and communication service providers and, second, by introducing new rights for data subjects. However, from the point of view of civil society, many areas are still lacking.

First, the PIPA's level of protection is generally lower than that of the EU's GDPR. Under the GDPR, an organization can receive a fine of up to 4 percent of its global annual turnover for violations. But under the Korean act, the upper limit of any fine is 3 percent of total turnover, and the basis on which the fine is calculated excludes turnover that is not related to the violations. Companies were the stakeholders most opposed to this provision, and their opinions were partly accepted by the National Assembly during the deliberation of the bill.

While the Second Amendment established new data subject rights about automated decisions, the amendment did not include the term of "profiling,"[105] unlike the GDPR. In addition, while the GDPR restricts decisions based solely on automated processing that has a significant impact on individuals, except in certain cases, the PIPA permits such decisions and grants data subjects the right to reject or opt out of them, with the same exceptions. It is questionable whether such a right can be properly guaranteed.

In the case of the GDPR, data subjects have the right to be notified about the processing of their personal information regardless of the legal basis for that processing, whereas under the PIPA, a data subject is notified of the relevant facts only when the personal information has been given with their consent. Therefore, if an automated decision is made about a data subject based on the legitimate interests of the controller, the data subject may be unaware of that decision and therefore unable to exercise their right to reject it.

Second, the right to request the transfer of personal information under the PIPA is similar to the right to data portability under the GDPR. However, while the GDPR provides for the right to request the transfer of personal information to a data subject or another data controller, the Korean law also specifically mentions transfers to third-party institutions that specialize in personal information management—referred to as My Data providers.

Whereas the policy of pseudonymized information was intended for the use of personal information without the consent of data subjects, the My Data policy sought to promote the use of such information with their consent. The Moon administration promoted the My Data policy, which civil society groups criticized as accelerating the commercialization of personal information. Although the policy is based on consent, it is possible for data subjects to consent to the provision of their personal information without being sufficiently aware of the negative impacts that the My Data businesses might have on them. In addition, when My Data providers integrate personal information in fields such as telecommunications, healthcare, and finance, the negative consequences for data subjects' rights can be even greater.

Third, the Second Amendment did not reflect the improvements requested by civil society groups in written opinions submitted to the PIPC before the amendment was announced. These demands included provisions to strengthen the accountability of personal information controllers, such as impact assessments for private-sector controllers; strengthen data subjects' rights, such as the right to be notified of the processing of their data; unify the Credit Information Act, the Location Information Act, and the PIPA; strengthen the requirements

for investigative agencies wishing to access personal information, such as a warrant to access information held by public institutions; and enhance the remedies for PIPA violations, including class action lawsuits. Civil society groups proposed amendments to the PIPA, but these were not considered by the National Assembly. For this reason, civil society does not have a favorable position toward the Second Amendment.

Summary

The 2020 and 2023 revisions of the PIPA were driven by the need to foster new industries, such as big data and AI. Although the main purpose was to promote the use of personal information, provisions to protect such information were also included as a counterweight. Many of the new provisions refer to the GDPR, although the EU regulation was not copied verbatim.

Overall, Korea's legislation on the protection of personal information is similar to the European system, and although the Korean level of protection is not low, it was intentionally set at a lower level than that of the GDPR. Some experts in Korea believe that one motivation for the EU's strong personal information protection is to keep U.S. technology companies in check, because the European technology industry is not highly competitive. These experts use this reasoning to support the argument that Korea's level of personal information protection should not be raised to a similar level to the EU's.

While this interpretation may not be entirely erroneous, it distorts the point of data protection policy. Does the goal of fostering Korea's domestic industry mean that the personal information of Korean citizens should be less protected than that of European citizens? It is not necessary to replicate EU policies into Korean law, but it is problematic to prioritize the need to foster domestic industries without discussing the pros and cons of the policies themselves.

Cybersecurity of Government Systems: Grade F

Because Korea has an advanced internet infrastructure and e-government system, cybersecurity is very important. But the country's cybersecurity governance is lagging behind other countries'. It was only in 2019 that the Moon administration first established a national cybersecurity strategy. Prior to that, the government had created what it called comprehensive countermeasures, rather than an overall strategy, in the wake of major cybersecurity incidents, such as when Korea's nuclear operator was hacked in 2014.[106]

The 2019 National Cybersecurity Strategy is essentially only an outline: it does not include specific implementation plans and was created without in-depth discussions with stakeholders, including civil society. Perhaps because of the tense relationship with North Korea,

South Korea's cybersecurity policy overemphasizes the aspect of national security.[107] In particular, the National Intelligence Service (NIS) is responsible for cybersecurity in the public sector, a setup that hinders the development of Korea's cybersecurity governance.

The NIS controls the National Cybersecurity Center and carries out tasks such as establishing national cybersecurity policies, detecting and responding to cyber attacks on public sector networks, and verifying security suitability and cryptographic modules for IT products used by public institutions. However, civil society members have criticized the NIS's cybersecurity work for having a weak legal basis. Although the service's work on digital public sector infrastructure and on security and cryptographic verification is based on relevant government acts, there was no similar legal basis for establishing national cybersecurity policies or regulating the cybersecurity of public sector networks. These moves were based on the 2005 National Cybersecurity Management Regulations, which resulted from a presidential order with no higher legal basis.

For this reason, the NIS has been trying to establish a legal basis for its cybersecurity work and, to this end, has proposed legislation: the National Cyber Terror Prevention Act and the National Cybersecurity Framework Act. However, these efforts failed in part because of societal opposition. There has been a great deal of concern that the NIS—a secretive intelligence agency notorious for its surveillance of civilians and politicians, its fabrication of espionage cases, and its interference in politics[108]—could expand its surveillance power throughout cyberspace. Ironically, however, when the act that created the NIS was amended on October 19, 2021, for the purpose of reforming the service, the revised act specified the NIS's authority in the field of cybersecurity.

One of the key responsibilities that allowed the NIS to abuse its power in the past was the service's investigatory authority. Therefore, the Moon administration, which had pushed for NIS reform, revised the service's duties to abolish its investigatory power while adding further cybersecurity-related tasks. Despite criticism from civil society about the NIS's cybersecurity authority, the government and the ruling party at the time did not consider these concerns to be important.

The reason why Korean civil society opposes the NIS's cybersecurity mandate is not just because the service has a history of human rights violations and political interference. Civil society's distrust of NIS remains high, as its illegal activities continued until recently. In 2015, leaked data revealed that the NIS had been using a hacking program called RCS, developed by the Italian company Hacking Team, for online surveillance.[109] There are still major concerns that the NIS's authority over cybersecurity will allow the service to strengthen its online surveillance and monitoring.

In addition, although cybersecurity intelligence collection might be a valid role of the NIS, it does not have to be the intelligence agency that establishes cybersecurity policies or prevents and responds to cyber attacks. Indeed, if the NIS is responsible for these tasks,

cooperation with other stakeholders may become more difficult because of Koreans' distrust of the service. The participation of civil society is essential to establish cybersecurity policies based on openness and human rights, but the government has not consulted with civil society to this end. Transparency in the NIS's cybersecurity work and oversight by the National Assembly, the media, and civil society has also become difficult, because the service is subject to fewer transparency obligations and less parliamentary oversight than other government departments.

Although the 2021 revision of the NIS Act stipulated the service's cybersecurity authority, Korea still lacks consistent and systematic cybersecurity laws. Different terms and concepts are used in cybersecurity-related laws, such as the Network Act, the Information and Communications Infrastructure Protection Act, and the NIS Act and its enforcement ordinances. There is also no national cybersecurity governance mechanism stipulated by law. While there is a need to improve the consistency of these laws, it is unlikely that a societal consensus will be reached in the foreseeable future, as long as the NIS retains its cybersecurity powers.

Digital Identity: Grade C

Every country has a system of national identification numbers for citizens to access public services. Korea's system of resident registration numbers (RRNs) has been criticized as a major privacy violation. All Korean citizens are given an RRN at birth, which does not change throughout their lives. The numbering system includes personal information such as date of birth, gender, and place of birth. In the past, RRNs have been collected for personal identification in various fields, both public and private. Korea also uses other numbers, such as a person's driver's license number, passport number, and national health insurance number, but all of them are linked to the RRN. RRNs are still collected in major sectors such as finance, telecommunications, and healthcare.

In the early days of informatization, large-scale leaks of personal information occurred frequently. For instance, in 2008, a breach of the internet auction site Auction affected 18 million personal information records. In 2012, 35 million records were leaked from Cyworld, a social networking service. The leaked personal data included RRNs, which acted as a key to link up different types of personal information, increasing the damage caused by the breaches.[110]

As a result, Korean society has demanded improvements to the RRN system. On August 8, 2014, the National Human Rights Commission of Korea recommended three major changes. The first was to limit the purpose of processing RRNs, so that the numbers would be used only for administrative work related to resident registration and judicial administration, with a separate identification system for other public areas. The second recommendation

was to change the numbering system of RRNs to a random number format that does not contain personal information. Third, the commission recommended the creation of a process for data subjects to change their RRN if they wish to do so.

These recommendations have so far been implemented in only a very limited way. On February 17, 2013, the collection of RRNs through information and communication networks was prohibited; and on August 7, 2014, the collection of RRNs was banned in all areas of society without a legal basis. However, since the numbers can be collected under the provisions of laws or enforcement decrees, most public institutions continue to do so. On May 19, 2016, the National Registration Act was amended to allow data subjects to change their RRN. However, such changes are possible only in limited cases where there is a risk of damage to life, body, or property due to the number being leaked.

In the private sector, where the collection of RRNs was already restricted, another identification number similar to the RRN was introduced. Before the advent of Korea's internet real-name system for identifying users, many internet companies initially used RRNs to voluntarily verify the identities of their users. Later, when RRN leaks became a societal problem, companies were required to adopt an alternative identification method that did not collect RRNs, and so the i-PIN service was launched.

Originally, i-PIN generated a unique user identifier for each digital interaction, which meant that the same user would have a different identifier for each website they signed up to. The government then introduced so-called connecting information (CI) to identify the same user across different operators. CI consists of 88 bytes of information created by encrypting an RRN and is a one-to-one match with the RRN from which it is derived. CI is therefore effectively a second RRN used by the private sector, with the difference that it does not contain personal information. While it should be up to companies to decide how to partner with each other, the Korean government introduced CI without any legal basis to facilitate identity verification in the private sector. In September 2021, civil society groups filed a constitutional complaint, arguing that CI had no legal basis and excessively violated citizens' basic rights, including the right to privacy.

When a customer signs up for a cell phone service in Korea, it is mandatory to verify their identity through SIM card registration. Because of the combination of RRNs, CI, and SIM card registration, Korean users have no choice but to use the internet based on their real identities, which means that Koreans can be easily tracked anytime, anywhere. The Personal Information Portal,[111] operated by the PIPC, provides a service that allows citizens to check their identification details and, if they wish, withdraw their information from a website. A user can see when and where they verified their identity, see what services they signed up for, and request to be removed from sites they no longer want to use. It is ironic that a service that allows the government to know citizens' internet service subscriptions is offered in the name of privacy.

Content Moderation: Grade C

Since the early days of the internet, Korea's administrative agencies have reviewed online content and demanded that illegal or harmful content be deleted or blocked. Since 2008, the Korea Communications Standards Commission (KOCSC)[112] has performed this role under the Network Act, which prohibits the distribution of illegal material, such as pornography, defamation, and online stalking. The content examined by the KOCSC includes material that could be harmful to children as well as content types stipulated in the Network Act and other legislation.

The Deliberation Rules on Information and Communications, which set out in detail the types of content that require deliberation, also list a wide range of content that the KOCSC considers harmful, rather than illegal. As a result of its deliberation, the commission may request corrective measures, such as the deletion or blocking of the material or the suspension or termination of a user's account. Although such measures are technically only a recommendation, they are in effect mandatory. This is because the KCC can issue a correction order, which is mandatory, if the KOCSC's recommendation is not accepted. In the case of material that leaks state secrets, violates the National Security Law, is intended for criminal purposes, or aids or abets a crime, if the KOCSC's request for correction is not followed, the KCC must issue a correction order.

In 2022, the KOCSC reviewed 248,130 cases,[113] of which 234,263 were determined to require corrective action. The most common type of corrective request was to block access to illegal or harmful information from overseas, which occurred in 192,621 cases. There were 21,867 decisions to disable or suspend users' accounts and 19,378 decisions to delete the content. By type of violation, material that constituted an online sexual offense was the most common, with 54,994 cases (23.5 percent of the total), followed by gambling content, with 53,177 cases (22.7 percent), and obscene content, with 46,195 cases (19.7 percent). Material that violated the National Security Law was found in 2,071 cases (4.2 percent).[114]

Korean civil society groups have criticized the KOCSC's deliberations as state censorship. Indeed, in a 2018 report, the UN special rapporteur on freedom of opinion and expression noted that some countries require the blocking of foreign websites and content that are deemed illegal under domestic law, which can lead to serious violations of the freedom of expression. The report found that "states should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression."[115] In the case of content that causes serious damage to a specific individual, such as digital sexual violence, there may be an urgent need to delete or block the material. However, targeting content that is deemed to undermine societal interests can stifle criticism of power and violate the freedom of expression.

In particular, content related to North Korea has been easily subjected to regulation. For example, on March 24, 2016, the KOCSC blocked access to North Korea Tech,[116] a website that specializes in ICT issues in North Korea, citing violations of the National Security Act.

In response, Martyn Williams, the operator of the site, with the support of OpenNet Korea, filed an administrative lawsuit, and a court of first instance ruled that blocking the entire website was illegal as it violated the principle of minimum regulation. In an appeal decision on October 18, 2017, the Seoul High Court upheld the decision of the court of first instance and dismissed the appeal.[117]

Encryption: Grade B

Debates about encryption policies usually revolve around whether such policies should make it easier for government agencies to crack ciphers and to force private companies to crack them. Korea does not have such a policy, nor does it regulate the development and adoption of cryptographic technologies in the private sector. This is quite puzzling given the country's tense relationship with North Korea and the fact that the NIS has considerable surveillance power, which it has abused in the past.

The NIS Act authorizes the service to carry out security work on documents, materials, facilities, areas, and personnel pertaining to state secrets, while a related enforcement decree provides specific regulations on the management of cryptographic materials. In addition, the NIS verifies the safety and implementation suitability of cryptographic modules used to protect important information in the materials communicated by public institutions such as administrative agencies. While this system has some impact on private cryptography, it does not regulate the free development and adoption of cryptography in the private sector.

The Framework Act on Intelligent Informatization requires the government to "prepare measures to facilitate the development and use of cryptography technology and to ensure the safety of intelligent information services using cryptography technology."[118] The Korea Internet and Security Agency operates a website for the "vitalization of cryptography technology,"[119] but this does not fall under any regulation on the use of cryptography technology. The Framework Act on Electronic Documents and Electronic Transactions, meanwhile, stipulates that "the government may restrict the use of encryption products and take necessary measures to access the original encrypted information or encryption technology if it deems it necessary for national security,"[120] but this provision has not been controversial.

In November 2020, under the Moon administration, then justice minister Choo Mi-ae sparked controversy when she instructed her office to consider a bill that would allow the government to forcibly unlock a suspect's smartphone for investigative purposes. Because her instruction came in the context of a conflict with Yoon, who was the prosecutor general at the time, conservatives pushed back against it. Progressives and liberals, who formed the Moon administration's support base, were also critical of the move. Civil society objected as well, saying that such a bill might violate people's fundamental rights. In the end, the bill did not move forward.

AI Regulation: Grade C

In 2016, a match of the board game Go between AlphaGo, an AI program developed by DeepMind, a subsidiary of Google, and Lee Se-dol, a professional player, shocked Korean society because Go is considered by many to be the most difficult board game in the world—and Lee lost. The event increased the interest in and adoption of various AI tools across Korean society, including chatbots, translation aids, recruitment tools, and social media algorithms. At the same time, there have been controversies related to the development and use of AI. The chatbot Lee Luda, launched in December 2020, was the first in Korea to raise the issue of discrimination and hate speech by AI; Lee Luda was shut down after three weeks. The PIPC conducted an investigation into the chatbot's misuse of personal information and imposed a total of 103.3 million won (around $78,000) in fines and penalties on Scatter Lab, the developer.[121]

Controversies have also arisen over AI tools for public-sector recruitment. In 2020, civil society groups requested the disclosure of information on AI recruitment tools used by public institutions. These groups criticized the fact that the institutions had adopted AI tools from private companies without reviewing their problems and performance and that they did not have adequate data to answer complaints from parties affected by AI. Several advocacy groups called for the establishment of a system to ensure public institutions' accountability. In addition, in 2021, it became known that the Ministry of Justice had about 170 million records containing facial recognition data and other information on Korean and foreign citizens that had been collected during immigration inspection processes.[122] All of this data was shared with private companies for AI learning and algorithm verification—without the consent of the data subjects—for the purpose of upgrading the country's immigration system.

Despite these controversies, discussions of how to regulate the risks of AI in Korean society are still at a rudimentary level. So far, government policies have focused on fostering the AI industry and emphasized AI ethics and self-regulation rather than active regulation. On December 17, 2019, the Moon administration released the National Strategy for Artificial Intelligence,[123] which understood AI as a civilizational change and expressed the government's intention to use the technology as an opportunity to develop Korea's economy and solve social problems. The strategy presented future visions for the AI era in three areas, to be realized through nine substrategies and one hundred action tasks. One of the nine substrategies, bold regulatory innovation, has as its guiding principle "allow first, regulate later."

On December 23, 2020, the Ministry of Science and ICT and the Korea Information Society Development Institute released the AI Ethical Standards,[124] which aim to achieve "AI for humanity" through three basic principles to be observed in the development and use of AI: human dignity, the public good of society, and technology that is fit for purpose.

To practice and implement the three basic principles, the standards set out ten core requirements that must be met in the entire process of AI development and use: a guarantee of human rights, protection of privacy, respect for diversity, a prohibition on infringement, public good, solidarity, data management, accountability, safety, and transparency. In an accompanying press release, the government stated that the standards were "not binding 'laws' or 'guidelines' but rather moral norms and voluntary codes."[125]

Then, on May 13, 2021, the Ministry of Science and ICT released the Strategy for Realizing Trusted AI, which, unlike previous national strategies, focused on concerns about AI. The strategy recognized that it is difficult for AI to be accepted socially and industrially without societal trust in the technology. The strategy proposed three substrategies and ten action tasks for trusted AI while focusing on building a support system to secure reliability in a voluntary way in the private sector.[126]

A year later, the National Human Rights Commission released the Human Rights Guidelines for the Development and Use of AI to prevent human rights violations and discrimination that may occur in the process of developing and using AI. The commission is currently developing tools to support AI developers and deployers as they conduct human rights impact assessments.

In early 2023, the National Assembly and the Ministry of Science and ICT pushed for a basic law on AI. The bill presented was a consolidation of bills previously proposed by various members of the assembly. When it became known in February 2023 that the bill had passed the committee review stage, civil society groups strongly objected. These groups argued that the Ministry of Science and ICT, which was the lead ministry for the bill, was not an appropriate supervisory body for AI as it prioritizes industrial development over risk management.

In addition, the bill's approach of "allow first, regulate later" has raised concerns that it could permit high-risk AI applications to enter the market and undermine human rights and safety regulations. The bill defines high-risk AI, but according to many critics, the definition does not include enough areas; and unlike the EU's AI Act, the Korean bill does not define which forms of AI should be banned. The bill does provide some compliance requirements for AI in high-risk areas, but these are not sufficient to mitigate risks and are ineffective because there are no penalties for noncompliance.

Civil society is not opposed in principle to a bill to regulate AI but believes that the current proposal does not include sufficient safeguards to mitigate the risks of the technology. More discussion is needed on this issue as well as the questions of how high-risk AI should be defined, which usages should be prohibited, and which ministries should be responsible for overseeing AI.

CHAPTER 4

Malaysia: Focused Implementation Is Key to Realizing Potential

Elina Noor

Like most of its neighboring countries, Malaysia has made digital transformation a high priority. But it is far from being a new item on the national agenda. For the past three decades, the country has sought to leapfrog to digital heights. The Multimedia Super Corridor (MSC), launched in 1996 by then prime minister Mahathir Mohamad, was the government's first ambitious initiative to seize the promise of information and communications technologies in a new millennium.[127] Envisioned as a "global facilitator of the Information Age," underpinned by cyber laws and investment-friendly guarantees, the MSC aimed to link several of the country's mega development projects. These included the new e-government administrative capital, Putrajaya; the Kuala Lumpur City Centre; and the Kuala Lumpur International Airport. The planned nucleus of the MSC was Cyberjaya, Malaysia's version of Silicon Valley in the United States. All of these projects were ultimately built to blueprint. Yet for various reasons—including the state of domestic politics but more significantly the shock of the Asian financial crisis and its reverberations for years after—the MSC never reached its true potential.

Still, the Malaysian government has persisted in mapping the country's digital future, rolling out numerous policies and strategies: for example, the National Broadband Initiative (2010), Digital Malaysia (2011), the National Internet of Things Strategic Roadmap (2015–2025), the Malaysia Smart City Framework (2019–2025), and the Digital Economy Blueprint (2021). The government has courted, and counted on, the investment and experience of large multinational companies to boost development of the country's digital economy. It has also benefited from the enterprise of state governments, especially those with their own digital transformation plans.[128] In December 2023, Prime Minister Anwar Ibrahim created a new cabinet position to take over the country's digital portfolio after splitting the Ministry of Communications and Digital into two separate entities.

But despite having ample vision and aspiration, Malaysia's digital leadership has been constrained by inconsistent implementation and conventional frameworks. This chapter provides a "report card" on how well Malaysia (at all levels of government) is doing in developing and implementing policies for digital transformation (see table 2). These grades are subjective and are based on literature reviews, interviews, and media reports. The United Nations' International Telecommunication Union (ITU) ranked Malaysia fifteenth overall in its 2023 ICT Development Index, above both South Korea and Japan (as well as most countries in Europe).[129] However, progress is uneven; the country is better at developing infrastructure than at fostering talent, innovation, and adoption. Similarly, the report card reveals a mixed picture when it comes to digital policy. Further, more comprehensive perspectives on digitalization that go beyond narrowly defined economic priorities and that anchor discussions to the relationality of technology to human beings and the environment are seldom if ever discussed in the Malaysian context. These alternative reference points—increasingly prevalent among communities in the global majority ("Global South") and far from mere philosophical reflections—bear greater practical urgency amid geopolitical frictions and the climate crisis. Stakeholders in Malaysia should explore these deliberations to strengthen the country's agency, autonomy, and stewardship in a fragmenting technological space.

Table 2. Report Card on Digital Leadership in Malaysia

Key Digital Issues	Letter Grade
Connecting the unconnected	A
Broadband competition	B
Encryption	C
Cybersecurity of government systems	F
Cybersecurity of nongovernment systems	C/F
Digital identity	I
Content moderation	C
Data localization	B
Data architecture	C/I
Data protection	I
Online copyright	B
Digital inclusion	C

Note: A = superior, B = above average, C = average, F = failing, I = incomplete. The grades only indicate how well or poorly the government is doing in various areas; they cannot be used to compare a country's performance with that of other countries.

Connecting the Unconnected: Grade A

The foundation of a digital economy is affordable and widely available broadband service. The Malaysian government's strategy to connect the nation can be traced back to at least 2010, when it launched the National Broadband Initiative. To meet the realities of Malaysia's geography (the country is cleaved by the South China Sea) as well as the topographical challenges of building and deploying internet infrastructure in the country's rural and remote parts, the government has partnered with industry to provide 100 percent internet coverage in populated areas by 2025.[130]

The country's five-year national digital infrastructure plan (JENDELA), launched at the height of the coronavirus pandemic in September 2020, aims to achieve 100 percent connectivity in populated areas and to expand 5G use by the end of its term in 2025.[131] There is also now state-level recognition of communication infrastructure as a public utility, meaning the funding and provision of such infrastructure is government-led, particularly in "rural areas deemed unprofitable to private service providers."[132] The government claims to have achieved already, as of 2022, a 4G coverage of 96.9 percent in populated areas and a 5G rollout rate of 47.1 percent. In some urban states, 5G connectivity has even exceeded 70 percent.[133] A combination of geostationary satellite and Starlink satellite technology is supposed to plug the connectivity gap, especially in rural and remote areas.[134] Although "digital inequalities and the challenges to meaningful connectivity and digital inclusion" remain, the country fares well in the ITU's measure of "universal and meaningful connectivity."[135]

Broadband Competition: Grade B

A competitive telecommunication market is key to spurring investment and driving down prices. In Malaysia, because one player dominates the *fixed* broadband market, nationwide penetration in that sector remains below 50 percent.[136] Meanwhile, however, there are four major players in the *mobile* broadband market and the country's fiber network has expanded, leading to liberalized access for users and consumers.[137] In February 2023, the government introduced the Mandatory Standard on Access Pricing, which aimed to reduce high-speed broadband costs once access agreements between service providers were finalized.[138] Satellite broadband provision through SpaceX's Starlink is meant to expand connectivity in remote and interior locations, but without subsidies, upfront and subscription costs will put it largely out of reach for populations in those areas.[139]

Encryption: Grade C

A critical tool for improving privacy and cybersecurity is end-to-end encryption. Yet as in many countries, there is a tension between the need for better data protection and the desire of police and intelligence agencies to perform online surveillance. In Malaysia, police or other law enforcement officers conducting lawful searches have the right to access to

computerized data.[140] Laws such as the Criminal Procedure Code (Act 593), the Digital Signature Act 1997, the Communications and Multimedia Act 1998, the Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007, and the Strategic Trade Act 2010 afford officers access by way of a "necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data."

Cryptography in Malaysia's public sector is guided by the National Cryptography Policy 2013 (which supports the National Cybersecurity Policy) and is integrated at the agency level through internal ICT security policies. Yet implementation remains patchy; for example, the country has created its first local cryptography product to help reduce vulnerabilities posed by foreign encryption vendors, but there is still some unauthorized modification of records and the use of digital signatures remains limited by administrative inertia.[141] There are encouraging measures being taken, though, such as the development of a Malaysia Cryptography Module Validation scheme based on international standards and the creation of a portfolio of nationally trusted cryptographic algorithms (MySEAL).[142]

Cybersecurity of Government Systems: Grade F

Despite numerous government circulars and guidelines to develop a robust cybersecurity culture, federal and state government agencies have been hit by a string of breaches that have compromised the personal data of many Malaysians.[143] Between 2021 and 2022, the names, identity card numbers, addresses, and photographs of nearly 27 million Malaysians (over 80 percent of total population)—including of the minister of home affairs—were offered for sale.[144] Poor cybersecurity practices associated with the country's national coronavirus management app (as detailed in the Auditor-General's 2021 report), as well as the exposure of files containing personal information at government sites, including public universities, point to a lackadaisical or careless approach by those in charge.[145] And to make matters worse, political leaders have shirked responsibility or minimized the national security threat of these breaches.[146] A key complicating factor has been the contracting out of application programming interface (API) provision to the private sector, leading to poorly defined responsibilities and liabilities.

Cybersecurity of Nongovernment Systems: Grade C/F

Data leaks have been rampant in Malaysia's commercial sector, affecting some of the country's largest corporations (in some cases repeatedly).[147] The finance, telecommunication, aviation, and e-commerce industries have been particular targets, though substantial personal data have also been stolen from medical associations, a housing loan application aggregator, and a popular job site.[148] In at least one case, the security measures and network organization of a regional enterprise were deemed so dismal and so "chaotic," respectively, that even a ransomware gang felt the enterprise was an unfair target.[149] In other cases, the data were

leaked online a few years after the breaches, and there was no apparent rush to take remedial action despite the risks to individuals.[150] Where lawsuits were filed, court documents were sealed or undisclosed.[151]

Micro-, small-, and medium-sized enterprises (MSMEs) form the backbone of Malaysia's economy (over 97 percent in 2021).[152] But although many of them seek digitalization, they still have limited cybersecurity awareness, capacity, or capability.[153] In 2021, the Malaysian government launched a public-private partnership initiative to assist SME cybersecurity adoption. However, little has been reported of its progress since.[154] On a more positive note, Cybersecurity Malaysia (an agency under the Ministry of Digital) and Malaysia's Computer Emergency Response Team have long offered technical incident and response hotline services to any individual or organizational user. It is this availability of support that raises the grade average from a pure F.

Digital Identity: Grade I

Malaysia's foray into establishing a national digital identity system, MyDigital ID, has had fits and starts since 2011.[155] In 2020, the government revived the initiative with a public consultation and plans for full implementation in 2024—one year ahead of target as listed in the country's MyDigital Blueprint.[156] In the first phase of the rollout in December 2023, Anwar Ibrahim was the first individual in the country to receive his digital ID. His cabinet members also received theirs. The general public will receive their IDs by July 2024, once use cases have first been established among civil servants and government beneficiaries such as subsidy recipients.[157]

In a parallel move, the Malaysian state of Sarawak has also been contemplating a digital identity platform to expand access to public and private sector services.[158] It is unclear how or whether the state- and federally issued digital identities would be differentiated.

Content Moderation: Grade C

Because of sensitivity around issues of race, religion, and royalty in Malaysia, content moderation efforts are driven simultaneously by both a legitimate responsibility to preserve the country's social fabric and politically tinged overzealousness, particularly in the run-up to elections.[159] Social media platforms like TikTok and Facebook have also been called into question for their lack of transparency in moderating inflammatory content.[160]

In 2019, the government repealed an anti–fake news legislation passed by the previous administration and criticized as repressive.[161] In March 2021, however, under the declaration of a nationwide emergency prompted by COVID-19, the government instituted the Emergency (Essential Powers) (No. 2) Ordinance, criminalizing fake news related to the pandemic with extraterritorial jurisdiction. This ordinance lapsed once the emergency

period ended in August 2023, but fake news may still be prosecuted under other laws such as Section 505(b) of the Penal Code and Section 233(1) of the Communications and Multimedia Act. Malaysia now also has fact-checking websites, which operate according to international standards.[162]

Data Localization: Grade B

Section 129(1) of Malaysia's Personal Data Protection Act 2010 (PDPA) restricts the transfer of personal data to places outside Malaysia unless the minister has determined that the receiving country is able to grant an adequate level of protection equivalent to that afforded by the PDPA.[163] Section 129(3) lists other exceptions. In striking a finer balance between data protection and privacy on the one hand and ensuring a smoother transborder flow of data for commercial purposes on the other, the government may update the PDPA by moving away from its current whitelist approach to establishing a blacklist approach instead. Under the latter, cross-border data transfers will generally be allowed to jurisdictions that have not been prohibited.[164]

Data Architecture: Grade C/I

The Malaysian government has been committed to an open and accessible data policy since at least 2014, when it introduced the first iteration of the Public Sector Open Data Portal, which includes searchable and downloadable data sets related to public administration.[165] In January 2023, the Department of Statistics launched a separate platform, OpenDOSM NextGen, which gives policymakers, businesses, researchers, journalists, and data scientists access to official figures from its own datasets, including statistics on household income and expenditure, labor markets, and the financial sector.[166]

Redundancies that potentially complicate rather than clarify empirical records as well as lack of integration of repositories created by different agencies are some of the challenges that government at all levels will need to overcome to meet the open data targets of Putrajaya's Digital Economy Blueprint.[167] Additionally, there has been insufficient consideration of the tensions between the value and risks of open data as well as the benefits and ethical hazards of big data analytics, especially given the poor track record of data protection in Malaysia thus far.

In January 2024, the government launched the nation's Central Database Hub (PADU) to consolidate various databases managed by over 400 agencies. This streamlining effort also aims to improve government disbursement of subsidies and to remedy wastage. But despite the government's assurances that PADU had been stress-tested by independent experts, the portal came under considerable criticism for technical difficulties and privacy and cybersecurity concerns.[168] Its success will depend on responses to this criticism and the level of uptake among both people with and people without digital access for registration.[169] It is for this reason that the grade for this section floats between a C (average) and an I (incomplete).

Data Protection: Grade I

Malaysia's early passage of the PDPA 2010 illustrates the country's progressive stance on the matter. However, the act's limitations—including its applicability to only commercial transactions and the absence of a mandatory breach notification—have hampered transparency, accountability, and the effective redress of significant data leaks (see the sections on cybersecurity).[170] A set of twenty-two proposals to update the PDPA was due to be tabled in parliament in October 2022, but parliament was dissolved that month to pave the way for general elections.[171]

In January 2024, however, Malaysia's new digital minister, Gobind Singh Deo, revived efforts to update the Act. A draft amendment bill is currently being finalized to be tabled in parliament this year. In the meantime, the Department of Personal Data Protection will draw up guidelines in seven significant areas: notification of data breach, data protection officers, data portability, cross-border data transfer, data protection impact assessment, privacy by design, and profiling and automated decisionmaking.[172]

Online Copyright: Grade B

In 2022, the Malaysian parliament passed the Copyright (Amended) Act to include "offences relating to streaming technology," punishable by a fine between 10,000 and 200,000 ringgit (about $45,000 to $900,000 USD) or imprisonment for up to twenty years, or both.[173] Two individuals were charged that same year for selling Android boxes pre-loaded with unauthorized content—the first case that would be prosecuted in court under the act.[174] Additionally, the Ministry of Domestic Trade and Consumer Affairs (now the Ministry of Domestic Trade and Cost of Living) also launched the Cyber Copyright Enforcement program in 2022 to combat digital film copyright infringement or piracy by blocking or removing unauthorized content within forty-eight hours of notification by the program's participants to the ministry.[175] While these nascent measures are encouraging, it remains unclear how Malaysia's copyright laws along with other existing statutes might adequately regulate generative artificial intelligence outputs in the country's context.[176]

Digital Inclusion: Grade C

One of the six strategic thrusts of the Digital Economy Blueprint is the creation of an inclusive digital society. To achieve this goal, the government proposes to establish a centralized database on vulnerable groups. The database would track inclusion levels among the bottom 40 percent of income group earners, women, and people with disabilities. However, success seems to be premised on integrating these populations into e-commerce platforms. And while the longer-term socioeconomic outcomes of different levels of the digital divide in Malaysia have been assessed, there has been very little policy discussion, if any, on whether the government's digital vision as it stands today is even desired by all segments of society.[177]

Conclusion

Malaysia has made promising headway in laying the building blocks of its digital transformation and its successes to date place the country among the region's top performers in this space. Yet serious cybersecurity breaches will need to be effectively addressed at the policy and implementation levels for Malaysia to fulfill the ambitious goals outlined in its many blueprints. This will take political will and commitment, alongside a comprehensive partnership with the private sector and citizen stakeholders.

CHAPTER 5

Japan: Learning From Early Digital Standard-Setting Experiences

Kenji Kushida

The Japanese government and private sector have been engaged in numerous efforts to embrace various aspects of the digital transformation. In 2021, the government established the Digital Agency, which consolidated related efforts from various ministries and drew staff from other ministries and private firms to formulate strategies, update outdated laws, and manage much of the government's digital infrastructure.

In terms of standards, however, Japan is not positioning itself aggressively as a standard-setter. This decision stems from a long and unsuccessful history of Japan setting its own information technology (IT) standards, only to find that these standards isolated the country's domestic market from the global dynamics of competition.[178] This isolation put Japanese firms at a disadvantage in global markets, and also ended up making these firms less competitive than they otherwise might have been.

In areas such as artificial intelligence (AI) and cybersecurity, Japan is looking to the United States and Europe to find ways to take the best parts of their different approaches to regulating these technologies. Japan's baseline level of physical infrastructure development for broadband and wireless is extremely high. When looking only at infrastructure deployment, Japan was highly successful in early broadband and fiber-optic penetration and wireless network deployment, driven by political dynamics revolving around a focus on egalitarian access and strong government regulation of incumbent telecommunications firms designed to allow competitors access to their networks. However, after seeming to win a race in building physical broadband and wireless infrastructure, Japan discovered that this was not enough to unlock vast new forms of value creation in the economy.

Japan's proprietary digital wireless standards were technically advanced, but they isolated the Japanese market.[179] The country's Personal Digital Cellular and Personal Handy-phone System standards were incompatible with Europe's Global System for Mobile Communication standard, and North America was slow to adopt digital wireless standards, so Japan found itself "leading without followers."[180] Japan then moved to help create global 3G wireless standards and deployed new 3G infrastructure faster than anywhere else.[181] But it turned out that creating standards and deploying the new infrastructure several years ahead of everywhere else also led to a situation in which Japan's domestic market was advanced and full of features unavailable elsewhere,[182] which left Japan isolated and did not confer any advantages to its manufacturers, service providers, or content ecosystem, all of which were locked into the domestic market. The term coined for this situation was "the Galapagos effect," named after the geographically isolated Pacific islands where evolution took its own proprietary course.

In another case, Japan's digital television standard, known as Integrated Services Digital Broadcasting–Terrestrial, was adopted in several South American and Latin American countries, beginning with Brazil before it spread to Argentina, Peru, Chile, Costa Rica, Nicaragua, and others in the late 2000s and early 2010s.[183] In Asia, the Philippines adopted this standard as well. The standard was developed primarily by Japan's national broadcaster NHK, with government support and funding. Efforts to get other countries to adopt the standard, especially with Brazil as the first mover, were a Japanese industrial policy initiative, entailing governmental working groups, technology transfers, industry support measures, negotiations around intellectual property, and financial assistance from Japan. However, it turned out that Japan gained little direct commercial value from creating its standard and getting that standard adopted. Manufacturers of televisions, mostly from other Asian countries, only needed a small, low-cost chip to gain compatibility.

The lesson learned was that setting standards does not necessarily confer any real international competitive advantage for a nation's companies. The question is *which* standards matter. Since these experiences, the Japanese government has been eager to deploy global standards in many areas and to avoid isolating its domestic market.

Japan is embracing global companies far more than it did in previous decades. For example, it embraced global cloud-computing service providers like Amazon, Google, Microsoft, and Oracle to create its government cloud capabilities. Japan had devolved government IT systems to localities when the initial computer systems were installed in the 1980s and 1990s, and the country ended up with a large number of incompatible, semi-custom local computer networks provided by Japanese systems integrators such as NTT Data, Fujitsu, and NEC. However, since most of these systems were unable to communicate with one another, the Digital Ministry, upon its creation in 2021, spearheaded efforts to create a government cloud that localities could migrate to—and global cloud providers could provide these services. The major Japanese firms did not apply due to the stringent security requirements stipulated by the government, with which they were unable to comply.[184]

Here is a far-ranging assessment of the Japanese government's performance to date in various areas of digital policy (see table 3).

Table 3. Report Card on Digital Leadership in Japan

Key Digital Issues	Letter Grade	Notes
Connecting the unconnected	A	
Broadband competition	A	
Encryption	I	
Cybersecurity of government systems	C	Improving overall, with an A in some areas and an F in others.
Cybersecurity of nongovernment systems	C	An A in some areas and an F in others.
Digital identity	B	
Content moderation	C	
Data localization	A	

Note: A = superior, B = above average, C = average, F = failing, I = incomplete. The grades only indicate how well or poorly the government is doing in various areas; they cannot be used to compare a country's performance with that of other countries.

Connecting the Unconnected and Broadband Competition: Grade A

Japan's political dynamics have enabled it to excel in connecting almost all the country's people with high-speed broadband and wireless connectivity. The politics focusing on infrastructure deployment for rural areas to bridge urban-rural divides have been applied to the deployment of fiber-optic infrastructure, as Japan built high degrees of fiber-optic coverage at an early stage internationally, with 95 percent of metropolitan businesses and residential areas covered by 2001 and almost 100 percent nationwide coverage by 2020 (99.1 percent).[185] Wireless coverage has also been extensive, with internet connectivity as well as platforms for third-party application provided by telecom carriers since the late 1990s, almost a decade before the advent of smartphones. Japanese internet users enjoyed high broadband penetration levels, low prices, and fast connection speeds due to the surprisingly strong regulations that the Ministry of Internal Affairs and Communications (MIC) imposed on the incumbent carrier, NTT, and due to a new regulatory structure that emphasized competition.[186] A new pattern of entrepreneurship emerged in Japan's telecommunications sector: new entrants offered fast services at low prices with support from regulators, a dynamic that led the incumbent NTT to unwillingly adjust course; it was NTT's adjustment away from proprietary networks and services that led to Japan's fast, low-cost broadband.[187] MIC was also active in facilitating mobile virtual network operators, forcing incumbents to lease out their cellular capacity to newcomers.

Although the topic is outside the scope of this piece, it is worth noting that Japan discovered after building out fast, low-cost broadband and advanced mobile services that this was not enough to unleash waves of global innovation. The country very much needed a robust startup ecosystem to make use of this broadband environment. Japan's startup ecosystem has been maturing, but at a slow pace until recently, given the interlocking ingredients needed for a successful ecosystem.[188]

Cybersecurity of Government Systems: Grade C

Various parts of the Japanese government have suffered a wide range of cyber attacks in recent years, including distributed denial-of-service attacks on local governments, government websites, and infrastructure firms including railways and electric companies before the G7 summit in Hiroshima in May 2023 and serious hacking and penetration of Japan's intelligence and defense agencies in 2020.[189] The latter cyber attacks reportedly emanated from the Chinese military, and these attacks highlighted Japan's vulnerabilities and the need for more and better cybersecurity measures.[190]

Japan's response to these pronounced cybersecurity deficiencies was a flurry of administrative centralization and capacity-building. The Ministry of Defense created a new cyber defense unit in 2022 that consolidated several units from the Ground, Maritime, and Air Self-Defense Forces, with plans to increase the number of personnel assigned to cyber defense by a factor of four.[191] The Ministry of Defense will also include a cybersecurity department at the National Defense Academy to train personnel and better equip them to handle cyber defense.[192]

Analysts long have pointed to Japan's constitutional constraints barring it from building offensive capabilities as a hindrance to its cybersecurity capabilities, according to the logic that good defensive capabilities require building and deploying offensive capabilities as well. To address this challenge, the Japanese government announced that it would establish a new legal framework to develop active cyber defense. Japan's cyber defense efforts are embedded into its relationships with U.S. actors, including the activities of some standing groups such as the U.S.-Japanese Cyber Defense Policy Working Group, created in 2013.[193] Based on these developments, Japan receives a C grade, with an A in some areas and an F in others.

Cybersecurity of Nongovernment Systems: Grade C

The Japanese economy consists of a few large, globally competitive corporations and many small- to medium-sized enterprises, the latter of which employ a majority of the population—70 percent according to a 2017 Organisation for Economic Co-operation and Development (OECD) report.[194] The large, globally competitive firms have been shifting their IT infrastructure from proprietary systems provided by Japanese companies such as NTT Data, NEC, and Fujitsu toward systems provided by global U.S.-based cloud service

providers such as Microsoft and Amazon as well as databases and customer relations management software from firms like Oracle, Salesforce, and others. The cybersecurity provided by these firms' systems has put Japan at the forefront of major corporate IT security. However, recent high-profile ransomware and other attacks from various state and nonstate actors have targeted the proprietary or legacy systems used in manufacturing systems and other areas of operation.

Small- to medium-sized businesses in Japan are extremely vulnerable if they are using outdated systems—unless they are so far behind the digital transformation that most processes have limited computerization or are so obsolete that they are not subject to modern cyber attacks (such as local banks that still using floppy disks to transfer data or businesses that rely on fax machines to place orders and communicate.)[195]

A Cyber Risk Index created by Trend Micro, a private company that sells security systems, rates countries around the world. The Cyber Risk Index is a function of the degree of cyber threats facing the countries, measured by a Cyber Threat Index, and the degree to which companies in each country are prepared, measured by a Cyber Prepared Index that is created by sending surveys to companies to assess their level of preparedness. In 2021, Japan ranked as the ninth-most at-risk country, but in 2022, it rose to second-most. The threat increased, but less than the degree of preparedness. However, beyond the ranking itself, these reports are noteworthy for identifying the specific ways in which Japanese companies are vulnerable.[196] The 2021 report noted that Japan was particularly ill prepared against ransomware attacks and that top managers and boards were less involved than their counterparts at firms from other OECD countries in their companies' cybersecurity policies. On the other hand, Japan was ranked highly in efforts to prevent phishing and social engineering. In contrast to firms from other countries in North America, Europe, and Asia, Japanese firms saw cybersecurity threats as most threatening to facilities and physical infrastructure rather than profits or brand image. Japan therefore receives a C grade, with an A in some areas and an F in others.

Digital Identity: Grade B

Japan was a latecomer to implementing digital identities, but as the country implemented a nationwide system it was beset by a peculiar set of scandals that led to delays and postponements in the rollout and integration of various government functions related to the digital identity system. Japan introduced a digital chip-embedded system called My Number Card in 2016, which includes personal information such as a person's name, birth date, address, and passport photo, and a twelve-digit number unique to each individual.

The idea was to streamline and centralize various governmental administrative procedures and data, since official records on citizens and residents had previously been stored by the municipalities where people had registered their permanent domiciles. This required obtaining physical copies of an individual's records from the municipality corresponding to

their permanent domicile, which could be far from and otherwise unrelated to where they actually live. In extreme cases, particularly in rural municipalities, such documents had to be obtained in person in order for the individual to complete administrative tasks like renting an apartment, registering a death or birth in the family, applying for a passport, or opening a bank account.

After some public dissent against creating a national registry that identified people by number, the My Number Card system was implemented, and by July 2023, roughly 70 percent of the population had obtained a card.[197] Japan's digital minister announced that My Number Card would be integrated into the national healthcare system and serve as the national healthcare card. But in 2023, a scandal broke out when over 8,000 cases of mistaken identities involving My Number Card were uncovered by August of that year. It seemed that municipal-level registration procedure errors had led to these problems. It became a significant domestic political issue, and it may have directly contributed to a fall in the approval ratings of Prime Minister Fumio Kishida's administration.[198]

Content Moderation: Grade C

As of January 2024, the Japanese government has been holding discussions about creating rules that would regulate content classified as defamation on social media platforms, including those of U.S. tech companies like Meta, Google, and X (formerly known as Twitter) as well as Japanese firms. The new rules would require platform providers to create avenues for online defamation victims to report cases, clarify and inform users of how the reporting process works, and notify users about the platform's responses within a week.[199]

Data Localization: Grade A

Japan does not have an overarching national legal structure for governing data localization.[200] Only a few specific industries, such as medical information systems, have government-issued guidelines. Importantly, Japan was able to fight off political efforts to impose restrictions on foreign provision of government IT systems when the Digital Agency created specifications to solicit bids for its government-contracted cloud-computing vendors and did not impose additional data localization requirements. In the first two rounds of bids, only U.S.-based global multinationals like Amazon Web Services Google Cloud Platform, Microsoft Azure, and Oracle Cloud Infrastructure submitted bids, and all of them were awarded certification to provide services.[201] Some conservative parliamentarians in the ruling Liberal Democratic Party opposed the selection of U.S.-based multinational firms, arguing that potentially sensitive information should not be in the hands of multinational companies and that data should be stored locally. However, the Digital Agency fought off these claims and proceeded to certify and finalize arrangements with global cloud services, with Amazon Web Services becoming the largest vendor.[202]

CHAPTER 6

Lessons on Standards and Standardization From the United States

Michael R. Nelson

The United States has a very long history of digital leadership. Presidents have been giving speeches about information and communications technologies, launching high-profile projects, and personally using new products and services for at least seventy years. President John F. Kennedy was a champion[203] of communications satellites and pushed hard for the Communications Satellite Act of 1962, which led to the formation of COMSAT, a public, federally funded corporation intended to develop commercial and international satellite communications. Later, in 1973, president Gerald R. Ford got personally involved in pushing for the breakup of AT&T.[204] Late in the twentieth century, president Bill Clinton, with the help of then vice president Al Gore, reached the high-water mark for U.S. digital leadership (so far). Here are some examples of how Clinton and Gore demonstrated their leadership:

- About a month after being inaugurated, they both traveled to Silicon Valley to launch the Clinton administration's new tech policy strategy.[205]
- They launched the White House website, one of the first national government websites anywhere in the world, in 1994.[206]
- Gore was personally involved—for more than three years—in passing the 1996 Telecommunications Act, which removed many of the barriers that were hindering development of a competitive market for commercial internet services.[207]
- The president's National Information Infrastructure Task Force, consisting of key deputy secretaries and agency heads, was created by the White House and tasked with coordinating policy development and resolving differences between departments.[208]

- On the standards side, the White House endorsed the internet protocol, TCP/IP, when many other developed countries were mandating a single standard (the International Telecommunication Union's much less flexible networking standard).

- Clinton and Gore visited schools to personally run internet cables into classrooms.[209]

In each administration, the involvement of the president (or vice president) helped break through bureaucratic logjams and reduce interagency turf fights. Equally importantly, high-profile speeches and events got journalists and the American public to understand new technologies and why they mattered.

In the mid-1990s, the global internet market was measured in billions of dollars and the entire IT sector in the United States totaled a few hundred billion dollars.[210] Today, the size of the U.S. IT sector exceeds $2.6 trillion.[211] In addition, the list of critical policy and standards issues is much longer, and those issues are more complex and interrelated, so the political fights (and the lobbying) are much more intense. That's why digital leadership is even more important today. Another reason is that, unlike in the early 1990s, the United States is not the only digital superpower. Getting digital policy right—and not getting slowed down by conflicting, confusing, and ever-changing policies—is essential if U.S. firms, both large and small, are to grow and compete globally.

The digital leadership report card for the United States is an attempt to indicate where the White House has devoted time and attention to finding consensus on key digital issues (see table 4). These grades reflect the full range of policy levers that presidents can pull: proposing legislation, shaping regulations, promoting the development and adoption of standards, handling procurement, giving speeches, engaging in marketing, and building international support. It's particularly hard to assign just one grade in each policy category when the picture has changed from administration to administration, and new developments like the coronavirus pandemic can spur major new initiatives. Rather than just focusing on the administration of current President Joe Biden (as of January 2024), these grades reflect the progress of the past ten years and also cover the administrations of his two predecessors, former presidents Barack Obama and Donald Trump. These grades reflect the views of just one analyst—but one who has worked on digital policy issues in Washington (and around the world) for more than thirty years. The other caveat is that these grades can change quickly. Another exercise like this in five years might return different results.

Table 4. Report Card on Digital Leadership in the United States

Key Digital Issues	Letter Grade	Notes
Connecting the unconnected	A	
Broadband competition	B	
Encryption	C	
Cybersecurity of government systems	B	
Cybersecurity of nongovernment systems	A	
Digital identity	C	
Content moderation	C	
Data localization	A	Grade is falling.
Data architecture	B	
Data protection	I	
Online copyright	C	

Note: A = superior, B = above average, C = average, F = failing, I = incomplete. The grades only indicate how well or poorly the government is doing in various areas; they cannot be used to compare a country's performance with that of other countries.

Connecting the Unconnected: Grade A

Realizing the vision of nearly universal internet access has been a U.S. policy goal since the 1996 Telecommunications Act, and tens of billions of dollars have been spent on subsidies to realize that goal. Unfortunately, programs have come and gone, and funding levels have oscillated. The coronavirus pandemic highlighted the need for affordable, reliable internet access, which Americans required in order to quarantine and work or study from home. Biden made this a priority and got bipartisan support for 2021 legislation that authorized roughly $65 billion for programs to make internet access more affordable for tens of millions of Americans.[212] More significantly, he's personally championed the programs he has created, which tends to make sure agencies implement them quickly and effectively.[213] He has now made broadband access a part of his standard campaign pitch as he runs for reelection in 2024. Unlike his predecessors, who often spoke of the need for internet access but could not get bipartisan support for bold, new programs, Biden and his administration have earned an "A." However, there is more to be done, and getting Congress to renew the funding provided by the 2021 legislation will not be easy without a great deal of digital leadership.[214]

Broadband Competition: Grade B

In mid-2021, most studies found that at least 50 percent of Americans had at least two affordable choices when it came to internet access.[215] Projections predict that that number could exceed 80 percent or even 90 percent by the end of 2025.[216] Telephone companies, cable television companies, wireless providers, and now satellite companies like Starlink

provide alternatives. White House decisions over the past ten years have helped foster competition. For example, it has often taken a push from the White House to get the Department of Defense to give up spectrum reserved for military uses so it could be used for commercial services. While there have not been high-profile speeches and statements on broadband competition, consumers have more choices today than ten years ago.

Encryption: Grade C

Strong encryption is not just needed to encrypt data transmitted over the internet. It is also vital to keeping data secure and private in data centers and on cellphones, computers, and other devices. Unfortunately, over the past ten years, U.S. statements and actions regarding encryption policy have been inconsistent—both domestically and internationally. During the Trump administration, the National Institute of Standards and Technology stressed the need for widespread deployment of strong encryption,[217] while then attorney general Bill Barr was advocating for encryption backdoors to give law enforcement access to stored data and communications.[218] The Biden administration has been no more consistent, advocating for law enforcement access at the Five Eyes meetings with allied intelligence agencies and not opposing (at least publicly) proposals from the United Kingdom that would require companies to decrypt encrypted messages.

Cybersecurity of Government Systems: Grade B

U.S. cybersecurity for government systems is an area where the Obama, Trump, and Biden administrations have been surprisingly consistent. This is in part because no White House wants to have to explain a major government data breach during its watch. Unfortunately, each of the last three presidents has had to do so.[219] Over the past ten years, the number of White House staff focusing on cybersecurity has increased, and the responsibilities of relevant offices and agencies have been more clearly defined. Importantly, in several cases key personnel at the White House and in the Department of Homeland Security dealing with cybersecurity carried over from one administration to the next.

Cybersecurity of Nongovernment Systems: Grade A

While the battle between malicious hackers and corporate information-technology teams is never-ending, in the United States, corporations have been devoting more resources to cyber defense and recovery from cyber attacks. The rise of ransomware in recent years has raised the stakes even higher and expanded the range of potential victims to include even small health clinics and mom-and-pop stores. Fortunately, more and more industry sectors have organized information-sharing and analysis centers and similar organizations to inform companies and nonprofit organizations about the threats they face and what measures they might take to address them. Various agencies have taken steps to encourage corporate boards

to address the threat of cyber attacks and divulge them when they occur. Because these efforts are more bottom-up than top-down, there is less need for digital leadership from the White House here.

Digital Identity: Grade C

In countries like Estonia, Korea, and India, establishing a national digital identity system that every citizen could use (and, in some cases, *must* use) has been a high priority of each country's president or prime minister. In contrast, U.S. government efforts to set digital identity standards, foster interoperability, encourage privacy-enhancing approaches, and promote the use of better digital identity technology have been scattershot and start-stop. Unfortunately, many Americans resist the idea of a national identification card (something that's commonplace in almost every other developed country). A president who used his or her bully pulpit to describe the huge benefits and savings that a better approach to digital identity could provide could be very helpful.

Content Moderation: Grade C

Over the past five years, few digital policy issues have been as emotional and political as the debate about what internet companies should block or filter online (particularly on social media platforms). Unfortunately, positions articulated by presidents and members of Congress have often been vehement, too simplistic, and self-contradictory. Too often, their statements boil down to something along these lines: "I support free speech wholeheartedly, but find a way to block stuff I don't like, and, whatever you do, do not block or shadow ban what I or people I agree with want to say." A key issue has been Section 230 of the Communications Decency Act, passed in 1996, which shields internet companies from being liable for content that their customers share using their services. Biden has stated unequivocally that he feels Section 230 should be "revoked, immediately,"[220] but he has not indicated which parts or what he'd replace it with; furthermore, he has invested almost no effort in working with Congress to find solutions to the many facets of the problem of unwanted or harmful content online.

Data Localization: Grade A (but falling fast)

For decades, under both Democratic and Republican administrations, the United States has been a strong supporter of cross-border data flows. It has worked through organizations such as the World Trade Organization (WTO), the Organisation for Economic Co-operation and Development, and the G7 to oppose data localization or regulations and nontariff barriers that block U.S. companies from providing services in other countries. Both parties in the U.S. Congress have supported this policy. Thus, it came as an incredible surprise when, in late October 2023, the U.S. Trade Representative announced that the United States would

no longer be pushing measures opposing data localization at the WTO.[221] The justification was unclear and poorly communicated to the business community and the public. Even more stunning was the way the policy reversal was made. Key agencies deeply involved in trade and digital issues were not part of the decisionmaking process, and, in some cases, they were not even informed that the announcement was coming. Pro-business organizations were furious and issued strong statements and policy papers opposing the move.[222] This seems like a clear example of how not to provide digital leadership. Administrations are free to make major shifts in policy but to do so without informing previous allies and foreign government partners seems to be a major mistake that could do lasting damage.[223]

Data Architecture: Grade B

Data policy has been a backwater of digital policy for decades. Data is a bit like electricity or drinking water: it's essential, but average citizens do not pay much attention to how it's produced and distributed. That's changing now that the rise of machine learning applications is leading to powerful new tools being applied across the economy and generating hundreds of billions of dollars in investment. High-quality, unbiased troves of big data are essential not only for artificial intelligence (AI) but also for potentially accelerating research in a range of fields including economics, epidemiology, and public safety. But the public needs to understand how data is being collected, how it will be protected, and how making more data available for new AI applications could help them live better lives. India has been a leader in developing its Data Empowerment and Protection Architecture, which is designed to tap into a wide range of government data and corporate data (often in an anonymized form).[224] This effort is very ambitious, especially for a nation of more than 1 billion people.

In contrast, the U.S. government has taken a more fragmented approach, with different agencies and industry consortia focused on different types of data related to different fields of research and business. Support for open data initiatives to make nonpersonal government data more accessible has ebbed and flowed. This is an area where there could be a huge return on investment if the White House could articulate a vision for how data governance could benefit average Americans and provide better privacy protection and cybersecurity.

Data Protection: Grade I

Data protection is related to questions of data governance and data infrastructure. Since even before the birth of the commercial internet, there have been companies that abuse data that has been collected online. The result has been a series of narrow policy proposals to address a narrow, sector-specific problem. For instance, in the Cambridge Analytica scandal, a company from the United Kingdom violated the privacy of Facebook customers (and the contract Cambridge Analytica executives had signed with Facebook) in order to use Facebook users' data to target them with election ads. Not only was Facebook pilloried, but Cambridge Analytica was sued and eventually forced to close. In addition, the Biden

administration has expanded programs to monitor and prevent digital election meddling. As more and more incidents like this have come to light, the pressure on the White House and Congress to pass comprehensive data protection legislation has increased. The Obama administration proposed a Consumer Privacy Bill of Rights, and, after their inauguration, many had expected Biden and Vice President Kamala Harris to build upon it.[225] But, for the past three years, most of the action on data protection has been happening in state capitols (or in cities, where restrictions on facial recognition are becoming more common). There are many reasons for this: hyper-partisan politics on Capitol Hill; the war in Ukraine and now the conflicts in the Middle East; and, perhaps most importantly, a lack of clear ideas on how to deal with the new privacy challenges posed by emerging technologies such as AI and the Internet of Things and by data brokers who build profiles for consumers by combining data from hundreds of databases. As Byoung-il Oh explained in an earlier chapter, Korea faces similar challenges in the country's debate over how to use big data and how anonymization could provide a partial solution to the tensions between users' need for privacy and companies' (and government actors') need for data.

Online Copyright: Grade C

Experts have been arguing about how to adapt copyright protections to the digital world for more than thirty years. One thing that is clear is that having different rules for different modes of delivering digital content (such as rules for streaming that differ from rules for downloads) makes little sense. Reforms are needed. It's also very clear that AI developers will be able to innovate faster if new approaches to copyright protections remove barriers to the use of copyrighted material in the training sets needed to train machine-learning algorithms. These are incredibly complex and thorny issues, and no one anywhere seems to be making much progress. Instead, courts are stepping in to make policy in a very patchwork and inconsistent fashion.

About the Authors

Evan A. Feigenbaum is a vice president for studies at the Carnegie Endowment for International Peace, where he oversees research in Washington, Beijing, New Delhi, and Singapore on a dynamic region encompassing both East Asia and South Asia. He was also the 2019–2020 James R. Schlesinger Distinguished Professor at the Miller Center of Public Affairs at the University of Virginia, where he is now a practitioner senior fellow.

Initially an academic with a PhD in Chinese politics from Stanford University, Feigenbaum's career has spanned government service, think tanks, the private sector, and three major regions of Asia. From 2001 to 2009, he served at the U.S. State Department as deputy assistant secretary of state for South Asia (2007–2009), deputy assistant secretary of state for Central Asia (2006–2007), member of the policy planning staff with principal responsibility for East Asia and the Pacific (2001–2006), and an adviser on China to deputy secretary of state Robert B. Zoellick, with whom he worked closely in the development of the U.S.-China senior dialogue. Following government service, Feigenbaum worked in the private and nonprofit sectors. He was vice chairman of the Paulson Institute at the University of Chicago and the co-founder of MacroPolo, its digital venture on the Chinese economy; head of the Asia practice at the markets consultancy Eurasia Group; and senior fellow for Asia at the Council on Foreign Relations.

Before government service, he worked at Harvard University as lecturer on government in the faculty of arts and sciences and as executive director of the Asia-Pacific Security Initiative and program chair of the Chinese Security Studies Program in the John F. Kennedy School of Government, and he was lecturer of national security affairs at the U.S. Naval Postgraduate School. He is the author of three books and monographs, including *The United States in the New Asia* and *China's Techno-Warriors: National Security and Strategic Competition From the Nuclear to the Information Age.*

Michael R. Nelson is a senior fellow in the Carnegie Endowment's Technology and International Affairs Program, which helps decisionmakers understand and address the impacts of emerging technologies, including digital technologies, biotechnology, and artificial intelligence. Prior to joining Carnegie, he started the global public policy office for Cloudflare, a startup that has improved the performance and security of more than 10 million websites around the world. Nelson has also served as a principal technology policy strategist in Microsoft's Technology Policy Group and before that was a senior technology and telecommunications analyst with Bloomberg Government. In addition, Nelson has been teaching courses and doing research on the future of the internet, cyber policy, technology policy, innovation policy, and e-government in the Communication, Culture, & Technology Program at Georgetown University.

Before joining the Georgetown faculty, Nelson was director of internet technology and strategy at IBM, where he managed a team helping define and implement IBM's next-generation internet strategy. He has served as chairman of the Information, Communication, and Computing Section of the American Association for the Advancement of Science, serves as a trustee of the Institute for International Communications, and was selected to be a "Global Leader of Tomorrow" by the World Economic Forum. From 1988 to 1993, he served as a professional staff member for the Senate's Subcommittee on Science, Technology, and Space and was the lead Senate staffer for the High-Performance Computing Act. In 1993, he joined then vice president Al Gore at the White House and worked with then president Bill Clinton's science adviser on issues relating to the Global Information Infrastructure, including telecommunications policy, information technology, encryption, electronic commerce, and information policy.

Dasom Lee is an assistant professor in the Graduate School of Science and Technology Policy at the Korea Advanced Institute of Science and Technology (KAIST).

She received her PhD in sociology and a minor in quantitative methods from Vanderbilt University. She worked as a tenured assistant professor at the University of Twente in the Netherlands before joining KAIST.

Lee specializes in societal challenges and regulations related to artificial intelligence. In particular, she focuses on identifying societal and legal challenges of AI and cyber-physical systems and publishes on regulatory solutions and harmonization. She is an associate editor for *ACM Journal on Responsible Computing*, and she is an editorial board member for *Humanities and Social Sciences Communications*.

Byoung-il Oh is the president of the Korean Progressive Network Jinbonet, an organization based in South Korea that advocates for human rights in the information society, especially the rights to communication, free speech, and privacy. He is a founding member of Jinbonet and has been working as a full-time staff member since its founding in 1998. He has been the organization's president since 2019.

Starting in 1999, Oh worked as a board member of IPLeft, a nongovernmental organization that has criticized the strengthening of intellectual property and promoting A2K. He was the representative of the organization from 2009 to 2023.

Oh has been involved in internet resource policies as a member of the name committee of the Name&Number Committee, which was an internet governance body in the early 2000s. Currently, he is a research fellow at the Institute for Digital Rights. He is a steering committee member of Korea Internet Governance Alliance and the chair of the South Korean Internet Governance Forum's program committee.

Elina Noor is a senior fellow in the Asia Program at Carnegie where she focuses on developments in Southeast Asia, particularly the impact and implications of technology in reshaping power dynamics, governance, and nation-building in the region.

Previously, Elina was director of political-security affairs and deputy director of the Washington, DC, office at the Asia Society Policy Institute. Prior to that, Elina was an associate professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies in Honolulu. She spent most of her career at the Institute of Strategic and International Studies Malaysia, where she last held the position of director, foreign policy and security studies. Elina was also formerly with the Brookings Institution's Project on U.S. Relations with the Islamic World.

Between 2017 and 2019, Elina was part of the Global Commission on the Stability of Cyberspace. From 2021 to 2023, she served on the International Committee of the Red Cross Global Advisory Board on digital threats during conflict. She currently serves on the United Nations Secretary-General's Advisory Board on Disarmament Matters.

Elina read law at Oxford University. She obtained an LL.M (Public International Law) from the London School of Economics and Political Science, University of London, graduating with distinction at the top of her class. A recipient of the Perdana (Malaysian Prime Minister's) Fellowship, she also holds an MA in security studies from Georgetown University, where she was a Women in International Security Scholar.

Kenji E. Kushida is a senior fellow for Japan studies in Carnegie's Asia Program, directing research on Japan, including a new Japan-Silicon Valley Innovation Initiative at Carnegie. He was formerly a research scholar with the Japan Program at the Walter H. Shorenstein Asia-Pacific Research Center at Stanford University.

Kushida's research and projects are focused in five streams: (1) Japan's transforming political economy; (2) how politics and regulations shape the development and diffusion of information technology such as artificial intelligence; (3) institutional underpinnings of the Silicon Valley ecosystem; (4) Japan's startup ecosystem; and (5) the role of foreign multinational firms in Japan. He has published several books and numerous articles in each of these streams and is the author of books and monographs in Japanese and English.

Kushida has appeared in media including the *New York Times*, *Washington Post*, *Nihon Keizai Shimbun*, *Nikkei Business*, *Diamond Harvard Business Review*, NHK, PBS NewsHour, and NPR. He is also a trustee of the Japan ICU Foundation, an alumnus of the Trilateral Commission David Rockefeller Fellows program, and a member of the Mansfield Foundation Network for the Future.

Kushida holds a PhD in political science from the University of California, Berkeley. He received his MA in East Asian studies and his BA in economics and East Asian studies with honors, all from Stanford University.

Notes

Introduction

1 "GDP (Current US$), Korea, Rep.," World Bank, 2022, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=KR.

2 Evan A. Feigenbaum and Michael R. Nelson, *The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way*, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/korean-way-with-data-how-world-s-most-wired-country-is-forging-third-way-pub-85161.

3 Evan A. Feigenbaum and Michael R. Nelson, *Data Governance, Asian Alternatives: How India and Korea Are Creating New Models and Policies*, Carnegie Endowment for International Peace, August 21, 2022, https://carnegieendowment.org/2022/08/31/data-governance-asian-alternatives-how-india-and-korea-are-creating-new-models-and-policies-pub-87765.

4 Kyung Sin "KS" Park and Michael R. Nelson, "Afterword: Korea's Challenge to the Standard Internet Interconnection Model, " in *The Korean Way With Data*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166.

5 So Jeong Kim and Sunha Bae, "Korean Policies of Cybersecurity and Data Resilience," in *The Korean Way With Data*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164.

6 Jang Gyehyun and Lim Jong-in, "Technologies of Trust: Online Authentication and Data Access Control in Korea," in *The Korean Way With Data*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/technologies-of-trust-online-authentication-and-data-access-control-in-korea-pub-85163.

7 Nohyoung Park, "A Korean Approach to Data Localization," in *The Korean Way With Data*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/korean-approach-to-data-localization-pub-85165; and Kyung Sin "KS" Park, "Korea's Path to Best Practices for Cross-Border Data Flows," in *Data Governance, Asian Alternatives: How India and Korea Are Creating New Models and Policies*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 31, 2022, https://carnegieendowment.org/2022/08/31/korea-s-path-to-best-practices-for-cross-border-data-flows-pub-87770.

8 International Telecommunication Union, "Measuring Digital Development: ICT Development Index 2023," 2023, https://www.itu.int/itu-d/reports/statistics/IDI2023.

Chapter 1

9 Carl Cargill, "Standardization, Not Standards Matter," in *Corporate Standardization Management and Innovation*, ed. Kai Jacobs (IGI Global, 2019), 1–15, https://www.researchgate.net/publication/333128581_Standardization_Not_Standards_Matter.

10 National Institute of Standards and Technology, "Quick Start Guide," August 2021, https://www.nist.gov/cyberframework/getting-started/quick-start-guide.

11 "Online Authentication and Data Access Control in Korea," Jang Gyehyun and Lim Jong-in, in *The Korean Way With Data: How the World's Most Wired Nation Is Forging a Third Way*, Carnegie Endowment for International Peace, 2021, https://carnegieendowment.org/2021/08/17/technologies-of-trust-online-authentication-and-data-access-control-in-korea-pub-85163w.

12 Mike Dano, "The COVID-19 Traffic Surge Is Over, Now It's Time to Tind the New Baseline," Light Reading, April 29, 2020, https://www.lightreading.com/optical-networking/the-covid-19-traffic-surge-is-over-now-it-s-time-to-find-the-new-baseline.

13 Kyung Sin "KS" Park and Michael R. Nelson, "Afterword: Korea's Challenge to the Standard Internet Interconnection Model," in *The Korean Way With Data*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166.

14 Trevor Wagener, "Myths Surrounding Network Usage Fees: South Korea," Computer and Communication Industry Association, November 21, 2023, https://ccianet.org/wp-content/uploads/2023/11/CCIA_Myths-Surrounding-Network-Usage-Fees-South-Korea.pdf.

15 Computer and Communications Industry Association, "Joint Industry Statement on Network Fees," October 20, 2023, https://ccianet.org/library/joint-industry-statement-on-network-fees.

16 Encryption Working Group, "Moving the Encryption Policy Conversation Forward," Carnegie Endowment for International Peace, September 2019, https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573.

17 Emma Woollacott, "U.K. Plans More Powers Over Tech Firms With Amended Snoopers' Charter," *Forbes*, November 7, 2023, https://www.forbes.com/sites/emmawoollacott/2023/11/07/uk-plans-more-powers-over-global-tech-firms/?sh=20df19101682.

18 "G7 Leaders Endorsed a Digital Ministers' Roadmap for Cooperation on Data Free Flow With Trust," European Union, July 7, 2021, https://data.europa.eu/en/news-events/news/g7-leaders-endorsed-digital-ministers-roadmap-cooperation-data-free-flow-trust?.

19 Alex Pentland, Alexander Lipton, and Thomas Hardjono, eds., "Building the New Economy · Works in Progress," *Works in Progress*, 2020, https://doi.org/10.21428/ba67f642.0499afe0; and Stanford Digital Economy Lab, "Building the New Economy: Data as Capital," November 17, 2022, https://digitaleconomy.stanford.edu/event/building-the-new-economy-data-as-capital.

20 Rahul Matthan and Shreya Ramann, "India's Approach to Data Governance," in *Data Governance, Asian Alternatives*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 2022, https://carnegieendowment.org/2022/08/31/india-s-approach-to-data-governance-pub-87767.

21 Lauren Ditzel, "J.K. Rowling Removes 'Harry Potter' Copyright to Allow Teaching," Bookstr, March 23, 2020, https://archive.bookstr.com/article/j-k-rowling-removes-harry-potter-copyright-to-allow-teaching.

22 "Internet Archive's Digital Library Has Been Found in Breach of Copyright. The Decision Has Some Important Implications," Conversation, August 22, 2023, https://theconversation.com/internet-archives-digital-library-has-been-found-in-breach-of-copyright-the-decision-has-some-important-implications-212091.

Chapter 2

23 "ISO - Structure and Governance," International Organization for Standardization, accessed February 4, 2024, https://www.iso.org/structure.html.

24 Robert H. Allen and Ram D. Sriram, "The Role of Standards in Innovation," *Technological Forecasting and Social Change* 64, no. 2–3 (2000): 171–181, https://doi.org/10.1016/S0040-1625(99)00104-3; and "Benefits of ISO Standards," International Organization for Standardization, accessed February 4, 2024, https://www.iso.org/benefits-of-standards.html.

25 Allen and Sriram, "The Role of Standards in Innovation"; Hong Jiang et al., "Competition of Technology Standards in Industry 4.0: An Innovation Ecosystem Perspective," *Systems Research and Behavioral Science* 37, no. 4 (2020): 772–783, https://doi.org/10.1002/sres.2718; and Timothy Simcoe, "Standard Setting Committees: Consensus Governance for Shared Technology Platforms," *American Economic Review* 102, no. 1 (2012): 305–336, https://www.aeaweb.org/articles?id=10.1257/aer.102.1.305.

26 "ID4D Practitioner's Guide," World Bank Group, October 2019, 195, http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide.

27 Katrin Hussinger and Franz Schwiebacher, "The Market Value of Technology Disclosures to Standard Setting Organizations," *Industry and Innovation* 22, no. 4 (May 19, 2015): 321–344, https://doi.org/10.1080/13662716.2015.1049866; and Timothy Simcoe, "Explaining the Increase in Intellectual Property Disclosure," SSRN Scholarly Paper, December 1, 2005, https://doi.org/10.2139/ssrn.1396332.

28 Leigh Dayton, "How South Korea Made Itself a Global Innovation Leader," *Nature* 581, no. 7809 (May 28, 2020): S54–S56, https://doi.org/10.1038/d41586-020-01466-7; and Tae Kyung Sung, "Industry 4.0: A Korea Perspective," *Technological Forecasting and Social Change* 132 (2018): 40–45, https://doi.org/10.1016/j.techfore.2017.11.005.

29 Michelle Jamrisko, Wei Lu, and Alex Tanzi, "South Korea Leads World in Innovation as U.S. Exits Top Ten (1)," Bloomberg Law, February 3, 2021, https://news.bloomberglaw.com/ip-law/south-korea-leads-world-in-innovation-as-u-s-exits-top-ten-1.

30 Soumitra Dutta et al., "Global Innovation Index 2022: What Is the Future of Innovation-Driven Growth?," World Intellectual Property Organization, 2022, https://doi.org/10.34667/TIND.46596.

31 Dutta et al., "Global Innovation Index 2022."

32 Silvia Appelt et al., "A Global Powerhouse in Science and Technology," Organisation for Economic Co-operation and Development, October 25, 2021, https://www.oecd.org/country/korea/thematic-focus/a-global-powerhouse-in-science-and-technology-61cbd1ad.

33 Appelt et al., "A Global Powerhouse in Science and Technology."

34 "Korea to Come Up With the Roadmap of Digital ROK, Realizing the New York Initiative," South Korean Ministry of Science and ICT, September 28, 2022, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=742.

35 "국제표준화기구(ISO) 수장으로 한국인 최초 당선," Korean Agency for Technology and Standards, September 9, 2022, https://blog.naver.com/katsblog/222882089965.

36 In Korean, KATS is called국가기술표준원.

37 "한국산업표준," Korean Agency for Technology Standards, accessed February 4, 2024, https://www.kats.go.kr/content.do?cmsid=28.

38 "한국산업표준," Korean Agency for Technology Standards.

39 In Korean, the Industrial Standard Review Committee is called 산업표준심의회.

40 In Korean, the relevant technical review committee is called 기술심의회.

41 In Korean, the specialized committee is called 전문위원회.

42 Jong-gi Kim et al., "디지털 전환 가속화에 따른 ICT산업의 신성장전략," Korea Institute for Industrial Economics and Trade, December 31, 2021, https://www.kiet.re.kr/research/reportView?report_no=1029.

43 JH Bae, "Korea, China Join Forces to Set a Global Standard for 5G Mobile Technology," KIPOST, July 5, 2013, https://www.kipost.net/news/articleView.html?idxno=54694; and Dan Meyer, "EC, South Korea to Work Towards Common 5G Standard," RCR Wireless News, June 16, 2014, https://www.rcrwireless.com/20140616/network-infrastructure/ec-south-korea-work-towards-common-5g-standard.

44 Korea Information Society Development Institute, *2022 ICT Industry Outlook of Korea* (2021): 36, https://mediasvr.egentouch.com/egentouch.media/apiFile.do?action=view&SCHOOL_ID=1007002&URL_KEY=22ed8f99-548d-424c-a1de-7acfdfb1944b.

45 Jieun Park, Seongcheol Kim, and Changi Nam, "Why Has a Korean Telecommunications Technology Failed: A Case Study on WiBro," *Telematics and Informatics* 32, no. 4 (2015): 603–612, https://doi.org/10.1016/j.tele.2015.01.002.

46 Doil Son et al., "5G Regulation and Law in South Korea," CMS, 2023, https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/south-korea.

47 "5G System Overview," 3rd Generation Partnership Project (3GPP), 2022, https://www.3gpp.org/technologies/5g-system-overview.

48 DJ Kim, YJ Jeong, and HY Lee, "5G 표준화 추진 동향 및 전망," *TTA Journal* 175, no. 21 (2018): https://koreascience.kr/article/JAKO201867551543473.pdf; and Hyeyoung Lee and Yongjun Jeong, "5G, 표준화의 성공 - 그리고 미래를 위한 노력," *TTA Journal* 184 (2019): https://www.tta.or.kr/tta/preportNewsNDownload.do?sfn=20230506112746829_RxbP.pdf.

49 Guang Yang, "Who Are the Leading Players in 5G Standardization? An Assessment for 3GPP 5G Activities," Strategy Analytics, 2020, https://www.strategyanalytics.com/access-services/service-providers/networks-and-service-platforms/reports/report-detail/who-are-the-leading-players-in-5g-standardization-an-assessment-for-3gpp-5g-activities.

50 "5G Patents Held by Leading Companies World Wide as of September 2021," Statista, November 29, 2023, https://www.statista.com/statistics/1276457/leading-owners-of-5g-patents-worldwide.

51 Francesco Gavino Brundu et al., "IoT Software Infrastructure for Energy Management and Simulation in Smart Cities," *IEEE Transactions on Industrial Informatics* 13, no. 2 (2017): 832–840, https://doi.org/10.1109/TII.2016.2627479; and Anurag Verma et al., "Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review," *IEEE Sensors Journal* 19, no. 20 (October 15, 2019): 9036–9046, https://doi.org/10.1109/JSEN.2019.2922409.

52 In Korean, the town is called 구자읍.

53 Seungrok Lee, "93억 들인 홍보관 3년째 방치...'세계 최대 실증단지' 지금은?' 제주의소리," Jejusori, February 28, 2019, http://www.jejusori.net/news/articleView.html?idxno=300031; Jean K. Min, "Jeju, Test-Bed for the World's Smart Grid Industry," *Jeju Weekly*, February 5, 2011, http://www.jejuweekly.net/news/articleView.html?idxno=1222; and Moon-hee Choi, "A Self-Driving Mobility Service Launched in Jeju," Business Korea, November 3, 2022, https://www.businesskorea.co.kr/news/aticleView.html?idxno=103370.

54 Auto View, "제네시스, 레벨 3 주행 속도 100km/h로 상향... 공개는 연말," March 31, 2023, https://www.autoview.co.kr/news/articleView.html?idxno=79662; and Young-sil Yoon, "Hyundai Motor Group to Launch Genesis G90, Kia EV9 Powered by Level 3 Autonomous Driving Technology in April," Business Korea, March 15, 2023, http://www.businesskorea.co.kr/news/articleView.html?idxno=110971.

55 Dasom Lee and David J. Hess, "Data Privacy and Residential Smart Meters: Comparative Analysis and Harmonization Potential," *Utilities Policy* 70 (2021): https://doi.org/10.1016/j.jup.2021.101188.

56 Lee and Hess, "Data Privacy and Residential Smart Meters."

57 Dasom Lee, David J. Hess, and Himanshu Neema, "The Challenges of Implementing Transactive Energy: A Comparative Analysis of Experimental Projects," *Electricity Journal* 33, no. 10 (2020): https://doi.org/10.1016/j.tej.2020.106865.

58 Pascal A. Schirmer, Iosif Mporas, and Akbar Sheikh-Akbari, "Identification of TV Channel Watching From Smart Meter Data Using Energy Disaggregation," *Energies* 14, no. 9 (April 27, 2021): https://doi.org/10.3390/en14092485.

59 Jae-gu Park, "'스마트그리드 표준화 포럼' 출범," Korea Nuclear Power Times, June 4, 2010, http://www.knpnews.com/news/articleView.html?idxno=1289.

60 Min, "Jeju, Test-Bed for the World's Smart Grid Industry."

61 Jeong-ho Kim, "폭망한 스마트그리드의 교훈...제주 미래성장산업은 어디로," 제주의소리, January 6, 2023, http://www.jejusori.net/news/articleView.html?idxno=410979.

62 Kim Seungbeom, "제주 스마트그리드 사업 '용두사미' 그치나," 제주일보, July 30, 2019, http://www.jejunews.com/news/articleView.html?idxno=2143092.

63 "SAE Levels of Driving Automation™ Refined for Clarity and International Audience," SAE International, May 3, 2021, https://www.sae.org/site/blog/sae-j3016-update.

64 For more information on the standards published by ISO, refer to International Organization for Standards, "Standards by ISO/TC 204: Intelligent Transport Systems," accessed February 4, 2024, https://www.iso.org/committee/54706.html.

65 "미래자동차 산업 발전전략 발표," South Korean Ministry of Trade, Industry, and Energy, 2019, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156355724.

66 Johannes Deichmann, "Autonomous Driving's Future: Convenient and Connected," McKinsey, January 6, 2023, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-drivings-future-convenient-and-connected.

67 "제네시스 G90 "세상에서 가장 빠른 자율주행 레벨3 시속 100km 상향 추진," AutoHerald, March 2023, https://www.autoherald.co.kr/news/articleView.html?idxno=46775.

68 Joo-Jeong Moon, "한-미 자율주행 표준 협력체계 구축," ZDNET Korea, December 14, 2022, https://zdnet.co.kr/view/?no=20221214152607.

69 Kyung-min Nam, "국표원, 자율차 표준화 추진 전략 수립 간담회 개최," Korean Agency for Technology and Standards, March 23, 2023, https://www.kats.go.kr/content.do?cmsid=240&cid=23662&mode=view.

70 "자율주행차 상용화 시대, 표준화로 앞당긴다," Korean Agency for Technology Standards, November 16, 2021, https://www.kats.go.kr/mobile/content.do?cmsid=482&skin=/mobile/&mode=view&page=1&cid=22715.

71 "자율주행차 안전성 높인다… 레벨3 안전기준 개정 추진," South Korean Ministry of Land, Infrastructure and Transport, May 26, 2022, http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?lcmspage=1&id=95086742.

72 "ETRI, 자율주행 레벨 국제표준 에디터 선임," Electronics and Telecommunications Research Institute, April 25, 2023, https://blog.naver.com/etripr/223084756861.

73 Darrell Etherington, "Samsung Acquires LoopPay, Maker Of An Apple Pay Competitor," TechCrunch, February 18, 2015, https://techcrunch.com/2015/02/18/samsung-acquires-looppay-maker-of-an-apple-pay-competitor.

74 "2022 인터넷 이용자 조사 NPR," NASMEDIA, 2022, https://www.nasmedia.co.kr/wp-content/uploads/2022/04/1.nasreport328-2022_NPR_%EC%9A%94%EC%95%BD%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf.

75 Korea Economic Daily, "韓, 간편결제 서비스 '애플페이' 도입 가능성에 이목 집중," S&T GPS, September 17, 2022, https://now.k2base.re.kr/portal/trend/mainTrend/view.do?poliTrndId=TRND0000000000047686&menuNo=200004&pageUnit=10&pageIndex=14.

76 Jinju Kim, "IC단말기에 NFC 기능 추가 놓고 카드사 갈등," 한국일보, March 11, 2015, https://www.hankookilbo.com/News/Read/201503110481061180?t=20240205074206.

77 Seul-gi Chang, "애플페이에 튄 불똥…'한국만 호구? 수수료 낮춰야'," Korea Economy TV, July 20, 2023, https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202307200138; and Ryu Jeong-hyeon, "궁지에 몰린 애플페이 수수료…신한·KB·BC카드 '고민되네,'" SBS Biz, October 19, 2023, https://biz.sbs.co.kr/article/20000140069.

78 Alex Hern, "Apple Pay Launches in US," *Guardian*, October 16, 2014, https://www.theguardian.com/technology/2014/oct/16/apple-pay-launches-us-contactless-mobile-payments.

79 Seonyoung Lee, "카드사와 '상생' 택한 삼성페이, 애플페이로 향하는 화살," BizFACT, July 21, 2023, https://news.tf.co.kr/read/economy/2032066.htm.

80 Yeong-San Han, "NFC 표준 기술 분석 및 전망," *Korea Multimedia Society* 16, no. 3 (2012): 17–23, https://koreascience.kr/article/JAKO201203939213657.pdf.

81 Yeon W Lee, "Enhancing Shared Value and Sustainability Practices of Global Firms: The Case of Samsung Electronics," *Strategic Change* 28, no. 2 (2019): 139–145, https://doi.org/10.1002/jsc.2255.

82 Jay Hyuk Rhee, René Bohnsack, and Sam Lee, "Hyundai Motor Company Case – Fostering Social Enterprises," in *The Role of Corporate Sustainability in Asian Development*, ed. Gilbert Lenssen, Jay Hyuk Rhee, and Fabien Martinez (Cham: Springer International Publishing, 2017): 119–143, https://doi.org/10.1007/978-3-319-45160-2_7.

83 Heoi Seung Kim, "최대실적 현대차 기아 2099억원 기부… 삼성전자 제쳐," November 22, 2023, https://www.hani.co.kr/arti/economy/marketing/1117369.html.

84 Nasiopoulos K. Dimitrios, Damianos P. Sakas, and D.S. Vlachos, "The Role of Information Systems in Creating Strategic Leadership Model," *Procedia - Social and Behavioral Sciences* 73 (2013): 285–293, https://doi.org/10.1016/j.sbspro.2013.02.054.

85 Jinkyo Shin, Md Alamgir Mollah, and Jaehyeok Choi, "Sustainability and Organizational Performance in South Korea: The Effect of Digital Leadership on Digital Culture and Employees' Digital Capabilities," *Sustainability* 15, no. 3 (January 20, 2023): https://doi.org/10.3390/su15032027.

86 "Governance and Management of Corporate Citizenship," Conference Board, July 20, 2022, https://www.conference-board.org/topics/corporate-social-impact-practices/governance-and-management-of-corporate-citizenship-overview.

87 Brad Biddle et al., "The Expanding Role and Importance of Standards in the Information and Communications Technology Industry," *Jurimetrics* 52, no. 2 (2012): 177–208, https://heinonline.org/HOL/LandingPage?handle=hein.journals/juraba52&div=16&id=&page=; and Sujai Shivakumar, "Securing Global Standards for Innovation and Growth," Center for Strategic and International Studies, January 27, 2022, https://www.csis.org/analysis/securing-global-standards-innovation-and-growth.

Chapter 3

88 International Telecommunication Union, "Measuring Digital Development: ICT Development Index 2023," 2023, https://www.itu.int/itu-d/reports/statistics/IDI2023.

89 International Telecommunication Union, "Measuring the Information Society Report 2017: Executive Summary," 2017, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2017-SUM-PDF-E.pdf.

90 "Guidelines for De-identification of Personal Data," South Korean Ministry of the Interior and Safety, June 30, 2016, https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000827480&fileSn=1.

91 "시민단체, 고객정보 3억4천여만 건 무단결합한 비식별화 전문기관 및 20개 기업 고발," Korean Progressive Network 'Jinbonet,' press release, November 9, 2017, https://act.jinbo.net/wp/33555.

92 "Recital 26 of the General Data Protection Regulation," Intersoft Consulting, European Union, accessed February 14, 2024, https://www.privacy-regulation.eu/en/recital-26-GDPR.htm.

93 "Results of the 3rd Regulatory and Institutional Innovation Hackathon," Presidential Committee on the Fourth Industrial Revolution, April 6, 2018, http://webarchives.pa.go.kr/19th/www.4th-ir.go.kr/pressRelease/detail/57?category=report.

94 "Data regulation innovation, a blueprint came out. - On 11.15, amendments to three laws related to personal information protection were proposed in the National Assembly," Ministry of the Interior and Safety, November 22, 2018, https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=67218.

95 Several user rights advocates were outspoken in their opposition. For example, see "개인정보 도둑법 강행하는 정부 규탄한다," Jinbonet, December 9, 2019, https://act.jinbo.net/wp/41952.

96 "Personal Information Protection Act," Korea Law Translation Center, March 14, 2023, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=62389&type=part&key=4.

97 "Personal Information Protection Act," Korea Law Translation Center.

98 "Personal Information Protection Act – All Reasons for Enactment/Revision," Korean Law Information Center, March 14, 2023, https://law.go.kr/LSW/lsRvsRsnListP.do?lsId=011357&chrClsCd=010202&lsRvsGubun=all/.

99 "개인정보 판매와 공유를 허용하는 개인정보보호법 반대한다!," Jinbonet, November 21, 2018, https://act.jinbo.net/wp/40024.

100 "개인정보 판매와 공유를 허용하는 개인정보보호법 반대한다!," Jinbonet.

101 "Scientific research" in English can be translated as "학술 연구" or "과학적 연구" in Korean. "Academic research" in this chapter, or "학술 연구," is research that takes place primarily within the academic community, often requires peer review, and whose results are shared with society and contribute to the expansion of society's knowledge base. "Scientific research" in this chapter, or "과학적 연구," may be used in a similar sense to "academic research," but it has strong nuances as research using scientific methods.

102 "Recital 159, Processing for Scientific Research Purposes," Intersoft Consulting, European Union, accessed February 14, 2024, https://gdpr-info.eu/recitals/no-159.

103 "A Preliminary Opinion on Data Protection and Scientific Research," European Data Protection Supervisor, January 6, 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

104 "Study on How to Improve the Personal Information Protection Legal System in Accordance With International Human Rights Standards Such as the European Union General Data Protection Regulation (GDPR)," Institute for Digital Rights, November 16, 2020, 71–72, https://idr.jinbo.net/673.

105 According to the GDPR, "profiling" refers to any form of automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." See "Art. 4 GDPR: Definitions," Intersoft Consulting, European Union, accessed February 20, 2024, https://gdpr-info.eu/art-4-gdpr.

106 "S Korea Nuclear Firm to Hold Cyber-Attack Drills After Hack," BBC, December 22, 2014, https://www.bbc.com/news/world-asia-30572575.

107 "Security" in English translates to "보안" or "안보" in Korean. If "안보" has a strong meaning of national security, "보안" is used in a neutral and technical context. For example, cybersecurity includes the security of individual computers and network systems, but the state can also be a factor that can threaten individual security. However, cybersecurity in terms of national security mainly emphasizes the threat of external attackers (especially North Korea in the Korean context). The National Cyber Security Strategy announced in 2019 used the term "보안." In other words, it focuses on cyber strategy in terms of national security. Cybersecurity naturally includes a national security context, but the national security aspect has been particularly emphasized in Korea, and this is one factor that distorts cybersecurity-related policies and social discourse in Korea.

108 Bong-jin Choi, "Can a National Security Agency That Tried to Turn Back the Clock Really Make a Difference?," OhmyNews, May 30, 2017, https://m.ohmynews.com/NWS_Web/Mobile/at_pg.aspx?CNTN_CD=A0002329933.

109 Kim Oi-hyun et. al, "NIS Hacking Targeted South Korean Nationals in China," *Hankyoreh*, July 22, 2015, https://english.hani.co.kr/arti/english_edition/e_national/701313.

110 Hee-seok Yoon, "[100대 사건_077] 대규모 개인정보 유출 사고 <2008년 2월>," ETNews, September 17, 2012, https://www.etnews.com/201209110625.

111 Personal Information Portal, South Korean Personal Information Protection Commission, https://www.privacy.go.kr.

112 Korea Communications Standards Commission, https://www.kocsc.or.kr.

113 Figures are from the KOCSC's 2022 Annual Report (in Korean). See "Annual Report 2022," Korea Communications Standards Commission, 2023, http://www.kocsc.or.kr/commons/pdfViewer/web/viewer.html?file=/upload/main/bbs/info_Casebook_main/BBS_20230627035311700 1#page=1&zoom=auto,-16,745.

114 "2022 Yearbook of Broadcasting and Communications Review," Korea Communications Standards Commission, 2023, http://www.kocsc.or.kr/commons/pdfViewer/web/viewer.html?file=/upload/main/bbs/info_Casebook_main/BBS_20230627035311700 1#page=1&zoom=auto,-16,745.

115 "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," UN General Assembly, April 6, 2018, Para 68, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F35&Language=E&DeviceType=Desktop&LangRequested=False.

116 North Korea Tech, https://www.northkoreatech.org.

117 KOCSC's blocking of North Korean ICT information media North Korea Tech was later found unlawful by the High Court. See "Court of Appeals Confirmed That the Blocking of 'North Korea Tech' Website Is Unlawful," Opennet, October 23, 2017, https://www.opennetkorea.org/en/wp/2208.

118 "Framework Act on Intelligent Informatization," Korea Law Translation Center, June 9, 2020, article 57(2) https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=54720&type=part&key=43.

119 Vitalization of Cryptography Technology, https://seed.kisa.or.kr.

120 "Framework Act on Electronic Documents and Electronic Transactions," Korea Law Translation Center, June 1, 2012, article 14(2), https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=27334&type=part&key=28.

121 "PIPC Imposes Sanctions Such as Fines and Penalties on Scatter Lab, Developer of 'Lee Luda,'" Personal Information Protection Commission, April 28, 2021, https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcUReVvzQtYI7AS40UKYXoOXo8.

122 Cheon Ho-seong, "Government Hands Over 170 Million Immigration Mugshots to AI Firm," *Hankyoreh*, October 21, 2021, https://www.hani.co.kr/arti/economy/it/1016022.html.

123 "Artificial Intelligence (AI) National Strategy Released," Ministry of Science and ICT, December 17, 2019, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156366736.

124 "MSIT Establishing the AI Ethics Standards,," Ministry of Science and ICT, December 23, 2020, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156428773.

125 "MSIT Establishing the AI Ethics Standards," Ministry of Science and ICT.

126 "Announcing a Strategy for Implementing Trusted AI," Ministry of Science and ICT, May 13, 2021, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156451595.

Chapter 4

127 Mahathir Bin Mohamad, "The Opening of Multimedia Asia on Multimedia Super Corridor," Mahathir: The Past and the Present, January 8, 1996, https://www.mahathir.com/malaysia/speeches/1996/1996-08-01.php.

128 Digital Penang, "Digital Transformation Masterplan 1.0 (2021-2023)", March 12, 2021, https://dp-www.storage.googleapis.com/wp-content/uploads/2022/03/08110121/DTMPBooklet.pdf; "About MySRBN," Sarawak Rural Broadband Network, accessed February 16, 2024, https://mysrbn.sarawak.digital/about-mysrbn/; and "Negeri Sembilan Digital Economy Blueprint 2027," Unit Perancang Ekonomi Negeri, April 2023, https://www.ns.gov.my/images/contents/Penerbitan/NSDigitalEconomyBlueprint_en.pdf.

129 "Measuring Digital Development – ICT Development Index 2023," International Telecommunication Union, 2023, https://www.itu.int/hub/publication/D-IND-ICT_MDD-2023-2/.

130 "Insight: Digital Connectivity," Malaysian Communications and Multimedia Commission, March 22, 2023, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/Insight-Digital-Connectivity.pdf.

131 "JENDELA Phase 1 Concluding Report," Malaysian Communications and Multimedia Commission, June 1, 2023, https://myjendela.my/Sitejendela/media/Doc/JENDELA-Phase-1-Concluding-Report.pdf.

132 "#Networked Nation: Navigating Challenges, Realising Opportunities of Digital Transformation," Khazanah Research Institute, June 2021, https://www.krinstitute.org/assets/contentMS/img/template/editor/KRI%20-%20NetworkedNation%20-%20Navigating%20Challenges,%20Realising%20Opportunities%20of%20Digital%20Malaysia.pdf.

133 "Penang 5G Coverage Stands at 73.4pc as of September 2023, Says State Exco," Malay Mail, November 23, 2023, https://www.malaymail.com/news/malaysia/2023/11/23/penang-5g-coverage-stands-at-734pc-as-of-september-2023-says-state-exco/103775.

134 Alexander Wong, "Starlink Now Available in Malaysia, Priced at RM220 Per Month for 100Mbps Satellite Broadband," Malay Mail, July 25, 2023, https://www.malaymail.com/news/malaysia/2023/07/25/starlink-now-available-in-malaysia-priced-at-rm220-per-month-for-100mbps-satellite-broadband/81603.

135 Khazanah Research Institute, "#Networked Nation: Navigating Challenges, Realising Opportunities of Digital Transformation," 31.

136 "4Q 2021 Communications and Multimedia Facts and Figures," Malaysian Communications and Multimedia Commission, April 8, 2022, https://www.mcmc.gov.my/skmmgovmy/media/General/C-M-Q4_220331_BI_PDF_1.pdf.

137 Malaysian Communications and Multimedia Commission, "JENDELA Phase 1 Concluding Report"; and Alexander Wong, "Ookla Crowns Time as Malaysia's Best Fibre Broadband Provider," Malay Mail, July 18, 2023, https://www.malaymail.com/news/malaysia/2023/07/18/ookla-crowns-time-as-malaysias-best-fibre-broadband-provider/80358.

138 Malaysian Communications and Multimedia Commission, "Commission Determination on the Mandatory Standard on Access Pricing: Determination No. 1 of 2023," March 1, 2023, https://www.mcmc.gov.my/skmmgovmy/media/General/registers/cma/Commission-Determination-on-the-Mandatory-Standard-on-Access-Pricing-16-February-2023.pdf.

139 Angelin Yeoh, "Starlink Offers 100Mbps Satellite Broadband for RM220 Monthly Without Contract," Star, July 25, 2023, https://www.thestar.com.my/tech/tech-news/2023/07/25/starlink-offers-100mbps-satellite-broadband-for-rm220-monthly-without-contract.

140 "World Map of Encryption Laws and Policies," Global Partners Digital, accessed February 16, 2024, https://www.gp-digital.org/world-map-of-encryption/.

141 Muhammad Rezal Bin Kamel Ariffin, Kriptografi Tempatan Dan Cabarannya," Universiti Putra Malaysia Institute for Mathematical Research, https://einspem.upm.edu.my/covid19maths/file/specific/CGSO%20v8.pdf; and "Cyber Security: Towards a Safe and Secure Cyber Environment," Academy of Sciences Malaysia, February 26, 2018, https://www.akademisains.gov.my/asmpub/?mdocs-file=124; and Teoh Pei Ying, "ADAM a Boost for Country's Cybersecurity," *New Straits Times*, December 20, 2022, https://www.nst.com.my/news/nation/2022/12/862681/adam-boost-countrys-cybersecurity; Zahratulhayat Mat Arif, "Muhyiddin: No Data Leakage From Us of Crypto AG Encryption Devices," *New Straits Times*, February 15, 2020, https://www.nst.com.my/news/nation/2020/02/565842/muhyiddin-no-data-leakage-use-crypto-ag-encryption-devices; MyDigital, "Malaysia Digital Economy Blueprint," February 18, 2021, https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf; and Elina Noor and Mark Bryan Manantan, "Raising Standards: Data and Artificial Intelligence in Southeast Asia," Asia Society Policy Institute, May 27, 2019, 34–35, https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf. .

142 Hazlin Abdul Rani, "Malaysian Validation Programs Overview," 2017, https://icmconference.org/wp-content/uploads/C24c-Hazlin-Rani.pdf.

143 Predeep Nambiar, "Penang Government Data Leaked Online," Free Malaysia Today, February 9, 2023, https://www.freemalaysiatoday.com/category/nation/2023/02/09/penang-government-data-leaked-online/.

144 Surin Murugiah, "Data of 22.5 Million Malaysians Allegedly Stolen from NRD Being Sold for Over US$10,000 Each," Edge Malaysia, May 18, 2022, https://theedgemalaysia.com/article/data-225-million-malaysians-allegedly-stolen-nrd-being-sold-over-us10000-each.

145 Suresh Ramasamy, "Exposed! Millions of Malaysian Personal Data Exposed by a Govt Site," LinkedIn, May 31, 2022, https://www.linkedin.com/pulse/exposed-millions-malaysian-personal-data-govt-site-ts-dr-suresh/; Ikmal Rozlan, "UiTM Leaks Personal Information of Almost 12,000 Foundation Applicants," Lowyat.net, May 10, 2023, https://www.lowyat.net/2023/299946/uitm-leaks-information-12000-foundation/; and Mazwin Nik Anis and Ragananthini Vethasalam, "Auditor-General's Report: MySejahtera Came Under Cyber Attacks," Star, February 17, 2023, https://www.thestar.com.my/news/nation/2023/02/17/auditor-generals-report-mysejahtera-came-under-cyber-attacks.

146 "Hamzah Concedes to Personal Data Leaks, but NRD Not to Blame," Malaysiakini, June 29, 2022, https://www.malaysiakini.com/news/626476; and Shahrin Aizat Noorshahrizam, "Deputy Minister: Three Million MySejahtera Users' Data Downloaded to Protect Them From Hackers," Malay Mail, February 27, 2023, https://www.malaymail.com/news/malaysia/2023/02/27/deputy-minister-three-million-mysejahtera-users-data-downloaded-to-protect-them-from-hackers/57002; and Justin Zack, "Hisham: Data Leak Won't Affect National Security," Star, May 20, 2022, https://www.thestar.com.my/news/nation/2022/05/20/hisham-data-leak-won039t-affect-national-security.

147 Rahimi Yunus, "Astro Hit by 2nd Data Breach in 14-Month Period," Malaysian Reserve, August 23, 2019, https://themalaysianreserve.com/2019/08/23/astro-hit-by-2nd-data-breach-in-14-month-period/.

148 Vijandren, "Personal Data of Millions of Malaysians Up for Sale, Source of Breach Still Unknown," Lowyat.net, October 19, 2017, https://www.lowyat.net/2017/145654/personal-data-millions-malaysians-sale-source-breach-still-unknown/.

149 Dissent, "AirAsia Victim of Ransomware Attack, Passenger and Employee Data Acquired," DataBreaches.net, November 19, 2022, https://www.databreaches.net/airasia-victim-of-ransomware-attack-passenger-and-employee-data-acquired/.

150 Vijandren, "46.2 Million Malaysian Mobile Phone Numbers Leaked From 2014 Data Breach," Lowyat.net, October 20, 2017, https://www.lowyat.net/2017/146339/46-2-million-mobile-phone-numbers-leaked-from-2014-data-breach/.

151 Foong Cheng Leong, "Bread and Kaya: 2018 Malaysia Cyber-Law and IT Cases – Fake News, Private Information and Instant Messaging," Digital News Asia, April 19, 2019, https://www.digitalnewsasia.com/insights/bread-kaya-2018-malaysia-cyber-law-and-it-cases-%E2%80%93-fake-news-private-information-instant.

152 "Profile and Performance of MSMEs in 2022," SME Corporation Malaysia, 2022, https://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/sme-statistics.

153 Vignesa Moorthy, "Cybersecurity Gap Threatens SMEs' Digitalisation," Malaysian Reserve, February 7, 2022, https://themalaysianreserve.com/2022/02/07/cybersecurity-gap-threatens-smes-digitalisation/.

154 Aiza Azreen Ahmad, "Building Trusted, Secure and Ethical Digital Environment for Malaysian SMEs," Edge Malaysia, July 16, 2021, https://theedgemalaysia.com/content/advertise/building-trusted-secure-and-ethical-digital-environment-for-malaysian-smes.

155 "MyDigital ID," MyDigital ID, accessed February 5, 2024, https://digital-id.my; and Soo Wern Jun, "Cabinet Green-Lights National Digital Identity," August 26, 2019, Malay Mail, https://www.malaymail.com/news/malaysia/2019/08/26/cabinet-green-lights-national-digital-identity/1784339.

156 "Public Consultation Paper No. 01/2020, Review of Personal Data Protection Act 2010 (Act 709)," Personal Data Protection Department of the Malaysian Communications and Multimedia Commission, February 14, 2020, https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf; Liew Jia Xian, "Govt to Introduce Digital ID System That Strengthens MyKad Security, Says Home Ministry," Star, October 20, 2021, https://www.thestar.com.my/news/nation/2021/10/20/government-to-introduce-digital-id-system-which-strengthens-mykad-security-says-home-ministry; and MyDigital, "Malaysia Digital Economy Blueprint," 53–55.

157 Chester Tay, "MyDigital Id to Be Made Available to Public by July 2024, Says Mimos," Edge Malaysia, December 06, 2023, https://theedgemalaysia.com/node/692914.

158 Sulok Tawie, "Sarawak Mulls Digital ID Platform," Malay Mail, May 19, 2023, https://www.malaymail.com/news/malaysia/2023/05/19/sarawak-mulls-digital-id-platform/70051.

159 "Content Code 2022," Malaysian Communications and Multimedia Commission, May 2022, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Content-Code-2022.pdf; and Freedom House, "Freedom on the Net 2022, Malaysia," 2022, https://freedomhouse.org/country/malaysia/freedom-net/2022.

160 Harris Zainul, "Tech Giants Should Be More Transparent About Content Moderation," Institute of Strategic and International Studies Malaysia, June 23, 2023, https://www.isis.org.my/2023/06/23/tech-giants-should-be-more-transparent-about-content-moderation/.

161 Laws of Malaysia, Anti-Fake News Act, Act 803, 2018, https://perma.cc/Y5H3-D6G8; and "Malaysia: Repeal 'Fake News' Emergency Ordinance," Article 19, March 15, 2021, https://www.article19.org/resources/malaysia-fake-news-ordinance/.

162 "Fact-Checking Journalism Evolves in Malaysia," Digital Watch, May 7, 2023, https://dig.watch/updates/fact-checking-journalism-evolves-in-malaysia.

163 Laws of Malaysia, Act 709, Personal Data Protection Act 2010, June 2010, https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf.

164 Christopher and Lee Ong, "Client Update: Malaysia," February, 2022, https://www.christopherleeong.com/media/4724/220211_client_update_on_the_pdpa.pdf.

165 "Open Data Policy," Government of Malaysia, accessed February 16, 2024, https://www.malaysia.gov.my/portal/content/30021; and "Malaysia's Official Open Data Portal," Government of Malaysia, updated February 3, 2024, https://data.gov.my/.

166 "Malaysia's National Statistics Organisation," Department of Statistics Malaysia, updated February 3, 2024, https://open.dosm.gov.my/.

167 MyDigital, "Malaysia Digital Economy Blueprint."

168 Mohd Nasaruddin Parzi, "Netizens Say They Faced Difficulties with OTP, Verification Processes on Padu Platform," *New Straits Times*, January 2, 2024, https://www.nst.com.my/news/nation/2024/01/996644/netizens-say-they-faced-difficulties-otp-verification-processes-padu; and Daniel Ahmad, "Suspend Padu Until Security Flaws Addressed: Former MITI Deputy Minister," *New Straits Times*, January 2, 2024, https://www.nst.com.my/news/nation/2024/01/996784/suspend-padu-until-security-flaws-addressed-former-miti-deputy-minister.

169 "IDEAS: Padu Is an Important Step in Closing Malaysia's Socio-Economic Gap but Uptake and Accessibility Are Key to Ensuring its Success," Institute for Democracy and Economic Affairs, January 4, 2024, https://www.ideas.org.my/ideas-padu-is-an-important-step-in-closing-malaysias-socio-economic-gap-but-uptake-and-accessibility-are-key-to-ensuring-its-success/.

170 Muhammad Zulhusni, "What's Going On With Cyber Security in Malaysia?," Techwire Asia, July 14, 2023, https://techwireasia.com/07/2023/whats-going-on-with-cyber-security-in-malaysia-in-2023-so-far/.

171 "Malaysia: 90 Days Under Malaysia Madani – Personal Data Protection Redux," Baker McKenzie, March 3, 2023, https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-90-days-under-malaysia-madani-personal-data-protection-redux.

172 "Gobind: Seven Guidelines to be Developed Under Personal Data Protection Act 2010," Malay Mail, January 16, 2024, https://www.malaymail.com/news/malaysia/2024/01/16/gobind-seven-guidelines-to-be-developed-under-personal-data-protection-act-2010/112720.

173 Laws of Malaysia, Copyright (Amendment) Act, Act A1645, 2022, 14, https://www.myipo.gov.my/wp-content/uploads/2022/03/Copyright-Amendment-Act-2022-Act-A1645.pdf.

174 "Two Individuals First to Be Charged Under Copyright Act for Selling Android Boxes," *Business Today*, April 6, 2023, https://www.businesstoday.com.my/2023/04/06/two-individuals-first-to-be-charged-under-copyright-act-for-selling-android-boxes/.

175 Ministry of Domestic Trade and Cost of Living Affairs, "Program Cyber Copyright Enforcement," January 6, 2022, https://www.kpdn.gov.my/en/media-kpdnhep/berita-kpdn/berita-terkini/2022-berita-terkini/1098-program-cyber-copyright-enforcement; and "Cyber Copyright Enforcement Programme Introduced to Combat Digital Piracy, Says Minister,"

Malay Mail, January 6, 2022, https://www.malaymail.com/news/malaysia/2022/01/06/cyber-copyright-enforcement-programme-introduced-to-combat-digital-piracy-s/2033423.

176 Jessie Tan, Liew Sue Yin, and Joel Prashant, "Artificial Intelligence – Malaysian Legislative Framework and Key Legal Challenges," Lexology, May 12, 2023, https://www.lexology.com/library/detail.aspx?g=d9211d03-f7fe-4e5e-a0f4-b73101b6d93c.

177 Noor Hadzlida Ayob, Mohd Amar Aziz, and Nor Azira Ayob, "Bridging the Digital Divide: innovation Policy and Implementation in Malaysia," International Journal of Academic Research in Business and Social Sciences, July 30, 2022, https://hrmars.com/papers_submitted/14554/bridging-the-digital-divide-innovation-policy-and-implementation-in-malaysia.pdf; Rachel Gong, "Digital Inclusion: Assessing Meaningful Internet Connectivity in Malaysia," Khazanah Research Institute, September 7, 2020, https://krinstitute.org/assets/contentMS/img/template/editor/20200907%20Inclusion%20v4.0.pdf; Noor and Manantan, "Raising Standards: Data and Artificial Intelligence in Southeast Asia," 34–35.

Chapter 5

178 Kenji E. Kushida, "Leading Without Followers: How Politics and Market Dynamics Trapped Innovations in Japan's Domestic 'Galapagos' Telecommunications Sector," *Journal of Industry, Competition, and Trade* (March 25, 2011): https://papers.ssrn.com/abstract=1861208.

179 Kushida, "Leading Without Followers."

180 Kushida, "Leading Without Followers."

181 "The Third Generation of Wireless Mobile Telecommunications Technology (3G)," International Telecommunication Union, accessed February 15, 2024, https://kimon.hosting.nyu.edu/physical-electrical-digital/items/show/1144#:~:text=The%20first%203G%20network%20was,by%20the%20International%20Telecommunication%20Union.

182 Kushida, "Leading Without Followers."

183 "ISDB-T Adopting Countries," Digital Broadcasting Experts Group, accessed February 14, 2024, https://www.dibeg.org/world.

184 "政府共通のクラウド基盤、国産サービスの応札は「なかった」　河野大臣がコメント[Minister Kono Comments There Were No Domestic Service Providers Bids for the Government Cloud]," ITmedia, October 5, 2022, https://www.itmedia.co.jp/news/articles/2210/05/news084.html.

185 Kenji E. Kushida, "Information and Communications Technology (ICT) Policy in a Post-LDP Japan: Caught Between Distributive Politics and Strategic Policy Again?," *Journal of Industry, Competition, and Trade* (March 25, 2011): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4716528; and Ministry of Internal Affairs and Communications, "Communications White Paper 2012," accessed February 20, 2024, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc113120.html.

186 Kenji E. Kushida and Seung-Youn Oh, "The Political Economies of Broadband Development in Korea and Japan," *Asian Survey* 47, no. 3 (June 1, 2007): 481–504, https://doi.org/10.1525/as.2007.47.3.481; and Kenji E. Kushida, "Entrepreneurship in Japan's ICT Sector: Opportunities and Protection from Japan's Telecommunications Regulatory Regime Shift," *Social Science Japan Journal* 15, no. 1 (January 1, 2012): 3–30, https://doi.org/10.1093/ssjj/jyr037.

187 Kushida, "Entrepreneurship in Japan's ICT Sector."

188 Kenji E. Kushida, "Public Private Interplay for Next Generation Access Networks: Lessons and Warnings from Japan's Broadband Success," *Digiworld Economic Journal* 91, no. 3 (October 3, 2013): 13–34, https://repec.idate.org/RePEc/idt/journl/CS9101/CS91_KUSHIDA.pdf; and Kenji E. Kushida, "Startup Japan: Series Overview," Carnegie Endowment for International Peace, August 9, 2022, https://carnegieendowment.org/2022/08/09/startup-japan-series-overview-pub-87648.

189 "Cyberattacks Increasing in Japan Ahead of G7 Summit," *Japan Times*, April 30, 2023, https://www.japantimes.co.jp/news/2023/04/30/national/crime-legal/cyberattacks-japan-g7/.

190 Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say," *Washington Post*, August 7, 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon.

191 "Japan's SDF Launches New Cyber-Defense Unit," *Kyodo News*, March 17, 2022, https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html; and Mao Kawano, "Japan to Quadruple Cyber Defense Forces, Meeting Threats Head-On," *Nikkei Asia*, January 5, 2023, https://asia.nikkei.com/Politics/Japan-to-quadruple-cyber-defense-forces-meeting-threats-head-on.

192 "Japan's Defense Ministry to Set Up Cyber Department at Its Academy," *Nikkei Asia*, January 10, 2023, https://asia.nikkei.com/Politics/Japan-s-Defense-Ministry-to-set-up-cyber-department-at-its-academy.

193 Kyle Sheahan, "United States and Japan Pledge Closer Cooperation in Cyber Defense Matters," JD Supra, June 12, 2015, https://www.jdsupra.com/legalnews/united-states-and-japan-pledge-closer-88013.

194 "Japan Policy Brief: Economy," Organisation for Economic Co-operation and Development, April 2017, https://www.oecd.org/japan/japan-economy-improving-the-performance-of-japan-sme-sector.pdf.

195 Lucy Craft, "Japan Is Struggling to Quit Floppy Disks and Fax Machines," CBS News, September 13, 2022, https://www.cbsnews.com/news/japan-struggling-to-quit-floppy-disks-and-fax-machines.

196 Trend Micro, "サイバーセキュリティリスク 意識調査レポート（日本）," [Cybersecurity Awareness Report (Japan)] Trend Micro, 2021, https://resources.trendmicro.com/rs/945-CXD-062/images/m471_%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%83%AA%E3%82%B9%E3%82%AF_%E6%84%8F%E8%AD%98%E8%AA%BF%E6%9F%BB%E3%83%AC%E3%83%9D%E3%83%BC%E3%83%88%EF%BC%88%E6%97%A5%E6%9C%AC%EF%BC%89.pdf.
Trend Micro, "サイバーリスク国際意識調査「Cyber Risk Index」~2022年上半期の結果から見える日本の課題は？~ [Cyber Risk International Awareness Survey 'Cyber Risk Index' - What Are Japan's Challenges Seen From the Results of the First Half of 2022?]," Trend Micro, 2023, https://www.trendmicro.com/ja_jp/jp-security/23/b/securitytrend-20230213-02.html.

197 "Japan PM Calls for Review of All 'My Number' Card Data by End of Nov," *Kyodo News*, August 8, 2023, https://english.kyodonews.net/news/2023/08/c71f87aebf48-japan-pm-calls-for-review-of-all-my-number-card-data-by-end-of-nov.html.

198 Kyodo News, "Japan PM Calls for Review of All 'My Number' Card Data by End of Nov."

199 Mayumi Hirosawa, "Japan to Require Big Tech to Respond to Online Defamation," *Nikkei Asia*, January 9, 2024, https://asia.nikkei.com/Business/Technology/Japan-to-require-Big-Tech-to-respond-to-online-defamation.

200 Hiroyuki Tanaka et al., "Data Localization Laws: Japan," Thomson Reuters, June 26, 2023, https://www.mhmjapan.com/content/files/00065279/Data%20Localization%20Laws%20Japan.pdf.

201 "日本政府の共通クラウド基盤に「Azure」「Oracle Cloud」追加　またも国産サービス入らず['Azure' and 'Oracle Cloud' Added to Japanese Government›s Common Cloud Infrastructure - Domestic Services Left Out Yet Again]," ITmedia, October 3, 2022, https://www.itmedia.co.jp/news/articles/2210/03/news069.html.

202 The Nikkei notes that AWS had over 90 percent of local government cloud installations. "AWS寡占に運用コスト増　ガバメントクラウド巡る不満 [Dissatisfaction Surrounds Government Cloud Amid Rising Operational Costs Due to AWS Oligopoly]," Nikkei, January 17, 2024, https://www.nikkei.com/article/DGXZQOUC267V10W3A221C2000000/.

Chapter 6

203 John F. Kennedy, "Remarks on Signing Communications Satellite Act, 31 August, 1962," John F. Kennedy Presidential Library and Museum, August 31, 1962, https://www.jfklibrary.org/asset-viewer/archives/jfkpof-039-051#?image_identifier=JFKPOF-039-051-p0003.

204 "The History of Computer Communications, Chapter 7 - Data Communications: Market Order 1973-1979," Computer History Museum, accessed February 12, 2024, https://historyofcomputercommunications.info/section/7.2/The-Justice-Department-IBM-and-AT&T/.

205 Jonathan Weber, "News Analysis: Clinton Plan Plays Well to Silicon Valley Crowd: Technology: The President Appears to Have Won Over Much of the Industry's Conservative Leadership," *Los Angeles Times*, February 23, 1993, https://www.latimes.com/archives/la-xpm-1993-02-23-fi-414-story.html.

206 Kajal Singh and Zach Sorenson, "Throwback Thursday: A Look Back at the White House Website 20 Years Ago," White House (President Barack Obama), October 23, 2014, https://obamawhitehouse.archives.gov/blog/2014/10/23/throwback-thursday-look-back-white-house-website-20-years-ago#:~:text=The%20first%20White%20House%20website,President%20and%20the%20Executive%20Branch.

207 "A Short Summary of the Telecommunications Reform Act of 1996," White House (President Bill Clinton), 1996, https://clintonwhitehouse4.archives.gov/WH/EOP/OP/telecom/summary.html.

208 "The National Information Infrastructure: Agenda for Action," Executive Office of the President, Informatio n Infrastructure Task Force, accessed February 12, 2024, https://ibiblio.org/nii/NII-Task-Force.html.

209 "Network Executives Clinton, Gore Help School Venture Into Cyberspace," *Spokesman Review*, March 10, 1996, https://www.spokesman.com/stories/1996/mar/10/network-executives-clinton-gore-help-school.

210 "Measuring the Digital Economy: An Update Incorporating Data From the 2018 Comprehensive Update of the Industry Economic Accounts, Bureau of Economic Analysis, 2018, https://www.bea.gov/system/files/2019-04/digital-economy-report-update-april-2019_1.pdf.

211 "How Big Is the Digital Economy?," Bureau of Economic Analysis, 2023, https://www.bea.gov/sites/default/files/2023-12/digital-economy-infographic-2022.pdf.

212 White House, *Building a Better America: A Guidebook to the Bipartisan Infrastructure Law for State, Local, Tribal, and Territorial Governments, and Other Partners*, White House, May 2022, https://www.whitehouse.gov/wp-content/uploads/2022/05/BUILDING-A-BETTER-AMERICA-V2.pdf#page=385.

213 Brian Fung, "Here's How Much Each State Will Get in the $42.5 Billion Broadband Infrastructure Plan," CNN, June 26, 2023, https://www.cnn.com/2023/06/26/tech/broadband-infrastructure-biden/index.html.

214 John B. Horrigan, "Are We There Yet?," Benton Institute for Broadband and Society, December 20, 2023, https://www.benton.org/publications/are-we-there-yet.

215 Mike Conlow, "An Update on the State of Broadband Competition in the U.S.," Benton Foundation, December 8, 2022, https://www.benton.org/headlines/update-state-broadband-competition-us.

216 "Broadband Competition Is Thriving Across America," Benton Foundation, June 23, 2022, http://www.benton.org/headlines/broadband-competition-thriving-across-america.

217 "Guideline for Using Cryptographic Standards in the Federal Government—Cryptographic Mechanisms: NIST Releases Draft NIST SP 800-175B Rev. 1," National Institute of Standards and Technology, July 3, 2019, https://www.nist.gov/news-events/news/2019/07/guideline-using-cryptographic-standards-federal-government-cryptographic.

218 Bruce Schneier, "Attorney General William Barr on Encryption Policy," Lawfare, July 23, 2019, https://www.lawfaremedia.org/article/attorney-general-william-barr-encryption-policy.

219 Patrick Radden Keefe, "The Surreal Case of a CIA Hacker's Revenge," *New Yorker*, June 6, 2022, https://www.newyorker.com/magazine/2022/06/13/the-surreal-case-of-a-cia-hackers-revenge; and "Biden Says Huge Data Breach Poses 'Grave Risk' to U.S., Promises Response," Reuters, December 22, 2020, https://www.reuters.com/article/idUSKBN28W2G7.

220 Makena Kelly, "Joe Biden Doesn't Like Trump's Twitter Order, But Still Wants to Revoke Section 230," Verge, May 22, 2020, https://www.theverge.com/2020/5/29/21274812/joe-biden-donald-trump-twitter-facebook-section-230-moderation-revoke.

221 David Lawder, "US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation," Reuters, October 25, 2023, https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25.

222 John G. Murphy, "How USTR Reversal of Digital Trade Could Threaten Workers, Companies," U.S. Chamber of Commerce, 2023, https://www.uschamber.com/international/trade-agreements/how-reversal-on-digital-trade-threatens-u-s-workers-businesses.

223 Nigel Cory and Samm Sacks, "China Gains as U.S. Abandons Digital Policy Negotiations," Lawfare, November 15, 2023, https://www.lawfaremedia.org/article/china-gains-as-u.s.-abandons-digital-policy-negotiations.

224 Rahul Matthan and Shreya Ramann, "India's Approach to Data Governance," in *Data Governance, Asian Alternatives: How India and Korea Are Creating New Models and Policies*, eds. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 21, 2022, https://carnegieendowment.org/2022/08/31/india-s-approach-to-data-governance-pub-87767.

225 Janét Aizenstros, "The Impact of the Biden Presidency on Consumer Data Privacy," *Forbes*, February 24, 2021, http://www.forbes.com/sites/forbesagencycouncil/2021/02/24/the-impact-of-the-biden-presidency-on-consumer-data-privacy/?sh=135ba0df53cf.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Asia Program

The Asia Program in Washington studies disruptive security, governance, and technological risks that threaten peace, growth, and opportunity in the Asia-Pacific region, including a focus on China, Japan, and the Korean peninsula.

Technology and International Affairs Program

The Technology and International Affairs Program develops insights to address the governance challenges and large-scale risks of new technologies. Our experts identify actionable best practices and incentives for industry and government leaders on artificial intelligence, cyber threats, cloud security, countering influence operations, reducing the risk of biotechnologies, and ensuring global digital inclusion.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org