



Instituting Data Governance for Advancing Digital Government

Abstract

Government innovation and digital government are in most cases driven by data. Data security and privacy issues have become significant concerns for both policy makers and citizens. Many recent incidents such as the Facebook data breach have triggered the debate on how government can effectively ensure that big IT companies protect personally identifiable information (PII) and comply with data protection laws. Against this background, instituting data governance for advancing digital government has gained even greater importance. Although the concept is continuously evolving, data governance is generally about setting “data standards and policies to manage the availability, usability, integrity, and security of the data employed in an organization”.¹ It is important to note that data governance is more about the framework and process than simple technical data management capabilities.

Data governance for government is different from that of the business sector, as government is the service provider using PII and also the data generator through its large-scale operations. Government also acts as the regulator and guardian of privacy of the users and citizens. Many countries have been making strenuous efforts to enhance resilience of IT infrastructure against cyberattacks, as cyberspace security in the contemporary digital era has been elevated to national security in many cases. Effective data governance requires that relevant laws and regulations are adapted to the changing digital dynamics and that compliance to these laws is ensured. This is evidenced by many country practices particularly the recent EU General Data Protection Regulation (GDPR) which has become effective as of May 25, 2018. Governments need to take a holistic and government-wide approach to institute data governance, in collaboration with all relevant stakeholders including private sector, academia, civil society organizations and citizens.

¹ <https://searchdatamanagement.techtarget.com/definition/data-governance>



I. Introduction

Government innovation is in most cases driven by data with increasing recognition and endorsement of open source, open code and open standard. The efficient delivery of digital government services has become more dependent on real time big data with close collaboration among all stakeholders including the private sector and citizens. In recognition of the importance of multi-stakeholder collaboration in the digital field, the United Nations Secretary-General António Guterres has recently established the High-level Panel on Digital Cooperation and appointed 20 Panel members across from government, private industry, civil society, academia and the technical community, with the aim of promoting a cooperation framework and interdisciplinary approaches “to ensure a safe and inclusive digital future for all”.²

Meanwhile, data security and privacy issues have become significant concerns for both policy makers and citizens. For example, the recent data leak controversy of the India’s digital ID System *Aadhaar* raised concerns about the government’s ability and responsibility to protect citizen’s private data and heightened fears on privacy violation [Box 1].

Moreover, the recent Facebook data breach incident [Box 2] triggered the debate on how government can effectively ensure that big IT companies protect personally identifiable information (PII) and comply with relevant data protection regulations and laws, especially when those big IT companies like Apple, Twitter, Google, and LinkedIn have become part of the ecosystem and the platforms for service delivery and citizen engagement. Against this background, instituting data governance for advancing digital government has gained even greater importance. Data governance, although the concept is continuously being developed and widely employed by IT sectors for many years, is generally about “data standards and policies that manage availability, usability, integrity, and security of the data employed in an organization”.³ More and more countries are developing and updating relevant regulations and laws adapting to the changing digital dynamics and ecosystems while enforcing the compliance by IT companies and private sector with legal framework, particularly the recent EU General Data Protection Regulation (GDPR) which has become effective as of May 25, 2018 [Box 3].

[Box 1]

India: Digital ID System *Aadhaar* Data Leak

India launched its biometric identity programme *Aadhaar* in 2009. Being the largest biometric identity programme in the world, nearly 1.2 billion Indian citizens and residents, which accounts for about 15 percent of the global population, are enrolled in *Aadhaar* (OECD, Embracing Innovation in Government: Global Trends 2018, p. 27). Each *Aadhaar* recipient receives a unique 12-digit ID number, and users’ photo and biometric data in the form of fingerprints and iris scans are submitted (Ibid). This system is now widely used in many parts of people’s everyday life in India, such as bank transactions and activating a mobile phone (Ibid).

However, in January 2018, *Aadhaar* was reported to have the problem of data leak and privacy intrusion, as it was possible to purchase access to *Aadhaar* details for every registered *Aadhaar* number, including names, addresses, postal codes, phone numbers and email addresses, from anonymous sellers, taking only 10 minutes and cost of 7 Euros (<http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>). This privacy breach raised concerns about the Indian government’s ability to protect its citizens from hackers and led to growing fears on privacy violation.

[Box 2]

Facebook-Cambridge Analytica Data Breach

It was reported in March 2018 that a British political consulting company Cambridge Analytica harvested personally identifiable information from the Facebook profiles of more than 50 million users without their permission. About 270,000 of those users actually consented to share some of their information, while the rest of the people had their data stolen in the security breach. The breach was significant for inciting public discussion on ethical standards for social media companies, political consulting organizations, and politicians. Consumer advocates called for greater consumer protection in online media and right to privacy as well as curbs on misinformation and propaganda.

² United Nations Press Release. United Nations Secretary-General Appoints High-level Panel on Digital Cooperation 12 July 2018, <https://www.un.org/press/en/2018/sga1817.doc.html>

³ <https://searchdatamanagement.techtarget.com/definition/data-governance>

[Box 3]**EU General Data Protection Regulation**

The EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and became effective on 25 May 2018. The GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. Stronger rules on data protection mean: i) people have more control over their personal data; and ii) businesses benefit from a level playing field.

As digital government is one of the core work areas of the UN Department of Economic and Social Affairs (UN DESA), and considering the importance of instituting a robust data governance for advancing digital government, the main objective of this Policy Brief is to provide a conceptual framework of data governance and its implications from the government perspective. This Policy Brief will also provide some policy recommendations for instituting data governance to advance digital government.

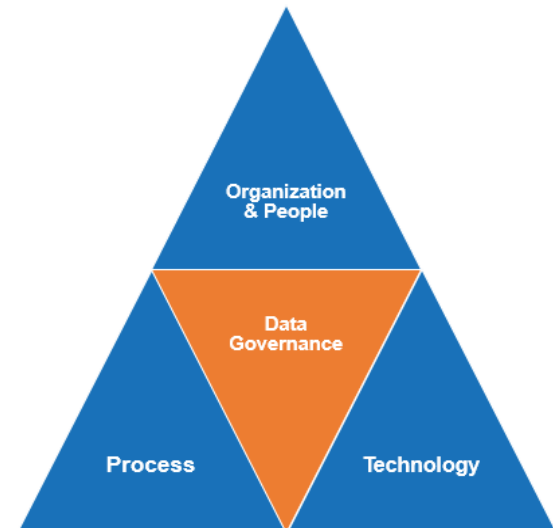
II. Data Governance from the Perspective of Government

2.1 What is Data Governance?

Data governance in general refers to “the overall management of the availability, usability, integrity, and security of the data employed in an enterprise.”⁴ Some other definitions of data governance include: “the practice of organizing and implementing policies, procedures and standards for the effective use of an organization's structured/unstructured information assets,”⁵ and “the execution and enforcement of authority over the management of data assets and the performance of data functions.”⁶

To be more specific, data governance includes three dimensions: i) **organization and people** at three levels, which in most cases include - *the strategic committee or board* for designing the

strategy, *the tactical team* for setting the approach to implementing the strategy, and *data stewards* for actually managing the data governance; ii) **process** – to define and enforce data standard and policies, and audit, monitor and control of data governance activities; and iii) **technology** – to secure infrastructure, identity and access control, information protection, auditing and reporting.



[Figure 1] Three Dimensions of Data Governance
(Source: By authors)

2.2 Data Governance from the Perspective of Government

The concept of data governance can be interpreted and applied differently in government from that of the general practice by the private sector. Considering the multi-dimensional nature of government as i) the provider of public goods and services, ii) data collector and keeper of personal data, iii) data generator through its massive operations, and iv) guardian of citizen privacy, coupled with the complexity and challenges of ensuring data security and privacy, data governance from the perspective of government requires a more holistic approach with collaboration of all stakeholders. In brief, it can be defined as “government-wide governance structure for setting the policy and strategy for data collection/gathering, data classification, naming conventions data processing, access control, usage and analysis, data release and data security throughout the information life cycle and consistent across government agencies.”⁷ Considering data governance

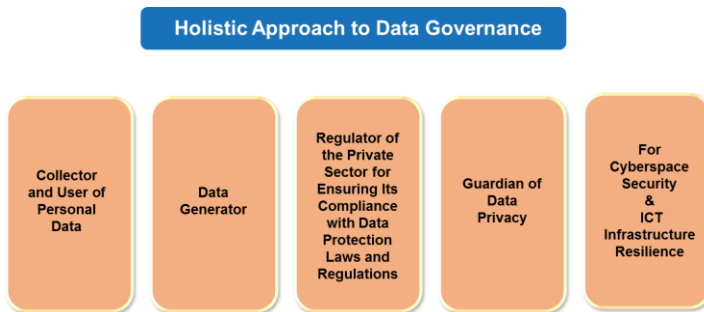
⁴ <https://searchdatamanagement.techtarget.com/definition/data-governance>

⁵ Ketan Phanse (2008) Data Governance using SAP MDM - Part 1. <https://archive.sap.com/documents/2008/02/29/60022998-5d17-2b10-dbaa-8e3ab357fa55/Data%20Governance%20using%20SAP%20Master%20Data%20Management%20-%20Part%201.pdf>

⁶ Robert S. Seiner (2006) The Data Stewardship Approach to Data Governance. <http://tdan.com/the-data-stewardship-approach-to-data-governance-chapter-1/5037>

⁷ Presentation on *Laws and Regulations & Data Governance* by Keping Yao, Governance and Public Administration Expert of UNPOG/DPIDG/UNDESA, delivered during the Executive Development Course on *Digital Government for Transformation Towards Sustainable and Resilient Societies – The Singapore Experience*, held on 2-6 April 2018 in Singapore.

as cross-cutting from the perspective of government, the multi-dimensional roles of government in data governance are further elaborated in this part.



[Figure 2] Holistic Approach to Data Governance
(Source: By authors)

Government as the collector and user of personally identifiable information

Governments collate and utilize personal data in designing and delivering digital government services and governments are generally the biggest users of personal data. Governments hold personally identifiable and commercially sensitive information, especially with more countries introducing eID or digital ID system, which include biometrics information, bank account information, driver license, customer registered info for providing integrated services.

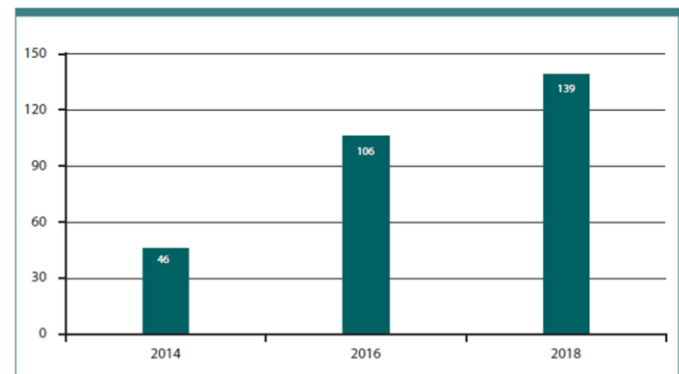
When collaborating with other agencies or outsourcing to third parties for delivering certain types of digital government services, governments should apply the same data governance rules. It may happen that other agencies or third parties could: i) gain access to database without knowing by or duly noting users; ii) use data without following proper rules and procedures; iii) not fulfill the data protection responsibilities; and iv) possibly maximize the commercial value for sharing data with other parties.

Meanwhile, it is important that governments collect and produce disaggregated data to ensure that the special and unique needs of vulnerable groups can be addressed through inclusive digital services. Governments and other stakeholders must work together to establish baseline data for the vulnerable groups and devise innovative strategies to identify and address their needs. Without disaggregated data, inclusive policies and programmes cannot be developed to address vulnerable groups' needs.

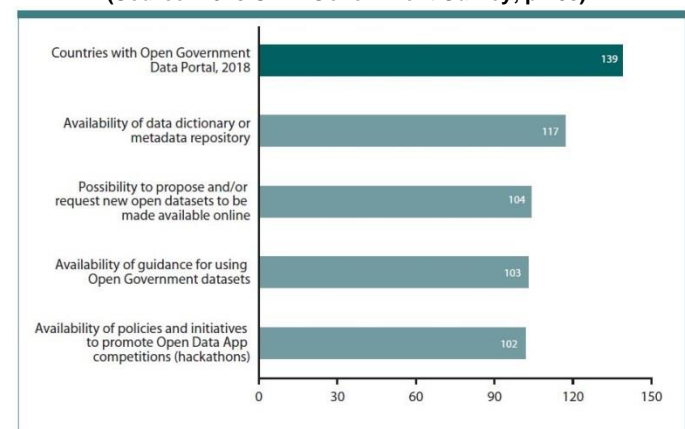
Government as data generator

Government operations also generate huge amounts of data, typically provision of essential public services, tax collection, government expenditures, disbursing social benefits, environment protection, and government efforts to address climate change. Opening government data to citizens has become a general trend for enhancing transparency and accountability of the public sector; and using open government data can create new services and lead to innovation and job creation.

One of the most prominent forms is open data, which refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.⁸ More and more countries these days are providing data in open standards. Open Government Data (OGD) enables citizens and the private sector to create new types of innovations and services by using the data provided. It also enhances transparency and accountability of government and contributes to achieving sustainable development as well.



[Figure 3] Countries with Open Government Data Portal and/or Catalogues in 2014, 2016 and 2018
(Source: 2018 UN E-Government Survey, p.108)



[Figure 4] Functionalities of Open Government Data Portals 2018
(Source: 2018 UN E-Government Survey, p.108)

⁸ <https://policy.cio.gov/open-data>



[Figure 5] Personal Data Protection Legislation Available Online
(Source: 2018 UN E-Government Survey, p. 74)

Government as regulator of the private sector for ensuring its compliance with data protection laws and regulations

One important role of government in data governance is to establish the legal framework and enforcing compliance by both government itself and the private sector, especially in the era of Internet of Things (IoT), big data analytics, and Artificial Intelligence (AI). Especially, there are now increasing concerns of further exclusion of vulnerable groups with the rise of AI in some countries. Most countries do not have a single and comprehensive law regulating the collection and use of personal data. For example, in the United States, there are several acts regulating the data use and collection with regard to consumer protection, financial transactions, medical information, credit reporting and computer fraud and abuse act⁹.

Regulating practices on data use and collection of big private commercial and IT companies is high on the government agenda. Many cases show that the data security breach could be caused by attacks by hackers, data selling by internal staff, and relevant agencies gaining access to database without the knowledge of users and in violation of the data protection responsibilities. One recently known data breach case released on March 20, 2018 is the data security breach by Orbitz, an Expedia subsidiary, which impacted around 880,000 payment cards and potentially the personal

information of its customers to hackers¹⁰.

Some private companies often share and exchange their customers' data for data mining to offer better services without duly notifying customers. Some private companies may buy customers' data from third parties to provide customized services to their customers, who are more attracted to personalized information specific to their needs. In this regard, many governments have started to regulate data-sharing among private companies.

Government as guardian of data privacy

In the digital era, citizens are weak in protecting their personal privacy. Therefore, governments need to play the key role of protecting privacy of citizens and companies. Governments need to develop and implement legislations that can protect citizen's privacy by putting it as a priority in designing strategies for digital government development. It is also the responsibility of government as a privacy guardian protector to ensure compliance of different rules and regulations for data and privacy protection.

Furthermore, many governments are developing and updating relevant laws and regulations to secure privacy of citizens under the changing digital environment. It is particularly important for governments to develop new legal frameworks and update existing laws and regulations, as the emergence of new technologies, such as AI, IoT, and blockchain, pose new types of challenges in privacy protection and data security. Systems and devices that are based on the application of these new technologies have access to PII, and it is important to ensure that laws and regulations are updated and adjusted to deal with data protection and security concerns arise from the use of these technologies. The regulation over the automated decisions made by AI and machine learning, as in the case of the GDPR, is one example.¹¹ Another example is legal code to regulate Bitcoin, which is becoming popular with the increasing use of blockchain, as in the case of the BitLicense issued by the New York State Department of Financial Services to businesses offering digital currency services.¹²

⁹ These include: i) The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) - a federal consumer protection law, which prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies; ii) The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827); iii) The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.); iv) Children's Online Privacy Protection Act of 1998; v) The Fair Credit Reporting Act (15 U.S.C. §1681) and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159); and vi) The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030).

¹⁰ <https://www.reuters.com/article/us-orbitz-cyber/expedias-orbitz-says-880000-payment-cards-hit-in-breach-idUSKBN1GW23V>

¹¹ D. M. West and J. R. Allen (2018) How Artificial Intelligence is Transforming the World. <https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/>

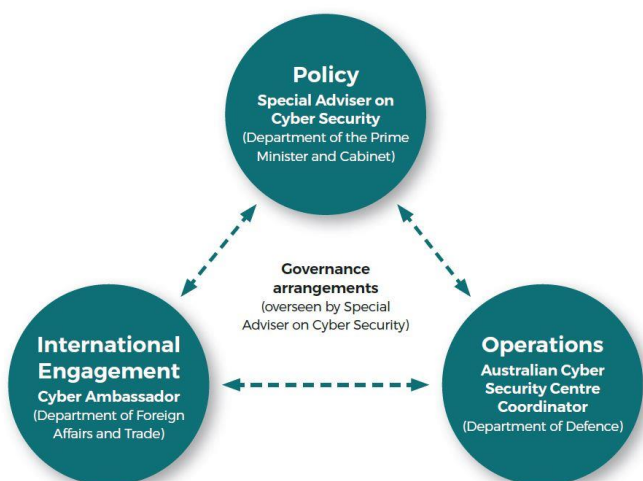
¹² New York Department of Financial Services, 'BitLicense Regulatory Framework' https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

Government for safeguarding cyberspace security and enhancing ICT infrastructure resilience

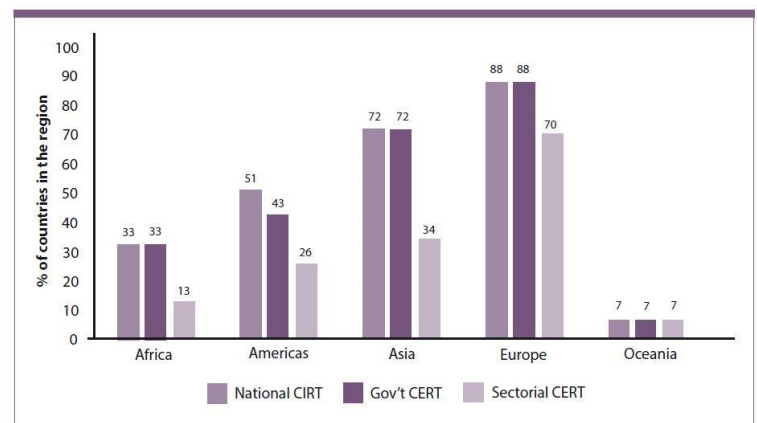
Cyberspace security has become of general concern to governments and building resilience in IT infrastructure against cyberattacks has been elevated to the level of national security. It is quite common practice that governments set up the national Computer Emergency Response Team (CERT), Cyber Incident Response Team (CIRT), or the Computer Security Incident Response Team (CSIRT). For example, in Australia, the Special Adviser reports to the Prime Minister and the CERT Australia works in collaboration with over 500 businesses and advises on cyber security threats to the owners and operators of Australia's critical infrastructure. The Australian Cyber Security Centre, established in 2014, gathers cyber security capabilities across the Australian Government to enable collaborating and sharing threat information.

In Malaysia, the Cyber Security Malaysia, which is the national information security coordination center, – safeguards national cyber security.

Governments must ensure the ongoing access to systems and records and business continuity of digital government services, particularly data archiving and backup in times of disasters and other emergencies.



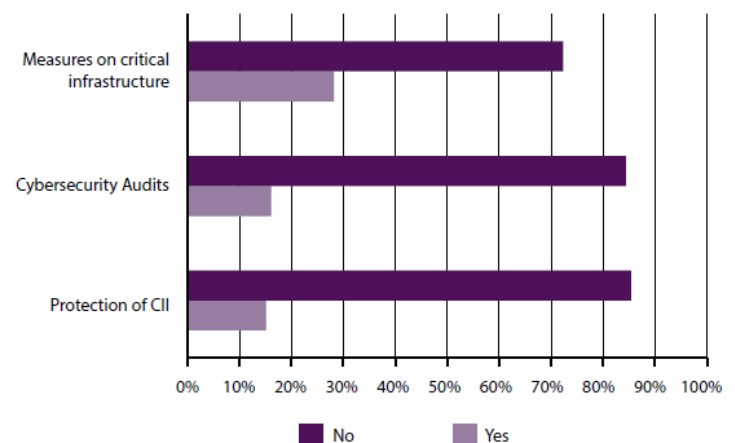
[Figure 6] Australia National Cyber Security
(Source: Australia's Cyber Security Strategy)



[Figure 7] Regional View of CERT/CIRT/CSIRT
(Source: 2018 UN E-Government Survey, P. 77)

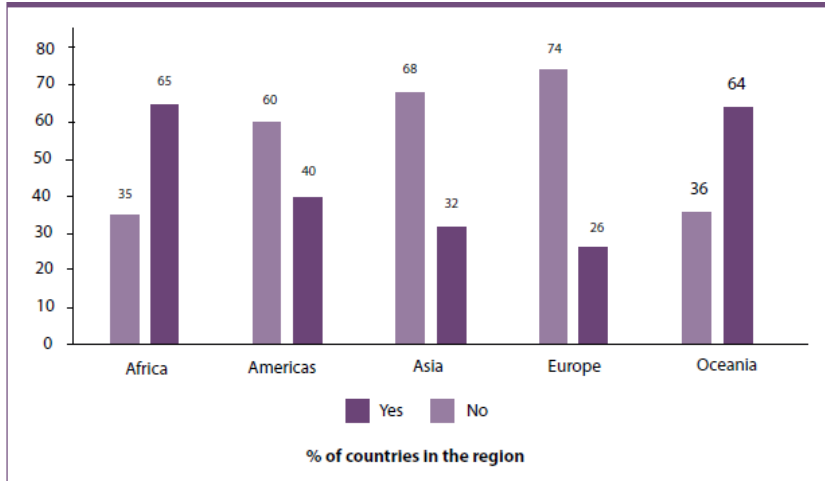
III. Importance of Data Governance for Digital Government

Instituting data governance is essential for digital government, which is increasingly dependent on real time big data. The importance of effective governing of data for government is growing significantly in the fast changing digital environment. It is projected that global data will grow to 44 zettabytes (ZB) by 2020, and 85% of this data growth is expected to come from new types.¹³ This means that the amount of data used, collected, stored and managed by government is increasing exponentially, and the types and characteristics of these data are changing rapidly as well. In addition to the privacy and data security concern illustrated in Part 2 of this Brief, there are a number of important factors related to data governance for digital government development.



[Figure 8] Percentage of Countries with CII Protection Included in Their Registration or Cyber Security Strategy
(Source: ITU GCI Report 2017)

¹³ The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. April 2014. <https://www.emc.com/leadership/digital-universe/2014/view/executive-summary.htm>.



[Figure 9] Countries with Cyber security Legislation Online
(Source: 2018 UN E-Government Survey, p. 74)

3.1. Data Governance for Effective Digital Public Services

Robust and effective data governance is important for effective public service delivery by government. A great part of public services delivered by government have gone digital, using data and other digital platforms. Many countries use big data and data analytics to better understand the demands of their citizens and improve the responsiveness, efficiency and effectiveness in their service delivery. This is particularly important in ensuring that their public services are inclusive and accessible by the poorest and most vulnerable. For example, big data analytics is used for essential areas such as healthcare and disaster risk reduction.

Also, effective data management is crucial for providing integrated digital services. For example, digital ID system, which is based on personal data of individuals including biometric data, is the basis for all other digital services. According to the 2016 UN E-Government Survey, 98 countries require a digital ID for online and mobile public services.¹⁴ Such cross-cutting data sharing between and among government agencies will promote whole-of-government approach to its public service delivery.

¹⁴ 2016 E-Government Survey, p. 8.

3.2. Data Governance for Transparent and Accountable Government

Effective management and sharing of data through working data governance is important for promoting transparent and accountable government as well. Many governments nowadays share open source, open code and open data with citizens. Open government data (OGD) has become a general trend for governments to enhance transparency and accountability. Many governments include open data as a separate evaluation category for assessing the performance of government and public institutions, and supports the commercialization of public ideas uncovered by various start-up contests and hackathons. For example, the Republic of Korea is pursuing data-driven sustainable economic growth through an active engagement and efficient use of public data in promoting the creation of new jobs and business opportunities. And, the Act on Promotion of the Provision and Use of Public Data has been enacted for the provision and use of public data.

3.3 Data Governance for Building Public Trust in Government and Encouraging User Uptake

Trust plays a very tangible role in the effectiveness of government¹⁵. According to OECD, trust in government is deteriorating in many OECD countries. Lack of trust compromises the willingness of citizens and business to respond to public policies and contribute to a sustainable economic recovery¹⁶. One important barrier for many citizens not using digital government services is lack of trust in government regarding the storage and access to personal data. According to the survey conducted by the Economist Intelligence Unit (EIU) for the Inclusive Internet Index 2018, a great number of respondents across regions have low trust in online privacy, and this discourages their use of the Internet.¹⁷

¹⁵ OECD Trust and Public Policy. <http://www.oecd.org/governance/trust-and-public-policy-9789264268920-en.htm>

¹⁶ OECD Directorate for Public Governance: Trust in Government. <http://www.oecd.org/gov/trust-in-government.htm>

¹⁷ The Economist Intelligence Unit (2018). The Inclusive Internet Index 2018 - Executive summary, p.2. <https://theinclusiveinternet.eiu.com/summary>

IV. Policy Implications

First, considering the multi-dimensional roles of government in instituting data governance, and the importance of a robust and dynamic data governance for advancing digital government, government should, **put data privacy first and establish legislation with foresight** and review and amend existing laws and regulations to be adapted to frontier technologies and new digital environment including the cloud environment.

Second, government should **build up a government-wide data governance system that brings in all government departments** to enforce the data governance in a consistent manner across all government agencies.

Third, government should **adopt inclusive and collaborative data governance through partnership and collaboration** between government and other stakeholders that collect, process and use data including PII. Active participation of the private sector, IT technicians, civil society organizations, academia, citizens and other relevant stakeholders is essential for effective and sustainable data governance system.

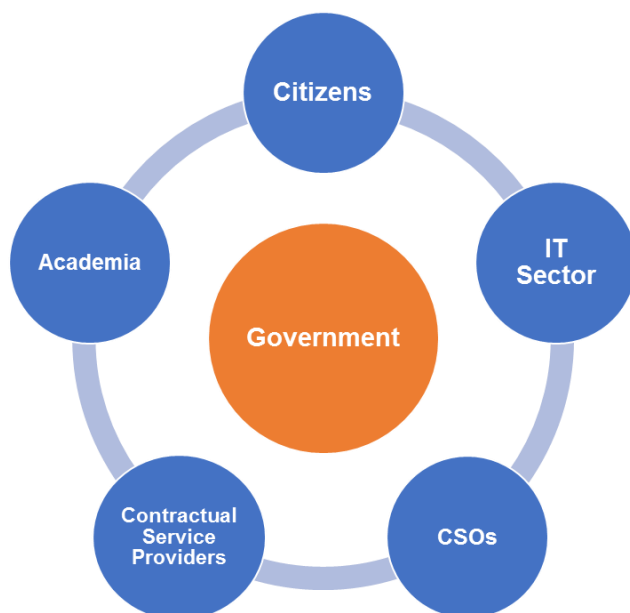
In particular, government needs to take initiatives to raise the awareness of data security and privacy among citizens.

Fourth, it is important to **develop a culture of data security and privacy, particularly increase the awareness among citizens about the detrimental impact of data breaches** and hacking of personal data. Citizens are less consistent in their perception of personal data and may deem medical, financial and civic data highly sensitive and other data such as nationality, gender or age less problematic. So, government should bring in citizens when reviewing and adapting the data governance system.

Fifth, government should **be prudential in outsourcing its digital public services to third parties in the cloud environment** and ensure that the third-party users, including the outsourced parties, comply with the same level of security standards set by the government. In order to maximize the commercial value, third-parties may gain access to databases without the knowing by users' knowledge and share the data with other parties. Also, they may use data without following proper rules and procedures, not fulfilling the data protection responsibilities.

Sixth, it is important for governments to **consider cyber security as part of national security**, due to the fact that a great part of governments system is now based on the networks and data on cyber space. Many developed countries that are also advanced in cyber technologies such as Australia, China and the US even appointed ambassadors for cyber security.

Finally, considering the trans-boundary nature of data and digital services, **an effective data governance also calls for international cooperation**. Protecting cyberspace security particularly needs cooperation between countries.



[Figure10] Multi-Stakeholder Cooperation for Data Governance
(Source: By authors)



References

- 1) Deloitte (2018). A Government Perspective: Tech Trends 2018: The Symphonic Enterprise. Available at: <https://www2.deloitte.com/us/en/pages/public-sector/articles/government-tech-trends.html>
- 2) Department of the Prime Minister and Cabinet, Australian Government (2016). Australia's Cyber Security Strategy. Available at: <https://cybersecuritystrategy.pmc.gov.au/>
- 3) Gartner Top 10 Strategic Technology Trends for 2018. Available at: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/>
- 4) OECD (2018). Embracing Innovation in Government: Global Trends 2018. Available at: <http://www.oecd.org/innovation/innovative-government/embracing-innovation-in-government-2018.pdf>
- 5) Rosenberg, M., Confessore, N., and Cadwalladr, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. The New York Times, 17. Available at: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>
- 6) UK Government Office for Science (2016). Distributed Ledger Technology: Beyond Block Chain. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
- 7) United Nations (2016). 2016 UN E-Government Survey. Available at: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.
- 8) United Nations (2018). 2018 UN E-Government Survey. Available at: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018>.

Keping Yao

Governance and Public Administration Expert

Mi Kyoung Park

Associate Research and Policy Analysis Expert

United Nations Project Office on Governance

Division for Public Institutions and Digital Government

United Nations Department of Economic and Social Affairs