Global Governance Futures

ROBERT BOSCH FOUNDATION
MULTILATERAL DIALOGUES

JUNE 2017

Data Power Dynamics: Who Runs the World in 2027?

CATHLEEN BERGER
YOLANDA JINXIN MA
VINCENT NI
ELIZABETH PRESCOTT
REIRUI RI
SHIREEN SANTOSHAM
RAHUL SHARMA
SATYARUPA SHEKHAR SWAIN
EVAN SILLS
SHOKO YOSHIHARA

Supported by

Robert Bosch Stiftung

GGF Partners

GPPi Global Public Policy Institute
Hertie School of Governance
The Tokyo Foundation
Keio University
Centre for Policy Research
ashoka University
Brookings
Woodrow Wilson School of Public & International Affairs, Princeton University

Table of Contents

About the Program

The Global Governance Futures program (GGF) brings together young professionals to look ahead 10 years and recommend ways to address global challenges. Building on a decade of successful rounds of the GGF program, GGF 2027 convened 25 fellows from Germany, China, Japan, India, and the United States (five from each country). Over the course of 2016 and 2017, the fellows participated in four dialogue sessions: in Washington, DC (May 8–12, 2016), Tokyo and Beijing (September 18–24, 2016), New Delhi (January 15–19, 2017), and Berlin (June 11–15, 2017).

The GGF 2027 fellows – selected from a highly competitive field of applicants from the public, private, and non-profit sectors – were assigned to one of three working groups that focused on data governance, global health and pandemics, and transnational terrorism. Utilizing instruments from the field of futures research, the working groups produced scenarios for their respective areas of focus. In addition to learning about and then implementing the scenario planning methodology, our fellows met with leading policymakers and experts from each participating country, whose insights helped shape the scenarios. Based on their findings, the fellows produced a range of publications – including this report – that present the process of creating histories of possible futures.[1]

The GGF team based at the Global Public Policy Institute (GPPi) works closely with the fellows to help them achieve their goals, and in the process, cultivates a community that will extend beyond the duration of the program, thanks to a growing and active alumni network.

1 The findings, interpretations, and conclusions expressed in this report are those of the authors and do not represent the views of the organizations they work for.

GGF is made possible by a broad array of dedicated supporters. The program was initiated by GPPi, along with the Robert Bosch Stiftung. The program consortium is composed of academic institutions, foundations, and think tanks from across the five participating countries. The GGF partners are GPPi, the Hertie School of Governance, the Brookings Institution, the Woodrow Wilson School of Public and International Affairs, the Tokyo Foundation, Keio University Tsinghua University, Fudan University, Ashoka University, and the Centre for Policy Research.

The core responsibility for the design and implementation of the program lies with the GGF program team at GPPi. In addition, GGF relies on the advice and guidance of the GGF steering committee, made up of senior policymakers and academics. The program is generously supported by the Robert Bosch Stiftung.

The fellows of the data governance working group would like to thank the organizers of GGF 2027, the Robert Bosch Stiftung, and everyone else who contributed to making the program possible – especially Thorsten Benner, Johannes Gabriel, Mirko Hohmann, Eka Rostomashvili, and Joel Sandhu. We are also grateful to TAU for its design work, Oliver Read and Maddie Wells for editing, and colleagues at GPPi and the GGF Alumni Seth Oppenheim and Jonah Force Hill for commenting on this report.

Executive Summary

In post-industrial societies, data, as well as data-driven technologies, are seeping into many aspects of life – involving a complex group of individuals, organizations, and governments who manage and own the technologies that create, use, alter, and destroy this data. Recognizing the growing centrality of these actors, this report considers how relationships between these diverse groups will change in the next 10 years. To explain some of these possibilities, we created three scenarios that portray not only what the digital world would look like in 2027, but also how those developments occurred. Following the scenarios, the report analyzes trends and insights gained from exploring these possible futures. Finally, we present the steps taken to build these scenarios.

We use the term data governance to encompass the relationships between the various and overlapping stakeholder groups that create, use, or own data. Beyond these initial actors, third parties also use data to discern entirely new things that were never intended by the original creator of the data.

The first scenario, "Towards 'De-Digitization,'" imagines a world where both a distrust in technology and difficulties in securing data takes hold in some parts of the world, leading individuals and communities to consider disconnecting from key systems, such as digital payment and banking systems, which cannot be secured from malicious actors. The second scenario, "Rise of the Digital Nation," considers how rapid technological growth combined with nearly universal and affordable access to the internet could outpace citizens' ability to understand the ramifications of the data they create, allowing exploitation by those who provide internet access. Finally, the third scenario, "Data Harmonization," envisions a world that becomes more interoperable, with technology and innovation driving world politics and changing the global governance landscape.

In creating these scenarios, a few key relationships and drivers emerge. Regardless of the rate of change and particular technologies that become entrenched, an important consideration is that the pace of technological literacy will impact who harnesses and benefits most from new technologies. Understanding the risks and the users of technologies was core to determining whether a technological development could have a positive or negative outcome, both for the present moment and in 2027. Additionally, the importance of trust in the integrity of data, as well as the transparency of data usage, emerged as pivotal factors in multiple scenarios. While cybersecurity is already an important topic, it is hard to overstate the importance of protecting networks and data as we become increasingly dependent on data that are vulnerable to corruption.

Introduction

Data governance is an evolving term. While it borrows from the processes and discussions established in and around internet governance, it brings data and its impact on individuals, societies, governments, and other stakeholders to the fore of the discussion. It draws particular attention to the social and political dimensions of data, and goes beyond the physical infrastructure associated with the internet.

This connotation of data governance led the group to explore how the "data ecosystem" impacts power dynamics between relevant stakeholders,[2] and what these would look like in 2027.

In constructing these scenarios, there was an overarching tension between progress and security. On the one hand, digitization and technological developments touch upon almost every aspect of human life, making many activities easier, faster, smarter, and more connected; these benefits can also be democratized to be enjoyed by the wider population. On the other hand, the everyday appeal and ubiquity of these benefits diminish individuals' ability to control their own data, leaving them subject to exploitation by others.

Today, data is already seen as one of society's most valuable resources. In this digital age, where governments and private entities alike gather, store, analyze, alter, sell, and use data, particularly sensitive personal information, regulatory regimes – where they exist at all – are fragmented and too slow to adapt to a rapidly evolving role in society. For most people, participating in digital life brings with it confusion or unawareness about how to control their information. A lack of both accountability tools for companies and credible government enforcement power leaves individuals vulnerable to exploitation – unable to keep pace with the changes brought on by technology, or powerless to protect themselves because they lack resources or a political voice.

The ambiguity of such developments stems from technology itself being neutral – it is per se neither a good nor a bad thing. Technology holds the promise of stronger accountability, more inclusive and participatory decision-making processes, and citizen mobilization. However, in the absence of legal and societal mechanisms to balance progress with individuals' security, large amounts of data could fall into the hands of a select few.

By exploring how power dynamics are affected by the evolving data ecosystem, the Global Governance Futures Fellows – split between those wary of and those enthusiastic about technology – explored the potential benefits of digitization, and how to prevent exploitation through data governance.

Each scenario addresses the question of empowerment. The first scenario outlines a future in which more and more people move towards de-digitization, either because they have been disillusioned by unfulfilled promises, or in an attempt to regain control over their private data. The second scenario imagines a future that provides universal access, which enables people to progress towards forms of digital citizenship and cross-border mobility. Lastly, the third scenario focuses on regulatory regimes, outlining a future where major breakthroughs in international agreements help shape citizens' consciousness through data harmonization. Each scenario highlights the complexities of the digital age and presents ways in which power dynamics are influenced by technological developments and social and geopolitical tensions.

2 Stakeholders include individuals, civil society, governments, companies, and other actors.

Scenario 1: Towards "De-Digitization"

Picture of the Future: 2027

The digital world has changed fundamentally in the past decade. Digital technologies are interwoven into human life through personal devices, self-driving cars, robotics, connected appliances, and smart interfaces.[3] At the same time, varied individual and societal experiences with the data revolution, ranging from changes in financial systems to elections, have in some cases created frustration over the disparity between the promised benefits of technological "improvements" and the inability to protect privacy, maintain connectivity, and secure data. Some groups are considering potential alternatives to technological dependency. In 2026, "De-digitization" was named the word of the year by the Oxford English Dictionary, which defined it as "the undoing of connectivity to limit potential harms."

De-digitization has manifested itself differently around the globe. In Africa, citizens are returning to paper money and less internet interaction following the breach of the financial transaction system M-Pesa, which crippled financial systems and resulted in monetary theft from many individuals and companies. In addition, some African citizens' internet access has been limited after several African countries began paying the Chinese government to restrict citizens' internet access, in effect creating a local version of technology similar to China's Great Firewall, which stymied innovation and personal freedoms. In the United States and Europe, repeated breaches coupled with rising inequality have produced, on the one hand, an elite class that can pay for sophisticated technologies that protect individual data ownership, and on the other, a larger community that sees no option to protect themselves other than to cut digital technology out of their lives completely. The major Asian powers have not been targeted as much as other parts of the world, thus avoiding significant data breaches and encouraging unabated and widespread digitalization.

In what some have called collusion with local and national governments, globally focused technology corporations have adapted their business models. Eager to give the appearance of providing free services to citizens, national governments are allowing companies to retain complete control of the data, deepening societal dependency on specific platforms provided for free. The resulting market concentration and centralization of access to data

3 Chris Dixon, "Eleven Reasons To Be Excited About The Future of Technology," *Medium*, August 18, 2016, accessed May 5, 2017, https://medium.com/@cdixon/eleven-reasons-to-be-excited-about-the-future-of-technology-ef5f9b939cb2#.s8pd7z1qe.

and information resources enable multinational corporations to influence enforcement regimes.

Moreover, the benefits of technologies such as artificial intelligence, e-voting, financial transactions, and public services have failed to deliver the quality-of-life improvements promised by their advocates. In Africa, this lack of improvement has been due to limited information; in Europe and the US, breaches of trust have caused some to lose faith in the digital world. People are questioning the overall value of ever-present data-driven technology and their dependence on it.

As a result of this skepticism, de-digitization is taking shape in several fundamental ways. First, while the implementation of IPv6 has continued, IPv4 was maintained for the specific purpose of identifying devices that require greater protection due to their use of sensitive data. Together, IPv4 and IPv6 make up the Internet Protocol layer, which allows data packets to travel across the internet. Devices that use less sensitive data, but do not primarily use sensitive data or regulate important systems, have been segmented to IPv6.

Second, at the individual level, those who can afford to can purchase a "wearable cloud" that allows them to maintain the benefits of technology without relinquishing control of their data to corporations or platforms.

Third, authoritarian regimes' use of repression, politically targeted breaches, and the denial of access to foreign press and civil society-building tools have turned popular perception against the internet, which is now seen as a tool of government oppression and a liability for the average citizen. Popular movements are forming around efforts to regain control of individuals' data by limiting access to different data sets, initiating regulations on the amounts of data that can be collected, stored, and analyzed in the first place (data minimization), and restructuring work and labor processes to include a human element in automated processes.

In sum, digitization and internet access in 2027 continue to play an important role in many aspects of life, including communication, leisure, and transportation, particularly in the developed world. But a growing awareness of control and dependency – as well as the fragility of infrastructure and security of personal data – are emboldening a pushback. Continued lack of trust in traditional sources of information and the inability to protect digital assets have led many to reconsider technology's role in their lives and their relationship with data owners and users.

History of the Future

In 2017, a focus on domestic issues, particularly focused on restricting trade and migration in many countries, has weakened international cooperation. In the EU, countries developed a biometric refugee database as an alternative to closing borders altogether; this appeared to lower social tension in the short term but at an unexpected long-term cost. Trade protectionism helped to reinforce the divide between the haves and have-nots, with provision of personal data required to gain access to basic government services and technologies. This exacerbated existing inequalities and left those at the bottom with few options but to give over control of their personal data to gain access to technology they would not otherwise be able to afford.

In the wake of a round of elections during which populist parties entered the political scene, parliaments around the world passed new surveillance laws with additional requirements for data localization, first in the United Kingdom, then followed by EU member states and reactionary governments around the world. This regulatory inhibition prompted corporations to begin looking to new, less developed markets in Africa and South Ameri-

ca, where they could have first-mover advantages and influence regulations.

Following political upheaval in Brazil dating back to 2016, the much-praised "Marco Civil da Internet," a bill of digital rights, was abolished. This triggered fissures in South American cooperation, ultimately fracturing the promise of harmonized regulatory regimes across the Organization of American States (OAS). In 2018, Argentina, Chile, and Venezuela – vying for regional leadership as the best country for multinationals to reside in South America – began offering technology companies preferential treatment to move to their countries, as well as centralized data collection on their citizens. Leaders were able to sell this politically to their citizens through two main narratives: preventing cyber-crime and terrorism, and economic growth through greater internet access. This limited the voice of civil society, who maintained that data collection was an unnecessary invasion of privacy.

In response to real and perceived national security concerns, in 2018 the European Union passed a new directive to centralize personal data in Brussels. Withstanding allegations of racial and religious bias by collecting data on everyone equally, EU authorities began monitoring recent refugees and immigrants from "countries of concern." In mid-2019, it is discovered that the biometric data of millions of recent immigrants and visa applicants to Europe was sold online the year before. This sale, and the spate of identity fraud that followed, left most with the impression that centralizing biometric authentication did not improve security.

Seeing an opportunity to reach vulnerable populations and stoke newfound sensitivity to privacy violations, internet advocacy groups and civil society attempted to intervene by stepping up their global engagement efforts. For instance, the Web Foundation initiated a pan-African campaign in 2019 to improve understandings of privacy by leveraging the digital literacy funds provided by the World Bank. Privacy International and European Digital Rights (EDRi) campaigns highlighted the abuses and vulnerabilities of centralized databases and pushed for data minimization.

Simultaneously, Alibaba became a key actor in bankrolling corporate-led global efforts to expand internet access to previously underserved parts of the world. Those efforts resulted in the acceleration of digital public services and opened new markets for data harvesting and the sale of citizens' data. In 2020, several African governments, including Zimbabwe, Nigeria, Uganda, Gabon, and Sudan, responded to limit these new public services by entering into agreements with China for guidance in constructing a Great Firewall in Africa, which they hoped would control access to content (and opposition voices) on the internet. The building of the firewall prompted discontent from citizens who felt they were no longer able to access services such as online education or remote medical care. Meanwhile, people in other parts of the world continued to focus on improving internet security.

Progress towards greater cybersecurity received a boost when in 2021 the MIT Civic Data Design Lab used quantum computing to develop a better encryption method that was both cost-effective and user-friendly, paving the way for mainstream adoption. This technical breakthrough allowed for the improvement of a range of technologies, including artificial intelligence, unmanned aerial systems, and medical care. In addition, it significantly strengthened citizens' trust in the security provided by encryption, anonymization, and authentication features. These changes led to the adoption of e-voting systems around the world, starting in 2022 in Italy, Canada, and Scandinavia. Progress was felt in the private sector too, where widespread access, combined with trust in new encryption technology for low-cost smartphones, allowed for the adoption of M-Pesa across the entire African Union and rapidly scaled Apple Pay to parts of the world that had previously resisted mobile payment systems.

However, much of this progress was undone by a massive internet disruption in 2023. The root server system, which underlies and enables the basic internet structure, unexpectedly failed during an encryption key exchange to it – the first exchange since the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN) multi-stakeholder oversight body. Vast

segments of the internet were inaccessible for months during the maintenance period, and most people lacked the technological knowledge to understand what happened and why. As frustration mounted, populist politicians attempted to direct the blame toward corporations, insisting that they had not developed sufficiently resilient systems as they pushed most of their services to cloud infrastructure. Some political parties adopted slogans that directly targeted digitization, urging their constituents to unplug and keep analog backups for essential services.

Later in 2023, a series of major financial breaches occurred in the United States and Hong Kong. The widely adopted Apple Pay system was breached, subjecting millions of people to financial loss and fraud. M-Pesa also became a target of a data breach, resulting in the loss of millions of dollars from Africans.

In response to this series of crises, ICANN developed a working group to improve the resilience of the internet. Late in 2024, the working group recommended segregating types of data – IPv4 for sensitive data and IPv6 for data deemed less sensitive – with the goal of increasing overall security. Duplicating IPv infrastructure around the world to maintain both IPv4 and IPv6 required massive infrastructural investment; however, this was seen as necessary for restoring trust in the internet in order to continue to grow markets while offsetting investments into other data-driven technologies.

In early 2025, the Sony Corporation, in partnership with the Linux Foundation, debuted a new device called the "wearable cloud," allowing a person to control their personal data and seamlessly integrate with any technology they encountered. The device allows for storage of all personal data by the individual, only sharing with technologies that need it on a just-in-time basis. By decentralizing data collection, individuals were enabled to wrestle control of personal data back from corporations and governments, limiting its susceptibility to theft. However, only a very small group of wealthy individuals were able to afford the device, which was priced at $50,000.

While international norms have largely protected attacks against critical infrastructure, the digital information generated by citizens and entrusted to companies and governments remained vulnerable to exploitation, leaving those unable to afford the wearable cloud prepared to take drastic measures. "Defending Analog" – a movement in the western United States that banned all digital technologies – began to gain momentum in 2026 as people became more desperate for a solution they could afford.

Now, in 2027, corporations have cemented their dominance in the regulatory sphere by embedding basic services such as finance into their platforms, frustrating those in the United States and Europe dependent on technology that often proved unreliable and untrustworthy. In Africa, disillusionment with technology companies is growing as citizens are unable to harness the benefits of an open internet as a result of government censorship. In contrast, in large parts of Asia, including Japan, India, and China, the lack of negative experiences has left the digital world unhindered and enmeshed in many aspects of life. Elsewhere, only a small group of elites are able to afford the wearable cloud devices that enable security of personal data. For others, a decade of privacy breaches, billions lost in internet outages, and challenges to even the most basic functions of democracy, like elections, are causing some to consider the wholsesale rejection of digitization as the only way to avoid financial and social losses.

Timeline

2017

› EU countries develop a biometric refugee database as an alternative to closing borders.
› Populist parties enter the political scene; new surveillance laws and data localization are introduced.
› In Brazil, the "Marco Civil da Internet" bill is abolished.

2018

› Argentina, Chile, and Venezuela offer technology companies preferential treatment to move to their countries.
› The EU passes a new directive to centralize personal data in Brussels.

› EU refugee biometric database is hacked and data sold online.
› A pan-African campaign is initiated to improve understanding of privacy.
› Alibaba starts corporate-led global efforts to expand internet access.

2019

2020

› Several African governments enter into agreements with China to provide expertise to construct a Great Firewall in Africa.

› MIT Civic Lab creates better encryption through quantum computing.

2021

2022

› Adoption of e-voting systems, starting with Italy, Canada, and Scandinavia.

› Massive disruption of the internet occurs.
› Widely-adopted Apple Pay and M-Pesa become targets of data breach.

2023

2024

› IPv4/IPv6 separated to segregate IoT data and personal data.

› The "wearable cloud" gives control over personal data, but is very expensive.

2025

2026

› A movement in the US that banned all digital technologies begins to gain momentum as people become more desperate for an affordable solution.

2027

Scenario 2: Rise of the Digital Nation

Picture of the Future

Global data governance in 2027 has been shaped by a decade of continuous, rapid technological progress at a pace that exceeded projections made in 2017. The rise of computers able to mimic human intelligence – broadly defined as artificial intelligence (AI) – combined with advances in fields such as robotics, advanced manufacturing, quantum computing, and synthetic biology, have created a new frontier for entrepreneurs, and challenged regulators to keep pace.

Throughout the decade, social, political, and economic tensions ran high as the convergence of technological disruption and nearly universal, affordable internet access became a reality. Technological breakthroughs in wireless technologies such as satellite-based and balloon-based internet improved access in remote and underrepresented parts of the globe, bringing billions more online. Despite rapid adoption of new technologies, technical literacy and awareness declined, leading many to use products without understanding their full ramifications.

From governments to companies, civil society, and citizens – various actors remain wary of technology. Universal internet access has not been the great leveler of inequality it was hoped to be in 2017, but most individuals now enjoy access to a wide range of services and data-driven consumer products. While embracing the benefits of digitized life, many individuals have become disillusioned with the path society is taking; they struggle to find fulfillment from increasingly polarized communities where people predominantly spend their time in the digital world.

Those familiar with emerging technology policy were unsurprised by the slow formation of regulations, norms, and interoperable standards to govern these new technologies, but few envisaged the geopolitical disruption that would unfold. As a growing portion of the world's wealthiest embraced data-driven technology in all parts of their lives, these digital elites became disillusioned by the failure of Westphalian nation-states to adapt to the new techno-political reality. In retrospect, the vulnerability of the Westphalian, geographically defined nation-state in a rapidly digitizing world should have been more obvious.

The inability of governments to craft viable regulatory frameworks that enable technical progress while also protecting citizens has led to the rapid demise of the geographically defined nation-state. Loosely formed coalitions of stake-

holders across the various actors continue to form coalitions with the goal to create a more fulfilling society, or to garner benefits from data-enabled disruption. With greater access to the internet, individuals have gained power to bypass enforcement of regulations. As more and more critical aspects of citizens' lives have migrated online, there is a growing sentiment that the sense of belonging to a nation should be no different.

When the concept of digital nations – non-geographically linked digital communities that form a political and regulatory state based on a shared governance philosophy – first emerged, some described it as a natural extension of democracy in a digital age. The option to choose between jurisdictions that govern a citizen's rights – including personal data collection, management, and use – has increased citizens' political power vis-à-vis the state, while also helping to alleviate tensions between civil society and the state.

However, some have been less enthusiastic about this freedom. They have warned of the potential for a race to the lowest common denominator, with dire health and environmental consequences. But many – largely members of the newly online – dismissed those concerns, claiming that jurisdiction shopping had always been an option for wealthier organizations and people.

Digital nation-states remain in their infancy. Nevertheless, universal access to the internet has already helped close the global inequality gap. Not only has this given a voice to citizens previously silenced by more powerful interests in their geographically defined nation-state, it could also lead to the birth of a marketplace of digital nations.

History of the Future

EXPOSING FAULT LINES

During the first term of the Trump administration, multinational companies witnessed a sharp spike in the number and intensity of hacking incidents targeting their trade secrets and customers' personal information.

A body of intelligence reporting leaked to the public by disgruntled CIA employees credibly claimed that Russia and China were behind the attacks. The US president refused to acknowledge accountability or take retaliatory actions. Instead, he tweeted that the United States would see the use of the leaked CIA documents by other nations to justify sanctions for the sustained hacking as a "personal betrayal" to the US. He also promised to slap trade tariffs on any country that tried to make policy using the leaked information without US permission.

It became evident in early 2018 that, given their long-standing involvement and past investments, without US leadership global political and governance forums such as the G20 would fail to build consensus around geopolitical or technical solutions to mitigate the ongoing attacks. Behind closed doors, political leaders worried that the US president would follow through on his threat to retaliate with trade barriers that could cripple their economies.

By late 2018 frustration grew – among citizens, companies, and civil society – at the apparent apathy of global political leaders who took no action to address the persistent and debilitating attacks, and who instead insisted that companies should be responsible for maintaining their own security.

Building on this simmering discontent, entrepreneur Elon Musk announced a data-privacy monitoring initiative in 2018, spearheading a broader movement of third-party actors. These actors, non-governmental organizations, individual citizens, and activists tried to educate a global population that was increasingly connected, but had

failed to grasp, let alone control, its own digital vulnerabilities.

Meanwhile, the global fallout deepened from multiple revelations of leaks: The first showed that the US Central Intelligence Agency and the British agency MI6 (Military Intelligence, Section 6) had created the capability to use internet-enabled household items – early predecessors of IoT – to capture conversations through malware coined "Weeping Angel." The second WikiLeaks release, in the fall of 2017, clearly demonstrated widespread government complicity in the development and application of Weeping Angel, which caused major embarrassment to several countries, including Germany. By this time, 80 percent of household items new to the market had the ability to connect to the internet, making connected goods indispensable to consumers.

UNREST, BACKLASH, AND DE-LINKAGE

Fed up with political failures preventing growth in the digital marketplace and seeing a strategic opportunity, several large multinational companies in 2018 colluded to launch parallel public outreach campaigns. They aimed to convince consumers that governments were no longer the solution to, but actually the source of, cyber vulnerability.

The campaigns – well-timed to capture the populist discontent with existing political disruptions sweeping the globe – further eroded trust in not only national political leaders, but also the concept of the nation and the definition of citizenship. This sentiment culminated in a viral movement called "Politeia."

Protests in the run-up to the 2020 general election in the United Kingdom generated substantial popular political momentum, leading several frontrunner candidates to make promises to de-link multinational companies from national jurisdictions. They claimed that this would allow multinational companies to serve their clients better, without being tied to a system that had failed to address their fundamental security concerns.

By 2020, "de-linkage" had started to take effect, and companies began deliberately selecting jurisdictions with light regulatory requirements and weaker government enforcement. However, knowing how easy it was to turn consumers against governments, companies began to embrace voluntary transparency and accountability.

Around the same time, China achieved 70-percent internet penetration as mobile devices became the primary mode of accessing the web. Additionally, China saw substantial growth in new machine interfaces that more seamlessly integrated with everyday activities – for example, ear pieces that connect to AI-enabled assistants.

In 2021, in an effort to extend the benefits of technology to all, development banks around the world (for example the China-led Asian Infrastructure Investment Bank, or AIIB) built multinational digital platforms for the delivery of services traditionally provided by governments, further diminishing the perceived value of a geographically co-located government.

THE RISE OF E-CITIZENSHIP

Seeing an increase in technical talent arriving on the market, countries like South Korea and Estonia spotted an opportunity to recruit digital-savvy professionals by expanding their e-residency programs to offer full "e-citizenship" in 2022.

These programs – leveraging the multinational digital tools built for SDG implementation – conferred additional services such as remote medical care and education for their "e-citizens" who, for the most part, had never set foot in either South Korea or Estonia. Nonetheless, the new relationship allowed e-citizens to contribute to the national economy through labor, launching new businesses and increasing tax revenue.

Meanwhile, the viral movement Politeia recruited at least 100 million global members, after offering a concept of citizenship based on shared obligations of citizens towards the community. Seen as an opportunity to be virtuous and as an alternative to the traditional government-citizen

relationship, members worked collaboratively to provide each member digital security, fulfillment, education, and support to those who craved deeper connection in an era of rapid social change catalyzed by technological development.

By 2024, the Politeia program had expanded further, experimenting with new approaches to nationality, including opening up citizenship to individuals with only digital ties to the nation, thus further eroding the modern conception of citizenship as defined under the Westphalian system of geographically defined nation-states. This new phenomenon also triggered a worldwide debate on the future of public administration.

Despite a global appetite for a new form of public administration, netizens around the world seem to be unprepared for potential weakness of the connected technologies. The Electronic Frontier Foundation, a San Francisco-based tech advocacy group, found that only two out of every five people in developed communities were able to identify the risks of hacking, and less than 5 percent of those surveyed were able to help remedy damages caused by hackings into their home devices.

Among citizens who had recently gained access to the internet, the rapid spread of digital devices caused an even greater discrepancy in technology literacy.

With the increased rate of connectivity, demand for political participation and the provision of basic services increased. As a result of "de-linkage" and the emergence of e-citizenship, private companies and collaborative communities generated from Politeia started packaging service bundles for e-communities in 2022 – providing a broad set of services (e.g., medical treatment without constraints of national borders, financial opportunities, and digital labor opportunities) that were perceived to be more trustworthy and efficient at service-delivery than those offered by conventional nation-states.

At the same time, "Bright Web," the largest and first globally available platform designed to offer both services and also a sense of community, experienced rapid growth. By 2026, the platform had 2.3 billion users around the world, who called themselves "Bright Citizens."

In early 2027, after reaching three-billion digital members, Politeia announced it was founding the first fully digital body of citizens called "Polis," where members are both the rulers and the ruled. Important political and judicial offices were rotated, and all citizens had the right to speak and vote in the political assembly.

Within days, Bright Web also reached a critical threshold, and the opinion polls conducted on it suggested that there was a great demand for digital nation status. Providing secure, efficient digital services, Bright Web enabled its users to build a shared notion of citizenship that guaranteed the rights to digital possessions, as well as common expectations. This formed a bond that uniting people that was more impersonal, universal, and multiform than Polis, which had failed to separate their public life from their private life, making the obligations of citizenship deeply connected with everyday life.

Timeline

2017
- Political leaders worry the US president will follow through on his threat to retaliate with crippling trade barriers if they use leaked information about the US.
- Frustration among citizens, companies, and civil society about increasing hacking attacks; global political leaders remain apathetic.
- Elon Musk announces a data-privacy monitoring initiative.
- Several large multinational companies collude to launch parallel public outreach campaigns aimed at convincing consumers that governments are no longer the solution to cyber vulnerability, but actually the problem.
- A movement called "Politeia" emerges and questions the traditional concept of nation-states.
- Internet-connected household items account for 80 percent of new release market; national hacking of these items for spying purposes is revealed.
- Multiple WikiLeaks revelations occur.

2018

2019
- Companies begin deliberately selecting jurisdictions with light regulatory requirements and weaker government enforcement.

2020
- China achieves 70 percent internet penetration.
- Development banks build multinational digital platforms for the delivery of services traditionally provided by governments.
- South Korea and Estonia expand their e-residency programs to offer full "e-citizenship" in 2022.

2021
- Politeia recruits its 1-billionth global member after launching digital citizenship.
- Private companies and collaborative communities begin packaging service bundles for e-communities.

2022

2023

2024
- More countries begin experimenting with new approaches to citizenship.

2025
- Literacy among the world's population remains highly uneven.

2026
- "Bright Web" platform has 2.3 billion users, or "Bright Citizens."
- Politeia reaches 3 billion digital members and announces the first fully digital body of citizens, called "Polis."
- Bright Web also reaches a critical threshold and declares digital nation status.

2027

Scenario 3: Data Harmonization

Picture of the Future

Summer of 2027: Malika, a girl from rural Kenya who has recently graduated from junior high school, visits a cybercafe in her neighborhood every day, where she works on a data-entry job for a Chinese start-up company. Outsourcing enables the 16-year-old to earn US $20 per day on a two-month project.

She learned internet and computer basics at school, which was supplemented by virtual classrooms that brought world-class education to rural Kenya. She also learned about data privacy and security in one of the digital literacy workshops at after-school sessions under the "Open Data for Social Good in Africa" initiative, operated by the African Union and supported by G20 countries. Her earnings are credited to her by Chinese internet giant Alibaba's Alipay account. Globally, individuals, even in less-developed countries, have embraced mobile payments, which are more secure and private than traditional cash and banking. Though her family cannot afford to send her to university in Kenya, she found free courses online provided by top universities from the United States and Europe, and hopes to earn enough to start her own digital business.

Malika's story is not an anomaly. In the last decade, the steady, moderate pace of technological development, coupled with the widespread adoption of technology, has allowed many people to benefit. By acquiring new skills, they have been able to adapt to changes without the frustration and social upheaval anticipated by some. With technology facilitating the delivery of high-speed internet at a low cost, Generation Z is reaping the rewards of digitally enabled education. Moreover, innovations like robotics in farming and remote medical care have benefited many people. In certain parts of the world, people still do not receive stable internet access due to prolonged political turmoil and active terrorism. In the least developed countries, internet penetration remains fairly low; thus, the inequality gap be-tween rich and poor, individually and regionally, continues to grow.

The globalization of technology, rising threats and challenges to cybersecurity, and cybercrimes across borders have pushed nation-states to collaborate in new ways. G20 nations have reached a consensus on an interoperable framework for cross border data flows, including regulatory cooperation and access across devices, to realize technology's full benefits for the digital economy. It has also led to more than 110 countries becoming signatory to the Budapest Convention on Cybercrime. Civil society's active engagement in educating the public on data literacy resulted in the replacement of the EULAs (End User License Agreement) with more meaningful and easy-to-understand agreements between users and owners of data, giving individuals greater control over the use of their personal data. Equipped with better access to technology and a better understanding of its usage, the public is aware of potential risks and is able to navigate the data age with both trust and caution.

History of the Future

THE EVOLUTION OF INTERNET ACCESS

Since the United Nations resolved in mid-2016 that internet access be considered a basic human right,[4] recognition of this decision has grown, especially among developed countries. Following Canada's lead,[5] in early 2018 the majority of European Union member states also declared internet access a fundamental right for their citizens. Such declarations sought to benefit the digitally unconnected population that had not used the internet, especially those in rural areas, the elderly, and low-income communities. Digital literacy programs were also introduced through community organizations and government subsidies.

Apart from political commitments and civil society efforts, technology giants in the West, including Facebook, Google, and SpaceX, invested in digital infrastructure to extend internet access to under-developed regions at a fraction of the cost of laying fiber optic cables. Such efforts included low-orbit satellites, millimeter wave networks, and drones. None of these efforts led to critical change until early 2018, when a major breakthrough in satellite technology to lower latency rates emerged, promising to solve internet access woes globally.

By 2020, use of such technology allowed for access to low cost, gigabit speed internet; thus, the goal of 20 percent internet usage among individuals in the least developed countries by 2020 – set by the International Telecommunication Union of the United Nations in the "Connect 2020 Agenda for Global Telecommunication Development"[6] – was successfully met. By the end of 2022, internet penetration reached 70 percent globally, and many in the least developed countries in Africa and Asia finally became connected.

The steady growth in internet access across the globe was also accompanied by wider adoption of digitally enabled advanced technology such as automation, artificial intelligence, and digital payment methods.

BENEFITS OF TECHNOLOGY ADVANCEMENT ARE SEEN IN MULTIPLE ARENAS

With the drive towards a "less cash" society in 2017, a surge of digital payment companies appeared in India and China. In less developed economies, even hawkers, vendors, and rickshaw pullers started accepting digital payments. By 2019, digital payments were accepted by more than 100 million merchants internationally, with MSMEs (Micro, Small and Medium Enterprises) constituting 70 percent of over 1 trillion transactions globally, and most carried out on smartphones. In many countries, global payment companies like PayPal and Alipay partnered with local companies like Paytm in India to provide such services. The US and India also began "central-bank controlled" digital currencies.

Growing access to the internet sped up the generation and collection of data across all sectors. At the International Open Data Conference 2021 held in Abuja, Nigeria, the "Open Data for Social Good in Africa" initiative was officially launched. The initiative lasted for five years and significantly enhanced the quality of open data across the continent in terms of accuracy, consistency,

4 Tim Sandle, "UN thinks internet access is a human right," *Business Insider*, July 22, 2016, last accessed May 5, 2017, http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7.

5 Lauren McCauley, "In Historic Decision, Canada Declares Internet Access a Fundamental Right for All, December 22, 2016, accessed May 5, 2017, http://www.commondreams.org/news/2016/12/22/historic-decision-canada-declares-internet-access-fundamental-right-all.

6 International Telecommunications Union, "Connect 2020 Agenda for Global Telecommunication Development," accessed May 5, 2017, http://www.itu.int/en/connect2020/Pages/default.aspx

and completeness; aggregated a regional cloud-based data portal where governments and private companies could publish data for public use; and supported a cross-border campaign for digital literacy education, especially on data privacy and security.

In December 2026, a magnitude 9.3 earthquake struck beneath the Indian Ocean near Malaysia, generating a massive tsunami that affected 11 different countries. New technologies were quickly deployed to address the deadliest natural disaster, which could have killed more than 200,000 people than in the 2004 tsunami. More than 1,000 drones were sent out for post-disaster assessment and medicine delivery to places where road access was not possible. Robots with cameras, microphones, and sensors searched for victims stranded in flooded homes and on rooftops. Centralized data from Unmanned Aerial Vehicles (UAVs) and robots were released in real time, and accessible by all the rescue teams on the ground. For those who were rescued but injured, Médecins Sans Frontières ran around-the-clock mobile clinics in remote areas where access to medical care was severely limited. Within the 72-hour "golden window" for rescue, more than 100,000 people were rescued or helped with the aid of AI-enabled UAV technology.

IMPACT OF AUTOMATION AND ARTIFICIAL INTELLIGENCE ON LABOR MARKETS

At the World Economic Forum 2019 meeting in Davos, developing countries like India and China highlighted the challenges posed by increasing automation on rising unemployment in domestic sectors such as manufacturing. Increasing automation and the widening application of artificial intelligence-enabled software significantly reformed some sectors, such as the emergence of automated farming and drone-equipped real estate development. As a result, many manual labor-oriented and service jobs were replaced. By 2020, smart robots powered by AI had displaced 15 percent of workers in Europe, compared with 2012. Meanwhile, high-skilled professions in fields such as law, analytics, and accounting also witnessed heavy use of AI-powered software. Determined to embrace technology and maximize its benefits for national economic development, Chinese and Indian manufacturing industries embarked on a journey to transform from labor-intensive to highly automated. They also became the world's largest producers of robots and drones, generating products that were predominantly exported to the West, where adoption of advanced technology was more widely accepted by industry and the public.

With labor displacement and automation also came large-scale social unrest. In 2022, mass protests swept major cities like London, Chicago, Shenzhen, and Kolkata, where manufacturing and service sector labor were rapidly replaced by automation. In response to civil unrest, companies benefiting from automation were required to pay a certain percentage of their earnings to the government, which then reinvested the funds into training programs to transition and upskill affected citizens to new jobs. Additionally, India's introduction of a universal basic income over five years inspired other developing and developed economies to follow suit. The rising use of new technology in emerging sectors also faced the challenge of a shortage in educated workers to operate high-tech robots and AI. To solve the problem, governments around the world began reallocating budget funds to educate workers on these new technologies through massive public training programs.

UNINTENDED CONSEQUENCES OF TECHNOLOGICAL ADVANCEMENT

Not all of the new technological advances since 2017 have benefited the social good. One of the worst cases in recent years was the drone attack at the 2020 Tokyo Olympics that injured and killed more than 300 members of the US and Israeli Olympic delegation, including political leaders and athletes. Daesh deployed weaponized commercial drones to attack the delegations attending the closing ceremony at the event, accurately targeting the zone where the US and Israeli delegations were, as a retaliation to operations in Syria and Iraq. It was orchestrated by hacking the radar system so that UAVs went undetected while they moved from a launch site

10 kilometers away towards the stadium. This incident, along with similar events around the world, led to international discussion on how to create additional, global standards and regulations on technologies. The reflections led to increased security and more controlled usage of technology, which was crucial to restore public confidence in technology.

As these events indicate, many were unhappy about technology's advances and its increasing role in their lives. For some, opposition has been driven by technology-related health issues such as eyesight problems or neck pain from longtime smartphone usage; some were concerned with over-reliance on technology dampening community cohesion and the ability to empathize with people from different walks of life; others saw it as a threat to their livelihood.

DEVELOPING INTERNATIONAL NORMS

As discussions about mass surveillance increased again following the 2017 WikiLeaks publication of CIA capabilities and operations – a sequel to the 2013 Snowden revelations – more nation-states felt the need to have a better grip on regulating and controlling cyberspace within their national boundaries to restrict external interference and surveillance. The growing wave of protectionism across the globe, coupled with the emergence of inwardly focused leaders and governments, resulted in some countries establishing sovereign DNS Root Server Systems by the end of 2018 to secure full control over DNS traffic generated in the country.

A few nations in the EU, such as Poland, Italy, and Greece, who were falling behind on the Digital Economy and Society Index, seized the opportunity to impose restrictions on the localization of Information and Communication Technology (ICT) assets and data, enforcing how data can be processed in their territories in the name of "citizens' privacy." Some Asian and African countries took similar steps as they sought to protect national security. This had a big impact on companies such as Google, which had less than 10 data centers by 2017, but had to set up more than 100 data centers around the world, as well as local offices with technical and legal support. By 2022, the economic impact of server localization was far reaching, with the business community joining forces and opposing the move, which led to a rapid decline in their profit margins and increasing regulatory pressure. The G20 took notice of the move, and initiated dialogue on increasing collaboration and trust to reduce pressure on the economy and trade.

In parallel, realizing the benefits derived from digital technology, and in order to address the misuse of AI-powered technology by cybercriminals and terrorists, international leaders gathered at the United Nations General Assembly 2020, to discuss effective collaboration and fighting common menaces. Moreover, given the challenges of interoperability across borders, the need emerged for standards and frameworks to enhance the use of technology and facilitate trans-border data flows. Europe's shrinking market share of the global digital economy led the EU to formally align its General Data Protection Regulation (GDPR) with APEC Cross Border Privacy Rules (CBPRs), which had very different approaches for governing data flows. GDPR was amended to incorporate changes. As a result, some of the stringent conditions for data transfers were relaxed to enable its businesses to leverage outsourcing benefits. Since the EU previously had been on a different track than the rest of the world on the issue of data flows, this move was appreciated by a majority of member states in the UN General Assembly.

As privacy and security standards were enhanced, global collaboration became the new norm, and moderate technology development was coupled with new social safety nets such as free re-education opportunities for high technology training. Security and privacy-enhancing technologies improved in tandem with overall technological progress. "Security by Design" and "Privacy by Design," defining principles of building secure products, were incorporated into the design of technology protocols, architecture, and standards, such as RFC 9310 of Internet Engineering Task Force (IETF) and IEEE 801.4 IoT Data Processing standard. Backed by the assurance of global cooperation,

the public's trust in technology increased and its adoption grew in all aspects of life.

Now, in 2027, the number of signatories to the Budapest Convention on Cybercrime has reached more than 110 countries, and is backed by the strong support of corporations asking for more effective regulations on privacy and security. Civil society's active engagement has also led to the replacement of the EULAs (End User License Agreement) with a more simplified and meaningful agreement, which now allows individuals increased control and better understanding over the use of their personal data.

Also, after a series of discussions among countries over the past 10 years, the UN tabled the Cybersecurity and Cybercrime Convention Draft in its 82nd General Assembly meeting. In order to deal with the differences in legal systems among countries and regions, The Hague has established a dedicated International Court of Justice for Cybercrime and Data Abuse based on the Convention, with support from UN, creating a common ground for mediation between all stakeholders.

Timeline

2017

- The majority of European Union member states declare internet access a fundamental right for their citizens.
- Digital literacy programs are introduced.
- Technology giants in the West work on universal internet access.
- Some countries establish sovereign DNS Root. Server systems to have full control over DNS traffic generated.

2018

2019

- Digital payments are accepted by more than 100 million merchants internationally.

2020

- Internet penetration reaches 70 percent globally.
- Companies are required to pay a certain percentage of their earnings into training programs run by federal, state, or local governments.
- The economic impact of server localization is far-reaching, with the business community opposing the move.
- "Security by Design" and "Privacy by Design" are built into the design of technology protocols, architectures, and standards.

2021

- Use of satellite technology enables people to have access to gigabit speed internet at a low cost.
- In Europe, smart robots powered by AI displace 15 percent of workers.
- China and India become the world's largest producers of robots and drones.
- Drone attack at the 2020 Tokyo Olympics by ISIS on US and Israli citizens.
- EU formally aligns its General Data Protection Regulation (GDPR) with APEC Cross Border Privacy Rules (CBPRs).
- At the International Open Data Conference 2021 held in Abuja, Nigeria, the "Open Data for Social Good in Africa" initiative is officially launched.
- A few nations in the EU, such as Poland, Italy, Greece, impose restrictions on Information and Communication Technology (ICT) assets and data.

2022

2023

2024

2025

- New technologies are quickly deployed to address the magnitude 9.3 earthquake that strikes beneath the Indian Ocean near Malaysia.

2026

- More than 110 countries become signatories to the Budapest Convention on Cybercrime.
- The UN tables the Cybersecurity and Cybercrime Convention Draft in its 82nd General Assembly meeting.

2027

Opportunities, Threats, and Major Insights

Looming Power Battles

Perhaps unsurprisingly, in all three scenarios the private sector will hold the most control over technology and data. And in every scenario there is an opportunity for technology companies to grow revenues and challenge traditional industrial players. This leads us to ask: How will technology companies deal with their increasing power? To what extent will other institutions and actors be left behind, and how will they respond to corporate dominance?

The evolving relationship between governments and companies is especially deserving of our attention. While there have already been first attempts to reign in international – often American – companies back, especially in Europe, these efforts will only increase if technology companies do not address the mistrust that they are encountering across the world. In the next years, governments may react with heavier regulation, which, if not coordinated across countries and regions, could not only lead to higher costs for technology companies, but challenge the nature of an open, interoperable internet.

Governments themselves will also face increasing pressure. They run the risk of seeming antiquated and unable to keep pace with technological advancements, but a far greater danger awaits if they fail to understand rising technological trends and their implications. There are a variety of looming threats that do need a governmental response: not only securing large amounts of data and shaping regulation so that companies do so as well, but also addressing societal instability and job loss due to automation. If governments fail to address these issues, they will lose legitimacy, as Scenario 2 outlines.

Automation relates to another major hand of our report: inequality. This relates to questions of social welfare: if robots take over jobs, how will profits be shared and taxed? This also touches on access to the internet and control of one's own data. Who will have the luxury to be online? Or, depending on the scenario, who will have the luxury to be offline? Such inequality will not only play out domestically, but between nations. In each of our scenarios, we see digital literacy as a key factor. Without a doubt, technology can empower individuals by allowing them to amplify their voice, connect, and organize online. Individuals also face the risk of becoming pawns in the battles described above. Cybercriminals, governments, and companies will all be after their data, and netizens will need to learn how to protect it.

Who Runs the World in 2027?

This opens up a window of opportunity for civil society organizations. They not only play a role in educating the public and fighting for civil liberties, but in facilitating dialogue between different stakeholders – especially as it has become clear to all involved in this process that the challenges at hand are too complex and important to be understood or dealt with by one organization or entity alone. To address the future of data governance, more multi-stakeholder exchange is necessary.

After developing our scenarios, the GGF 2027 data governance working group discussed the major insights derived through the process. Although we agreed that technology innovation is unstoppable and will inevitably change society and its governance discourse, we also believe that the way society and its actors respond to such technological changes will ultimately determine the future course of technological development.

Indicators

All the previously discussed scenarios are plausible, yet not all the aspects are likely to come true. To make it easier to track in which direction the world is headed, the indicators below serve as observable phenomena that point to the emergence of different scenarios.

Scenario 1: Towards "De-Digitization"	Scenario 2: Rise of the Digital Nation	Scenario 3: Data Harmonization
Critical infrastructures become disconnected from rest of the internet.	Number of countries providing e-citizenship increases.	Increasing number of countries ratifying Budapest Convention on Cybercrime.
Decrease in sales of devices.	Increase in population that considers itself a "global citizen".	G20 nations reach consensus on cross-border data flow arrangements.
Increasing number of devices that allow for data ownership and decentralization.	Number of people online increases.	Number of legal documents negotiated/ratified increases.
Increasing number of data breaches (both in governments and companies).	Corporations win increasing number of lawsuits against governments.	Improvement in health and educational outcomes attributed to access to internet and smartphones.
		EULAs are replaced by meaningful agreements between users and platform operators.
		Individual attacks without an overarching hierarchical group.

Scenario-Planning Methodology

The strategic foresight methodology provides a systematic approach to comprehending uncertain futures. For our task we utilized "scenario planning," which required three key steps. First, the working group collectively identified factors that would influence the future development of data governance. Then, we determined which factors are more impactful and more uncertain than others. Once these were identified, we projected outcomes for each factor, and used a consistent set of factor projections to create both a picture of the future in 2027, as well as the history of the future from 2017 to 2027.

FACTOR IDENTIFICATION: Our first challenge was coming to a shared understanding of the term "data governance." While this was not part of the formal methodology, the process was crucial to identifying important factors. Once we reached a shared understanding, it became apparent that the major factors were those that identified a trait about the interrelation of organizations and data. These included factors such as "trust among all actors," "tech literacy," and "evolving expectations of privacy." In a topic as nebulous as data governance, we ultimately identified over 50 potential factors that ranged from highly specific (e.g., "commercialization of military-grade technology") to more systemic (e.g., "global governance of identity").

FACTOR ANALYSIS: Grouping these factors into more concrete and distinguishable ideas helped define the major points and issues we thought were most impactful. Some areas, such as technological literacy, were easier to identify, while others, such as "regulation of the data economy," encompassed multiple ideas that stretched corporate, national, and international domains. Ultimately, we agreed on the following eight key factors:

› Technological development;
› Norms, protocols, and standards for data interoperability;
› Regulation of the data economy;
› Ability to enforce norms and regulations in cyberspace;
› Access to and affordability of the internet;
› Technical literacy and awareness;
› Tensions between actors (societal, political, economic);
› Trust in technology and data.

For each factor, we identified three to four different potential outcomes.

SCENARIO CONSTRUCTION: In the next step, we selected a factor and one of its projected outcomes until we had worked with all eight factors. We repeated the process two more times, always choosing differing outcomes for all factors. Eventually, this led us to develop three unique yet coherent and plausible scenarios. For each scenario, we developed a picture of the future, and later worked our way back to a history of that future. Once the three different futures began taking shape, we derived opportunities and threats for various actors across scenarios.

Fellows of the Data Governance Working Group

Cathleen Berger
Global Engagement Lead, Mozilla

Yolanda Jinxin Ma
Consultant, Asia Pacific Bureau of the United Nations Development Programme

Vincent Ni
Senior Producer, BBC World Service

Elizabeth Prescott
Deputy Director and CTO, National Security Technology Accelerator, National Defense University

Reirui Ri
Fellow, Stanford Law School

Shireen Santosham
Senior Policy Advisor and Chief Innovation Officer, Mayor's Office, San Jose, California

Rahul Sharma
Senior Consultant, Data Security Council of India

Satyarupa Shekhar Swain
Director, Government Outreach and Advisory group, Citizen Consumer and Civic Action Group

Evan Sills
Associate, Good Harbor Security Risk Management
Shoko Yoshihara, Research Fellow, Tokyo Foundation

Shoko Yoshihara
Research Fellow, Tokyo Foundation