Digital Trade and Data Governance Hub

The George Washington University

DATA INNOVATION AS Data Governance

By Susan Aaronson, Thomas Struett, Carolina Aguerre, and Adam Zable[1]

[1] Aaronson is the Director and Struett is the Research Director at the Hub. Aguerre is a Guest Scholar at the Hub and Senior Research Fellow GCR21 – UDE. Zable is a Koch Hewlett Emerging Tech Policy Leader, working as Research Associate at the Hub. The authors are grateful for research assistance from: Jared Byers, Siaka Togola, and Celeste Travis. Siaka Togola designed the lay-out for this paper and the associated website for this project.

Overview

The Data Governance Mapping Project at the Digital Trade and Data Governance Hub aims to illuminate how countries govern personal, public, and proprietary data at the national and international levels. We found considerable convergence in the hard law governing these various types of data.

This report, our second, examines which countries devised innovative laws and structures for data governance. By focusing on innovation, we can gain a better understanding of what governments are doing, how they are doing it, and why. Our five cases reveal that policymakers are both innovating in data governance and using data governance to achieve other important policy goals.

Table of Contents

INTRODUCTION 4

METHODOLOGY 6

CASE 1: FINLAND PIONEERS IN LAW GOVERNING RE-USE OF HEALTH DATA 9

CASE 2: AMERICA'S AD HOC APPROACH TO DATA PROTECTION AND CYBER-RISK 14

CASE 3: ESTONIA'S INTEGRATED APPROACH TO LINKING DATA GOVERNANCE, DIGITAL RIGHTS, AND DIGITAL ID 21

CASE 4: HOW AUSTRALIA CREATED A CONSUMER RIGHT TO DATA PORTABILITY 26

CASE 5: INDIA WEAVES TOGETHER DOMESTIC REGULATION AND DATA LOCALIZATION TO ATTEMPT TO ACHIEVE DATA SOVEREIGNTY 31

FOOD FOR THOUGHT 38

Introduction

Data is ubiquitous. Firms and governments have a variety of reasons for collecting data, including to create new products, stimulate innovation, solve complex problems, and deliver tailored public services.[2] Given these many different rationales for data collection and analysis, policymakers must find a balance between ensuring an appropriate enabling environment to stimulate data-driven innovation while simultaneously protecting their citizens from direct and indirect data-driven harms. It is important to get that balance right because the imposition of overly broad or onerous barriers to innovation can make a nation less competitive internationally.

The OECD defines data governance as principles, policies, standards, laws, regulations, and agreements designed to control, manage, share, protect, and extract value from various types of data.[3] Data governance is challenging for all nations for several reasons:

- Data's value is derived not by what data is, but by what researchers and firms can do to it to create value. Sometimes researchers and firms create that value by sharing data; other times they can create that value by denying others the ability to utilize that same set of data. Hence, how nations choose to govern data can affect how, when and whether researchers and firms can or cannot succeed at making money from data.[4]

- To appropriate that value, bad actors may hack, steal, or manipulate troves of personal or proprietary data held by firms and governments. Such actions can affect individuals, groups, and national security. Policymakers must clearly delineate specific rules to ensure that the rights of individuals, whether data subjects or creators, are protected while simultaneously clarifying the responsibilities of data collectors to protect data.

- Failure to effectively govern personal data can undermine economic development, and affect human agency, human rights, democracy, and collective self-determination.[5]

---

[2] Gov.uk, National Data Strategy, December 9, 2020. https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

[3] OECD, (2019b). The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies, OECD Publishing, Paris, <https://doi.org/10.1787/059814a7-en>. (19) (PDF) The interdependency of data governance and open government data: lessons from COVID-19. Available from: https://www.researchgate.net/publication/344304476_The_interdependency_of_data_governance_and_open_government_data_lessons_from_COVID-19 [accessed May 30, 2021].

[4] Leonard, Peter G, Is Data Your Most Valuable Asset that You Never Owned? (September 5, 2018). Available at SSRN: https://ssrn.com/abstract=3261221 or http://dx.doi.org/10.2139/ssrn.3261221

[5] Angelina Fisher and Thomas Streinz, Confronting Data Inequality, International Law and Justice Working Papers, 2021/1, pp. 2-6.

Clearly, policymakers must think creatively about how to govern data, particularly personal data. We found that data governance often led to governance innovation for personal data.[6] According to the World Economic Forum, governments that innovate in data governance are agile: they advance adaptive and inclusive strategies that allow all sectors of society to benefit from data while protecting the legitimate interests of all stakeholders. Such policies are trustworthy and accelerate responsible use of data.[7]

[6] Study Group on a New Governance Models in Society5.0, Government of Japan, Governance Innovation, Redesigning law and Innovation for Society 5.0, March 2021, p. 1, https://www.meti.go.jp/press/2020/07/20200713001/20200713001-2.pdf

[7] World Economic Forum, https://widgets.weforum.org/agilegovnavigator/ and https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-data-policy

Methodology

In the first phase of the project, we found significant convergence in data governance among our 52 case study nations.[8] As example, most nations had adopted an approach to personal data governance inspired by or copied from the central tenets of the Europe Union's General Data Protection Regulation.[9] However, in this paper, we tell a story of both divergence and convergence in personal data governance.

We chose our 5 cases because they had a divergent approach to personal data protection (what they did and how they did it). But we found some convergence on motivations (the why). Some governments sought to protect personal data through a patchwork of policies because they lacked an overarching data protection law (US and India). Yet, others sought to use data governance to improve governance in general. These nations adopted new approaches to governance built on data-driven services; hence they needed enhanced data protection authorities (Estonia, Finland, and India). Still others found gaps in their existing approach to data governance and sought to fill those gaps with additional laws, strategies, or policies (Australia, Finland, and US). However, all these governments sought to maintain trust in their approach and simultaneously encourage further economic growth based on data.[10]

"

Personal data governance is essential to building a data-driven economy

The World Bank Group

We did not intend to focus only on personal data, but it is where we found significant innovation in data governance. We believe this is because increasingly governments understand they must protect users' personal data. As the World Bank notes, "personal data governance is essential to building a data-driven economy. Personal data protection can support value creation from data by enabling individuals to benefit from clearer rights and greater agency over their data, while also increasing the transparency and accountability in how data is used. But in light of recent data breaches and incidents of data misuse, citizens are demanding that governments not only create personal data governance rules but update these rules in the face of technological change."[11]

The data giants as well as local firms monetizing data also recognize the importance of maintaining the trust of their consumers, and privacy/personal data protection is essential to maintaining that trust.[12] Finally, protecting data is now a key element of governance in most economies, especially since the pandemic as so much of government and business in many countries has moved online. Consequently, these days protecting personal data is essential to maintaining trust in governance.

National personal data governance regulations delineate the rights of users and the responsibilities of those who collect, store, and

[8] . Alfred D. Chandler Jr. Strategy and Structure: Chapters in the History of the American Industrial Enterprise, (Cambridge: MIT Press, 1962).

[9] The Regulation is at https://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[10] World Economic Forum, 2011. Personal Data: The Emergence of a New Asset Class, January, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

[11] World Bank, Digital Development Partnership, Unraveling Data's Gordian Knot, 2020, pp. 7, 20, https://documents1.worldbank.org/curated/en/863831612427670947/pdf/Unraveling-Data-s-Gordian-Knot-Enablers-and-Safeguards-for-Trusted-Data-Sharing-in-the-New-Economy.pdf

[12] World Economic Forum, Personal Data.

use personal data within their borders.[13] These laws also reassure users that there will be consequences if their data is misused.[14] But since the US first articulated the first set of principles to govern data in the Global Framework for e-commerce in 1997,[15] followed by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[16] policymakers have acknowledged they must also develop bridging mechanisms (interoperable data governance frameworks) to allow personal data to flow between entities in different countries.[17]

In assessing these cases, we built on the work of Harvard Business School historian Alfred D. Chandler who sought to explain how organizations dealt with innovation management. Chandler describes strategy as the determination of long-term objectives and how organizations allocate resources to achieve goals. He defines structure as how the organization is redesigned to administer the new strategy. Hence structure can include both new laws, policies, or plans as well as new organizations erected to achieve the desired strategy.

We proceeded as follows. As we found examples of innovation, we used process tracing to describe how these nations developed their innovative strategy and new structures of governance.[18] Process tracing is a qualitative tool that researchers utilize to establish whether and how a potential cause or causes influenced a specified change or set of changes.

We do not contend that these approaches present a representative sample, but these cases allow us to illuminate how policymakers are incipiently reconceptualizing governance to address the challenges of the data-driven economy.

[13] Estelle Masse, Data protection: why it matters and how to protect it, January 25, 2018, https://www.accessnow.org/data-protection-matters-protect/; and Nuala O'Connor, Reforming the U.S. Approach to Data Protection and Privacy, Digital Cyberspace and Policy Program, https://www.cfr.org/report/reforming-us-approach-data-protection.

[14] https://www.humanrightscareers.com/issues/reasons-why-privacy-rights-are-important/

[15] https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

[16] https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[17] Francesca Casalini and Javier Lopez-Gonzalez Trade and Cross-Border Data Flows, OECD Trade Policy Papers, No. 220,p. 6, OECD Publishing, Paris. http://dx.doi.org/10.1787/b2023a47-en

[18] Alfred D. Chandler Jr. Strategy and Structure: Chapters in the History of the American Industrial Enterprise, (Cambridge: MIT Press, 1962).

Summary Table

Case	What was innovative?	Structural Innovation that resulted	Relationship between data governance and other objectives
Finland and the re-use of health data	Finland built upon baseline legislation like the GDPR and its National Knowledge Society Strategy to advance its vision of a democratic and responsive digital society	New law on data sharing. Innovative new body to provide permits for reuse	Finland used data governance to build trust and move towards knowledge oriented economy
United States and corporate and investment governance	The US uses investment policy and corporate governance rules to protect troves of personal data from national security risk, an indirect regulatory route	Updated defense law that focuses on data-rich firms and their import to national security	US used corporate governance and investment reviews to achieve data governance in the absence of data protection law
Australia and data portability	While Australia was not the first government to enact data portability into law, it used data portability to encourage greater competition among platforms.	New law facilitating data portability	Australia used data governance to encourage greater competition
Estonia and E-Estonia	Estonia created a digital state based on meeting citizens' needs online efficiently and responsively	Three new laws building government services on digital identity	Estonia used data governance to build a responsive accountable state
India data governance and digital sovereignty	Building digital economy and regulatory system based on concept of data sovereignty, but focus is on state control rather than users	Digital identity to provide government services Framework to move to knowledge-based society Draft plans and laws to facilitate data sovereignty	India used data governance to achieve its vision of data sovereignty

The Five Cases

Finland, USA, Estonia, Australia, India

Case 1: Finland Pioneers in Law Governing re-use of Health Data

The EU Digital Economy and Society Index ranked Finland as number 1 in its 2020 ranking. The government set up the Social and Health Data Permit Authority to ensure the ethically sustainable use of data.

Finland

The European Union ranks its member states on their digital performance. In the most recent ranking for 2020, the EU Digital Economy and Society Index ranked Finland as number 1. The Commission noted that Finland's "leading performance" is due to its excellence in digital public services and the integration of digital technologies, enabled by active cooperation between the public and private sectors and an active start-up scene."[19]

As a member of the European Union, Finland follows EU laws and regulations related to personal data, but it has long had its own data governance strategies. In 2006, years before most other nations were thinking about these issues, Finnish officials drafted a National Knowledge Society Strategy for 2007-2015. The Strategy delineated how the country would become a knowledge intensive, "internationally attractive, human-centric, and competitive knowledge and service society." The strategy included 72 recommendations such as revamping copyright, reforming the innovation system, and working internationally. The Finnish officials understood that they must maintain trust if they wanted to promote change. They warned, "if data security and data protection are not handled well, a central element of the information society, trust, is threatened, which can have far-reaching consequences throughout society."[20]

In 2011, government officials tightened their strategy through further consultations

among experts and dialogue with citizens.[21] They proposed a forward-thinking plan that included devising an information infrastructure (including information security, data protection, copyright) and information model (shared concepts and architectures; revising legislation to promote the use of open information and digital content; balancing human rights and the rights of intellectual property holders; ensuring access to personal data contained in public and private information resources and making them available for personal use; assigning responsibility for ensuring the functioning of APIs and standards; and allocating funding to practices and communities that develop and promote the use and integration of data[22] Policymakers also set up a timeline for implementing this plan.[23] The following history delineates how they made this plan a reality.

[19] Finland Digital Economy and Society Index, 2020, 1, 12-13, https://digital-strategy.ec.europa.eu/en/policies/desi-finland

[20] Prime Minister's Office, Finland, "Renewing, human-centric and competitive Finland The National Knowledge Society Strategy 2007–2015," September 2006, 1, 9, 17, https://vnk.fi/documents/10616/622946/R2006_A+Renewing%2C+Human-centric+and+Competitive+Finland.pdf

[21] Ubiquitous Information Society, Advisory Board, Ministry of Transport and Communications Productive and inventive Finland, Digital Agenda for 2011–2020, 2011, p. 8, http://www.lincompany.kz/pdf/Digitaalinen_agenda_eng_fin.pdf

[22] Ubiquitous Information Society, Productive and Inventive, p. 30

[23] Ibid, p. 47.

Finnish officials recognized that Finland must develop legal provisions to facilitate data re-use by researchers and corporations. Government officials decided to try out this idea in the health sector, where "the main challenge for biomedical informatics is to allow for an effective and reliable integration of distributed, complex, and heterogeneous data sources."[24]

Sitra, the Finnish Innovation Fund, played an important role by helping to draft a law and create a new institutional structure to facilitate data re-use. Sitra is an independent public foundation which operates directly under the supervision of the Finnish Parliament to help draft laws and facilitate the permitting process. [25] Building on its suggestions, the Finnish Parliament passed a law in 2019 to create an authority to handle data aggregation and facilitate re-use of anonymous personal data in the health and social sector.[26] The law and the new structures created by Finnish officials were designed to comply with the data protection rights laid out in the EU's General Data Protection Regulation, which governs the use of personal data in the EU. It also aimed "to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data." [27] This law permits re-use of aggregated anonymous data if the re-using entity has a permit from the government. The government argued that this approach would facilitate innovation and development because companies will be able to receive ready-combined aggregated data for these purposes more comprehensively and quickly. [28]

The government set up the Social and Health Data Permit Authority to ensure, as promised in its data strategy, the ethically sustainable use of data.[29] The Authority grants permits for use of health and social data, and it allows data from different data controllers to be gathered and re-used.[30]

[24] S.J. Martin-Sanchez et al. Secondary Use and Analysis of Big Data Collected for Patient Care
Contribution from the IMIA Working Group on Data Mining and Big Data Analytics, yearbook of Medical Informatics, January 1, 2017, https://www.thieme-connect.de/products/ejournals/abstract/10.15265/IY-2017-008

[25] According to Wikipedia, its operations are funded with the profits of its endowment and the profits of its operations. According to law, the funds must be invested securely and in a profitable manner. https://en.wikipedia.org/wiki/SITRA

[26] Heli Parikka, A Finnish Model for the Secure and Effective Use of Data, June 2019, https://www.sitra.fi/en/publications/a-finnish-model-for-the-secure-and-effective-use-of-data/#foreword

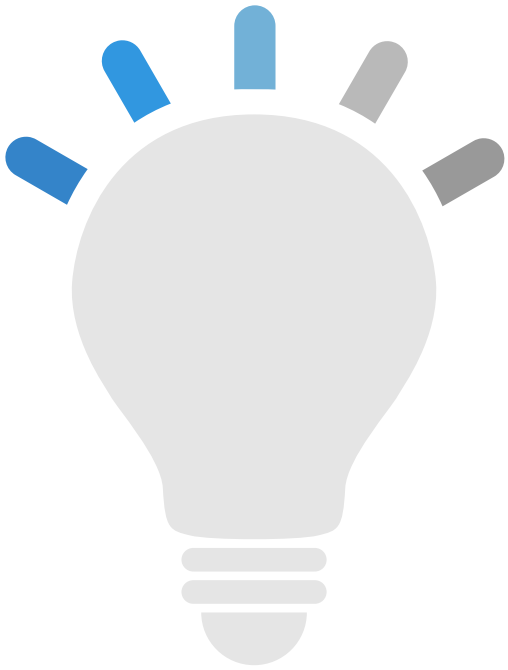
[27] https://stm.fi/en/secondary-use-of-health-and-social-data

[28] Government of Finland, Ministry of Social Affairs and Health Frequently asked questions about the Act on Secondary Use of Health and Social Data
Asset Publisher, https://stm.fi/en/frequently-asked-questions-about-the-act-on-secondary-use-of-health-and-social-data

[29] https://findata.fi/en/

[30] Government of Finland, Ministry of Social Affairs and Health Frequently asked questions about the Act on Secondary Use of Health and Social Data
Asset Publisher, https://stm.fi/en/frequently-asked-questions-about-the-act-on-secondary-use-of-health-and-social-data

In 2021, Sitra reviewed its efforts and wrote, "Finland has succeeded in creating a new ecosystem built around the use of health and well-being data through a national development project culminating in groundbreaking new legislation." But Sitra also noted that it would not have succeeded without the ability to maintain the Finnish peoples' trust. "In general, people in Finland have very high levels of trust in government and this proved to be one of the critical success factors for the new legislation and supportive operating model." Sitra asserted that it had created a venue—a trusted data lake—which could be replicated in other sectors for a trustworthy means of sharing data.[31]

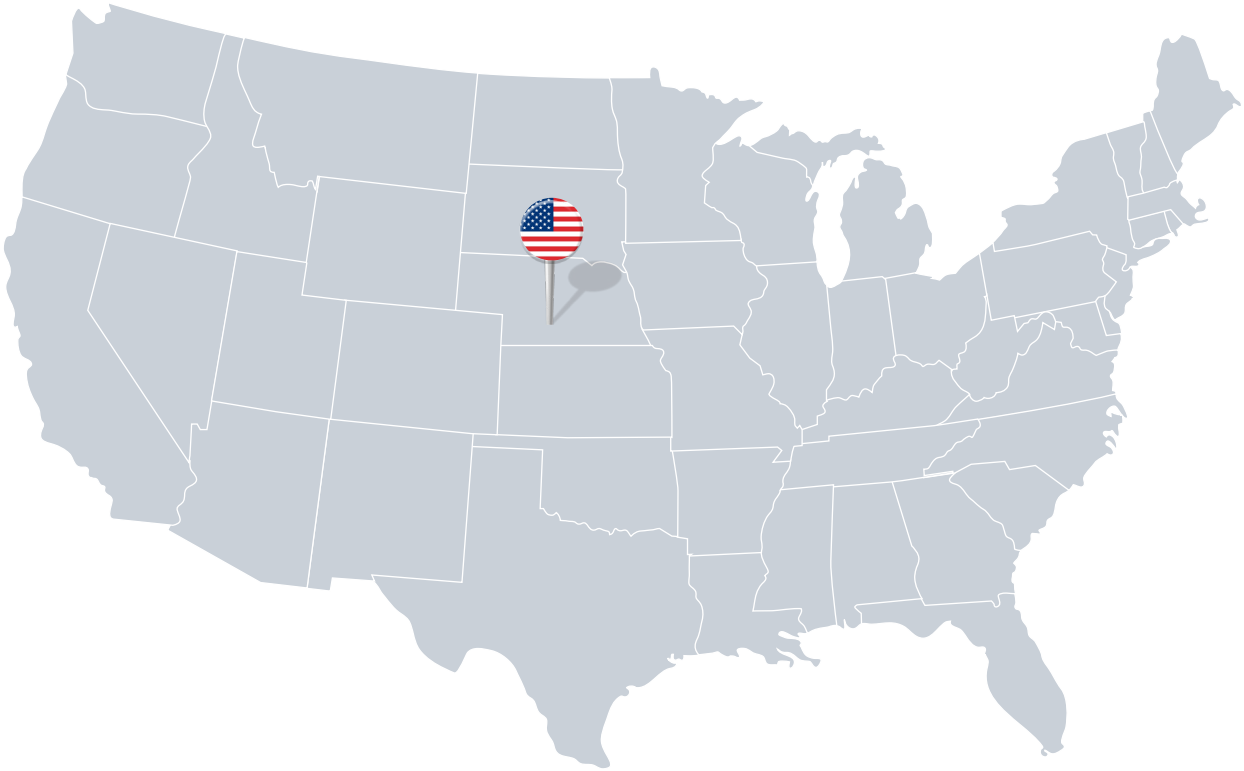


Why is this innovative data governance?

With this new law and permitting body, Finland was able to not only facilitate data re-use, but also move further towards its objectives of becoming a knowledge-based society where data serves the people and is built on trust.

[31] Heli Parikka, A Finnish Model for the Secure and Effective Use of Data, June 2019, https://www.sitra.fi/en/publications/a-finnish-model-for-the-secure-and-effective-use-of-data/#foreword

Case 2: America's Ad Hoc Approach to Data Protection and Cyber-Risk



"Supply chain risk is an essential part of the risk landscape. Organizational policies are often designed to address business risks that arise out of privacy violations, such as reputation or liability risks, rather than focusing on minimizing the risk of harm at an individual or societal level."

NIST, US Department of Commerce

USA

Many of the world's most popular platforms, apps, websites, and social networks are built on aggregated personal data. Moreover, many of these platforms, apps, websites, and networks were "made in the USA" and illuminate America's data prowess.[32] But US citizens do not have the same protections for their personal data as citizens in many other countries. America's failure to effectively govern personal data has led to ad hoc policies at home.

For much of its recent history the US viewed data protection purely as it pertains to consumer regulation, rather than having to do with protecting privacy, freedom of expression, and other human rights.[33] The US government adopted an approach that is legally binding on consumers and firms, but that did not provide individuals with extensive legal data protection rights. Without clear delineation of personal data rights, the US could not establish clear rules for how firms should protect the personal data they collected, stored, or monetized.[34]

The US has several sectoral laws designed to protect consumer privacy, but these laws do not require companies to obtain informed consent to use personal data, nor do they establish a baseline commercial data privacy framework. In February 2012, the Obama White House announced they had created "A Consumer Privacy Bill of Rights" and prodded Congress to develop enforceable privacy policies based on this proposed bill of rights.[35] But that effort failed. Since then, several US states including California and Virginia, have passed personal data protection laws. As of June 2021, Congress has some 30 bills related to privacy and personal data protection on its docket. So far none of them appear likely to become law because policymakers are wrestling with other top priorities.[36]

[32] Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, Which Countries Are Leading the Data Economy?, Harvard Business Review, January 24, 2019. https://hbr.org/2019/01/which-countries-are-leading-the-data-economy

[33] Such as the Electronic Communications Privacy Act (1986), the Children's Online Protection Act (1998) and regulators have issued guidance including the Federal Trade Commission (FTC) Code of Fair
Information Practices Online Report. (The Federal Trade Commission investigates and enforces many of these privacy policies.)

[34] Foley Hoag, Beyond the Privacy Policy: Toward Effective Data Governance, https://www.jdsupra.com/legalnews/beyond-the-privacy-policy-toward-20878/

[35] Susan Ariel Aaronson with Miles D. Townes, Can Trade Policy Set Information Free?
Trade Agreements, Internet Governance, and Internet Freedom, 2014,
https://www2.gwu.edu/~iiep/assets/docs/papers/2014WP/AaronsonIIEPWP20149.pdf and The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012.
https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

[36] Alexandra S. Levine, A U.S. privacy law seemed possible this Congress. Now, prospects are fading fast, Politico, June 1, 2021, https://www.politico.com/news/2021/06/01/washington-plan-protect-american-data-silicon-valley-491405; and Editorial Board, Congress has another chance at privacy legislation. It can't afford to fail again, Washington Post, May 9, 2021, https://www.washingtonpost.com/opinions/congress-has-another-chance-at-privacy-legislation-it-cant-afford-to-fail-again/2021/05/08/9409fa28-af5c-11eb-ab4c-986555a1c511_story.html

As a result of the inability of top lawmakers to come to a consensus on a federal approach to personal data protection, US officials have had to think creatively about how to incentivize organizations to protect personal data. Since the early days of the commercial internet, hackers have tried to exploit holes in security systems to insert malware, viruses, or ransomware or steal or manipulate troves (large stores) of personal and/or proprietary data. As these shackers got better and threats became more complex, individuals and companies developed new tools to protect data and systems (cybersecurity).

In 2003, the US created an agency within the US Department of Homeland Security to address the cybersecurity problem. [37] But in 2013, hackers breached the US Office of Personnel Management (OPM), where they stole personnel records from more than 21 million current and former federal government employees and contractors. [38] Several months later, the US government concluded that China was behind the OPM hack.

US government officials realized that adversaries such as China had strategic reasons for these thefts. These adversaries could combine official data with other data sets. [39] China could then use various analytics techniques to predict, better understand and even manipulate US personnel, policies, and actions. [40]

> Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The US slowly developed a series of strategies to encourage cybersecurity and encourage firms to protect various types of data. In 2013, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. [41] The Order directed an arm of the Department of Commerce, the National Institute for Science and Technology (NIST), to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. [42] Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to

[37] Help Net Security. "The History Of Hacking," April 8, 2002. https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/; CompTIA's Future of Tech. "The History of Cybersecurity." https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/. and Katie Chadd. "The History of Cybersecurity." avast blog, November 24, 2020. https://blog.avast.com/history-of-cybersecurity-avast.

[38] Aliya Sternstein and Jack Moore. "Timeline: What We Know About the OPM Breach." Nextgov.com, June 17, 2015. https://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

[39] Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America." CSO Online, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html, and Stone Fish, Isaac. "China Has Access to Grindr Activity. We Should All Be Worried." Washington Post, April 9, 2019. https://www.washingtonpost.com/opinions/2019/04/09/why-we-cant-leave-grindr-under-chinese-control/.

[40] Garret Graff, 2020. "China's Hacking Spree Will Have a Decades-Long Fallout." Wired, February 11. www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[41] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[42] The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. https://www.nist.gov/about-nist

the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health/safety, or any combination of those matters."[43] The voluntary framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, much of which relies on data and is held in the private sector.[44] The framework is widely used around the world and by US firms.[45]

But this framework did not stop daily cyberattacks, theft, manipulation, and misuse of personal data. The Trump administration decided to focus on one aspect of the problem—the ability of foreign firms to invest in, control, or acquire US data rich firms. In August 2018, Congress passed, and President Trump signed into law, the Foreign Investment Risk Review Modernization Act (FIRRMA), which expanded the scope and authority of the Committee on Foreign Investment in the United States (CFIUS). CFIUS was given jurisdiction over foreign investment transactions that deal with "sensitive personal data of United States citizens that may be exploited in a manner that threatens national security." [46] When considering national security risk, CFIUS must now consider the extent to which a transaction is likely to expose sensitive data of US citizens to exploitation by foreign actors. This new mandate includes foreign investment in new technologies, national security-related infrastructure, and other areas. [47] The law reflected congressional concerns that such transactions could expose personally identifiable information, genetic information, or other sensitive data of U.S. citizens to access and exploitation by an adversary.[48]

In May 2019, former President Trump issued an executive order that found that "the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities… and thereby constitutes an… extraordinary threat to the national security… of the United States." The president then banned such transactions.[49]

After seeking public comments, the Treasury Department issued final regulations that allowed the agency to review transactions where a foreign owned firm could exploit personal data in a manner that threatens US national security.[50] The Treasury developed 10 categories of sensitive data including genetic, biometric, medical, and data pertaining to personal finance, communications, and security clearances.[51]

The US is still tinkering with this approach, while Congress has been unable to pass data protection legislation. On June 9, 2021, the Biden Administration revoked a series of

[43] White House Office of the Press Secretary. "Executive Order -- Improving Critical Infrastructure Cybersecurity," February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[44] NIST. "New to Framework," June 3, 2021. https://www.nist.gov/cyberframework/new-framework

[45] NIST. "Success Stories," June 4, 2020. https://www.nist.gov/cyberframework/success-stories

[46] https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf

[47] Department of Treasury. "Summary of the Foreign Investment Risk Review Modernization Act of 2018" www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf

[48] James K. Jackson and Cathleen D. Cimino-Isaacs. 2020. "CFIUS Reform Under FIRRMA." Congressional Research Service, February 21. https://fas.org/sgp/crs/natsec/IF10952.pdf.

[49] www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[50] https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf.

[51] https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf.

executive orders signed during the Trump administration targeting TikTok, WeChat, and other Chinese apps as national security threats. It replaced them with a new executive order addressing apps linked to foreign adversaries, including China.

The new executive order instructs the Commerce Department to develop criteria for assessing potential national security risks associated with apps that are "owned, controlled, or managed by persons that support foreign adversary military or intelligence activities, or are involved in malicious cyber activities, or involve applications that collect sensitive personal data."[52]

At the same time that the US lacks a comprehensive approach to regulating the use of personal data, the US has not been able to develop a culture (or sufficient technological innovation) to protect personal data held either by firms or governments. Although the US government issued a wide range of guidance to US firms on the import of protecting troves of personal data, firms in the US and around the world continued to experience regular systemic hacks. During the Obama Administration, US policymakers decided they could use corporate governance rules as an incentive to firms (and in particular to boards of directors) by guiding investors. In 2011, the US Securities and Exchange Commission (SEC) issued guidance to publicly held companies on how they should protect personal data. The regulation urged firms to disclose information on risks and events that a reasonable investor would consider important to an investment decision. As example, information about data a firm holds that could give rise to material cybersecurity risks and the potential costs and consequences; cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; risks related to cyber incidents that may remain undetected for an extended period; and what insurance coverage the firm has to cover such costs.[53] However, the regulation did not create sufficient change in boardrooms or among investors. Many firms did not disclose or waited months after cyber-events to disclose.

On February 21, 2018, the Securities and Exchange Commission (SEC) approved interpretive guidance to supplement the regulation, so firms would better understand their obligations and understand that failure to act could result in an enforcement action by the SEC. [54] Thus, in the event of corporate awareness of a data breach, companies are instructed to consider the materiality of cybersecurity risks and incidents and if a breach is found to be a material risk, companies must disclose this information to shareholders and the general public in periodic and current reports.[55]

The SEC created a Cyber Unit to combat cyber-related threats by focusing on, among other things, violations involving distributed ledger technology, cyber intrusions, and hacking to obtain material, nonpublic information. [56] In 2018, the SEC brought its first formal enforcement action of this kind against web

[52] White House, Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, June 9, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/

[53] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[54] EY, Board Matters, "March 2018SEC guidance on cybersecurity: board considerations," https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

[55] SEC, Office of Compliance, Inspections and Examinations, Cybersecurity and Resiliency Observations, pp. 3-10, 13. https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[56] SEC, 2019 Annual Report: Division of Enforcement, pp. 12-13, https://www.sec.gov/files/enforcement-annual-report-2019.pdf and https://www.sec.gov/spotlight/cybersecurity-enforcement-actions

services company Yahoo!. The SEC claimed that Yahoo!,[57] after experiencing the then largest known cyber-intrusion in history, failed to "properly assess the scope, business impact, or legal implications of the breach, including whether, when, and how the breach should have been disclosed." The breach affected user account personal information and Yahoo! agreed to pay $35 million in penalties to settle the action.[58] In 2019, the SEC took a wider range of actions, including against Facebook. It argued that the firm's risk factor disclosures presented the misuse of user data as hypothetical when Facebook knew that user data had in fact been misused. Facebook was ordered to pay a $100 million civil penalty.[59] However, in 2020, the SEC took no enforcement actions against firms for failing to disclose cybersecurity risk.[60] The SEC's lack of action could be a result of a change in priorities, or fewer resources during the pandemic, or perhaps firms actually changed their activities and responses to cybersecurity breaches.

The Limitations of America's Ad Hoc Approach

Given the lack of a unified, federal US law providing for personal data protection, American policymakers had to act creatively to protect large troves of personal data from misuse and to encourage firms to disclose risks to their holdings of personal and proprietary data. Hence, the Trump administration did not directly tackle the national security risk from foreign access or control of big troves of personal data. They did not focus on strengthening personal data protection, developing technical solutions to protect privacy, or devising strategies to ensure that anonymization was effective when data sets are crossed.[61] Moreover, despite its long history of openness to foreign investment, the United States would now carefully review foreign investment in firms with large holdings of data. Lacking a federal regime for data governance, the nation developed a series of rules in corporate governance and investment policy to provide some measure of indirect control. The US ad hoc approach, while innovative, could not fully address the problem of unclear guidance to firms and users about who was responsible for data and how they must protect it when collected and aggregated.

The NIST admits that the ad hoc approach has problems for effective protection and privacy: "All organizations are part of, and dependent upon, product and service supply chains." Data is a key part of that supply chain. Supply chain risk is an essential part of the risk landscape. It is "difficult to assess the effectiveness of an organization's privacy protection methods. Furthermore, organizational policies are often designed to address business risks that arise out of privacy violations, such as reputation or liability risks, rather than focusing on minimizing the risk of harm at an individual or societal level."[62] Hence, NIST was essentially saying that while the current approaches are helpful, they are not mitigating the problem of inadequate personal data protection at the national level.

---

[57] SEC, 2018 Annual Report: Division of Enforcement, Nov. 2, 2018, p. 12, https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

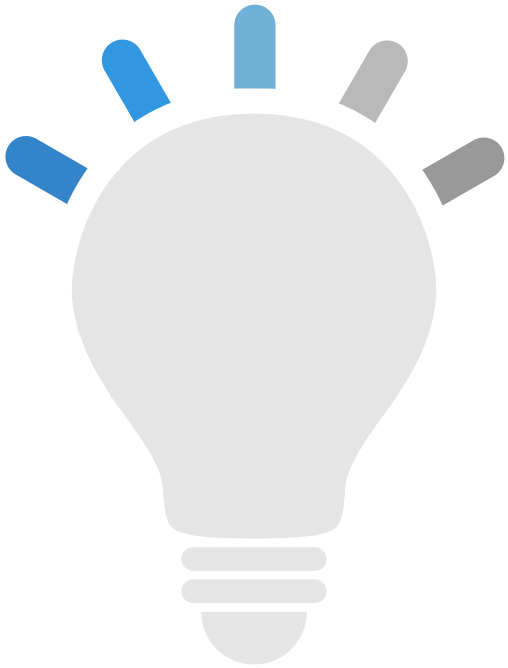
[58] Ibid.

[59] https://www.sec.gov/news/press-release/2019-140

[60] https://www.sec.gov/files/enforcement-annual-report-2020.pdf

[61] Susan Ariel Aaronson, Data is Dangerous: Comparing the Risks the US, Canada and Germany See in Data Troves, CIGI Papers No. 241, April 2020. Since then, the UK government has also enacted a law requiring review of foreign investment in data rich firms. See https://www.legislation.gov.uk/ukpga/2021/25/section/2/enacted; https://www.gov.uk/government/consultations/national-security-and-investment-mandatory-notification-sectors; and https://www.jdsupra.com/legalnews/uk-national-security-and-investment-act-1604883/

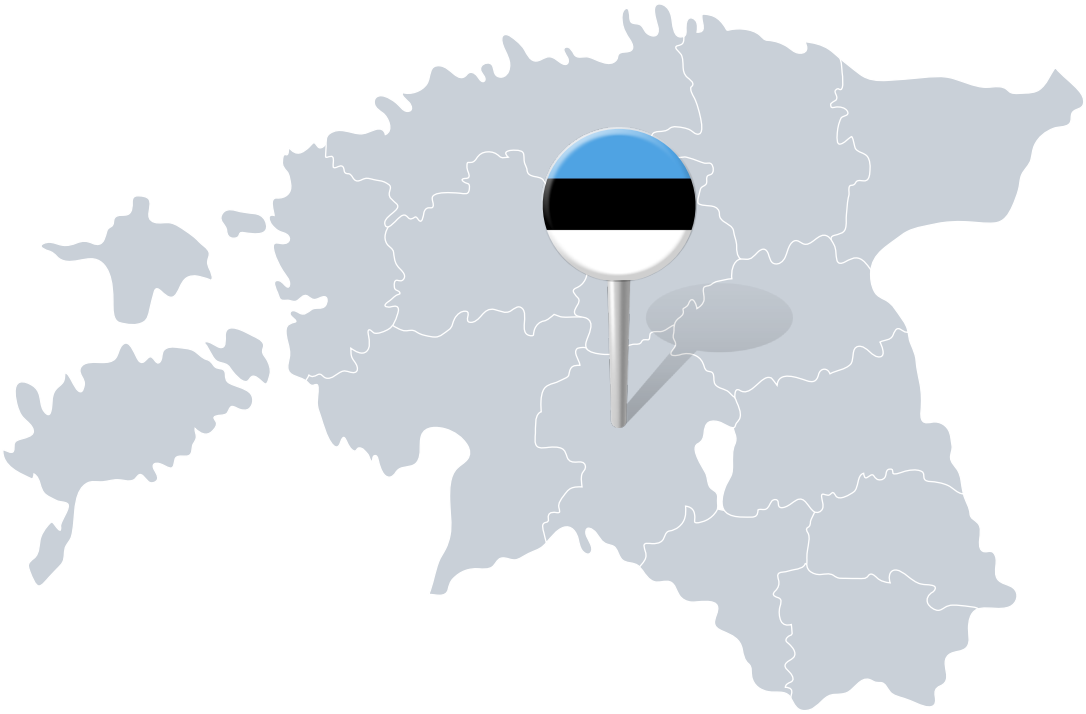
[62] https://www.nist.gov/cyberframework/related-efforts-roadmap



Why is this innovative data governance?

Despite its early transformation into a data driven economy, the US Congress has not approved a unified bill protecting privacy and personal data. Policymakers have had to rely on indirect strategies such as use other policies such as investment reviews and corporate governance rules to protect troves of personal data.

Case 3: Estonia's Integrated Approach to Linking Data Governance, Digital Rights, and Digital ID



The Estonian government claims that the digitization of public services saves in excess of 1,400 years of working time and 2% of its GDP each year. A 2019 survey found that 76% of survey participants said that they felt proud that Estonia is known as one of the most digital societies in the world.

Estonia

After centuries of Danish, Swedish, German, and Russian rule, Estonia attained independence in 1918. But in 1940, it was forcibly incorporated into the USSR. The country did not become independent again until the Soviet Union collapsed some 50 years later.[63] The Estonian people, newly freed from Russian influence, demanded radical change to how the state governed and served its people. Estonian independence provided the people with a rare opportunity to rebuild how society functioned, from the ground up. Some 20 years later, the government of Estonia was considered so innovative that the New Yorker reported that many of its innovative tech leaders wanted to work in government and not in the private sector.[64] The Estonian government proudly declares on its website that many outside observers consider the country the most advanced digital nation.[65]

While the US approach to thinking about how to protect personal data is has tended to be reactive and ad hoc, Estonia developed a coordinated and innovative approach that reflected its history. Estonia's ability to provide responsive digital services is built on three laws enacted in 2000. Although by today's standards their components are nothing new, at the time, and taken together, they represented a radical rethinking of how to establish a society for the digital era. The first new law, the Population Register Act, was designed to "ensure the collection of main personal data of the subjects of the population register in a single database for the performance of functions of the state and local governments provided by law upon the exercise of the rights, freedoms and obligations of persons, and the maintenance of records on the registration

of population."[66] This act set the parameters for how the government could collect and use its citizens' data. Secondly, the Digital Signatures Act delineated how and when citizen and the government could use digital signatures and digital seals, and the procedure for exercising supervision over the provision of certification services and time-stamping services.[67] The law requires that citizens interact with the government through their government established digital ID, built on blockchain technology. Since 2002 about 1.2 million of these credit-card size personal identification documents have been issued.[68]

According to the legislation, a qualified electronic signature is equivalent to a hand-written signature, stamp, or seal and all Estonian authorities are obliged to accept electronic signatures.[69]

Finally, the last of three foundational laws was Estonia's Public Information Act, also passed in 2000. The law was designed to "ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor

[63] https://www.cia.gov/the-world-factbook/countries/estonia/
[64] https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic
[65] https://e-estonia.com/
[66] https://www.riigiteataja.ee/en/eli/516012014003/consolide, Sections 1 and 2.
[67] https://www.riigiteataja.ee/en/eli/530102013080/consolide
[68] Kristjan Vassil. Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, Report for the World Development Report 2016, Digital Dividends, 2016, https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf
[69] PWC, Estonia, the Digital Republic Secured by Blockchain, p3.https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

the performance of public duties." This Act also delineates when public information can be reused as well as the basis for refusal to grant access to information; and forbade the government from establishing separate databases for the collection of the same data.[70]

The law (in concert with the two other laws) is innovative because it was based on the notion that the government could create efficiencies by facilitating the re-use of personal and business data held by the government. As example, Estonian citizens do not have to "prepare" a loan application; applicants have their relevant data— income, debt, savings— pulled from elsewhere in the system and aggregated.[71]

The Estonian government claims that this digitization of public services saves more than 1,400 years of working time and 2% of its GDP each year.[72] One can see this process on the government public service portal.[73] Voting provides a good example of how the system works. Citizens download a voting application to their computer and upon a request from the system identify themselves using the ID-card and the first pin-code so that the voting system knows who is behind the computer. "Next, the system checks whether the voter is eligible to vote in these elections and if affirmative, displays a list of candidates. This is the part of the service that uses the authentication functionality of the digital ID-card and allows eligible voters to browse between political candidates. No digital signature is required thus far. However, in order to cast an e-vote, the citizens must provide a second pin-code–the signing function will be used to confirm voter's choice. The latter is a transactional part of the citizen-state communication. When inserted correctly, the electronic vote is sent to the server and will be counted."[74]

Taken in sum, Estonia developed an approach to data governance that allowed the government to:

1. be responsive, efficient, and open as a result of changes to its laws and institutional structure.
2. provide the bulk of government services entirely online.

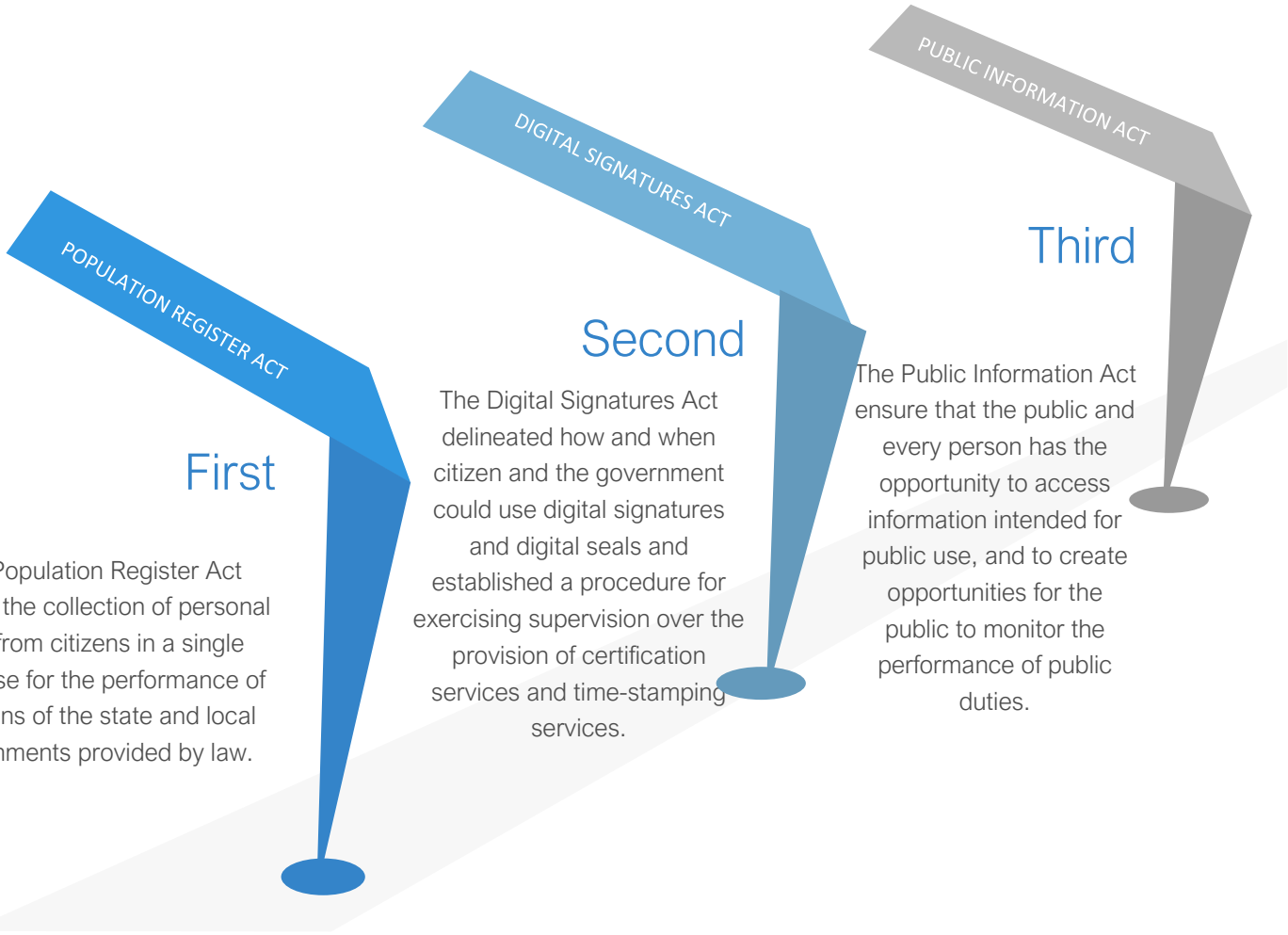
Building on that demand, policymakers thought coherently, creating "an intertwined ecosystem" of institutional, legal, and technological frameworks built on data.[75] Outside observers view the nation's approach to governance as both innovative and robust. In 2020, the Bertelsmann Transformation Index, which assesses quality of governance, ranked the country number 1 of 137 nations for governance.[76]

Polling data reveals that the Estonian people trust in the system. The government reported that 82% of respondents surveyed in 2019 said that they trusted the digital services provided by the Estonian government. Some 76% of survey participants said that they felt proud that Estonia is known as one of the most digital societies in the world.[76]

[70] https://www.riigiteataja.ee/en/eli/522122014002/consolide
[71] Kristjan Vassil, Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, Report for the World Development Report 2016, Digital Dividends, 2016,June, https://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf
[72] PWC, Estonia, the Digital Republic Secured by Blockchain, p3. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf
[73] https://www.eesti.ee/en/
[74] Vassil, p. 4, 22-28.
[75] Vassil, p.29.
[76] Florian Marcus, How Do you Build Trust in Government? E-Estonia, August 2020, https://e-estonia.com/building-trust-in-government/

RESPONSIVE DIGITAL SERVICES

BUILT ON THREE LAWS



First

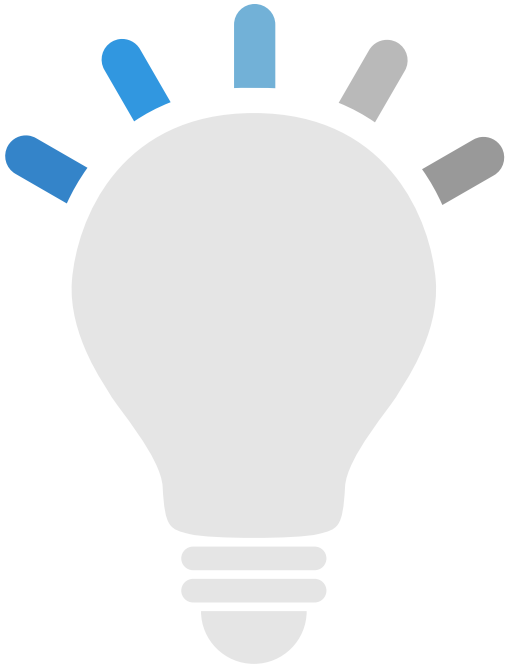
The Population Register Act allowed the collection of personal data from citizens in a single database for the performance of functions of the state and local governments provided by law.

Second

The Digital Signatures Act delineated how and when citizen and the government could use digital signatures and digital seals and established a procedure for exercising supervision over the provision of certification services and time-stamping services.

Third

The Public Information Act ensure that the public and every person has the opportunity to access information intended for public use, and to create opportunities for the public to monitor the performance of public duties.



Why is this innovative data governance?

Estonia used data governance to build trust in data and to make governance both responsive and efficient.

Case 4: How Australia created a consumer right to Data Portability

The Australian data-driven sector is estimated to contribute some 7% of Australia's GDP. The Australian government believes that a comprehensive right to data portability “may offer the capacity to underpin a new wave of competition policy."

Australia

has a booming digital economy. The data-driven sector is estimated to contribute some 7% of Australia's GDP.[77] The government played a leading role in facilitating that growth. In 2011, the Australian government put forward a National Digital Economy Strategy, which committed the government "to ensuring that by 2020… Australia is one of the world's leading digital economies." Australia seems well on its way, ranking highly in digital economy metrics.[78]

Australia recognized early on that data governance would be a key element for digital success and that competition policy reform would be needed for Australian firms to compete both nationally and globally.

2001 — The Australian government put forward a National Digital Economy Strategy.

2014 — The Australian government tasked the Productivity Commission to review the benefits and costs of increasing the availability and improving the use of data.

The government asked for a review of Australia's approach to competition policies.

2017 — Australia approved legislation creating the Consumer Data Right to give consumers greater control and choice over their data between services.

[77] Deloitte Access Economics and the Australian Computer Society, Australia's Digital Pulse 2015, https://www2.deloitte.com/au/en/pages/economics/articles/australias-digital-pulse.html, Deloitte Access Economics and the Australian Computer Society, Australia's Digital Pulse 2021, pp. 5-6, https://www2.deloitte.com/au/en/pages/economics/articles/australias-digital-pulse.html

[78] Chakravorti, Bhalla, and Chaturvedi, https://hbr.org/2019/01/which-countries-are-leading-the-data-economy and Joshua P. Meltzer, GLOBAL ECONOMY & DEVELOPMENT WORKING PAPER 118 | MAY 2018, pp. 10-11,

In 2014, the government asked an outsider, Professor Ian Harpur, to review Australia's approach to competition policies. The report recommended that the government establish new policies to facilitate competition, counter anti-competitive practices, and create a new body called the Australian Council for Competition Policy to advocate and drive reform and perform reviews of policy.[79]

Meanwhile, that same year, the Australian government tasked the Productivity Commission to review the benefits and costs of increasing the availability and improving the use of data. The Productivity Commission[80] in turn recommended that the government consider ways to improve individuals' ability to access their own data to inform consumer choices. The report lays out the fundamental aspects of what became the Consumer Data Right (CDR) while arguing that "[i]n an era where data collection and use is becoming ubiquitous, it seems counterintuitive that consumers cannot easily benefit from data about themselves." [81] The report suggested that a comprehensive right to data portability "may offer the capacity to underpin a new wave of competition policy."[82]

Building on its analysis, the Productivity Commission argued that the government should adopt a sectoral approach to ensure usability of data and to manage risks in data portability.[83] A sectoral approach would reflect different data uses and competition differences among sectors and could encourage greater participation among firms, consumers, and other market participants. [84] The Commission also recognized it needed to go beyond the European General Data Protection Regulation, which simply requires firms to make personal data portable in a structured and machine-readable format. [85] It needed a standardized approach that could be used by any firm in the sector.[86]

In 2017, Australia approved legislation creating the Consumer Data Right to give consumers greater control and choice over their data between services. [87] The CDR is innovative because it takes a sectoral approach to governing data portability by slowly rolling out the right to different sectors.[88] The CDR is also innovative in that it is meant to only focus on consumer data. The government consults with its constituents to define what they mean by consumer data for each sector. This process is meant to build trust and recognize sectoral differences.[89]

---

[79] Harper review: The key recommendations, Sydney Morning Herald, March 25, 2015, https://www.smh.com.au/politics/federal/harper-review-the-key-recommendations-20150331-1mc1x2.html

[80] The Productivity Commission is the Australian Government's independent research and advisory body on a range of economic, social and environmental issues affecting the welfare of Australians. https://www.pc.gov.au/about

[81] Productivity Commission. Data Availability and Use: Productivity Commission Inquiry Report No. 82, 31 March 2017., 2017. https://nla.gov.au/nla.obj-2821073955. P. 174

[82] Productivity Commission. Data Availability and Use: Productivity Commission Inquiry Report No. 82, 31 March 2017., 2017. https://nla.gov.au/nla.obj-2821073955. P. 191

[83] Productivity Commission. Data Availability and Use: Productivity Commission Inquiry Report No. 82, 31 March 2017., 2017. https://nla.gov.au/nla.obj-2821073955. p. 221

[84] Productivity Commission. Data Availability and Use: Productivity Commission Inquiry Report No. 82, 31 March 2017., 2017. https://nla.gov.au/nla.obj-2821073955. Pp. 204 and 210

[85] Article 20, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[86] OECD. "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies." Accessed June 4, 2021. https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

[87] https://www.cdr.gov.au/what-is-cdr

[88] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

[89] https://www.legislation.gov.au/Details/F2019L01153/Explanatory%20Statement/Text

The process works as follows. Individuals opt-in to a service that utilizes application programming interfaces (APIs) to share a consumer's data between accredited institutions within a specific sector, like banking.[90] Providers of services in each sector go through an accreditation process that then allows them to transfer consumer data between providers. [91] As of 2021, the government has set up this process in the banking sector and plans to expand it next to the energy and telecommunications sectors.[92]

The CDR is regulated by the Australian Competition and Consumer Commission (ACCC) while the Australian Data Standards Body (DSB) is tasked with creating the technical standards for the data sharing and the Office of the Australian Information Commissioner (OIAC) monitors compliance.[93]

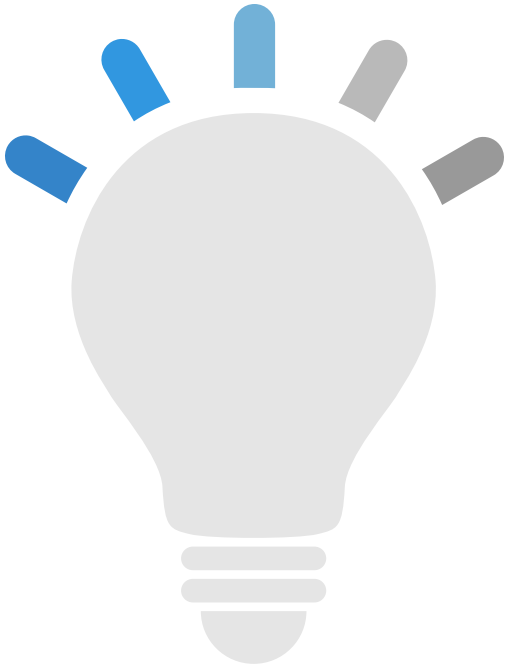
In sum, Australia innovated by finding a new approach to personal data protection that bridges consumer protection and competition policy. By giving users a means of ownership and control, Australia facilitated a more competitive market for data. According to Australian legal scholar Peter Leonard, "many countries confer significant rights upon data subjects to control how data about them is used and disclosed… A right to take personal data elsewhere has some attributes of an ownership right."[94] Leonard is referring to the notion that by giving individuals the right under law to take their data from a service and transfer or "port" it elsewhere, individuals are ostensibly asserting some ownership and control over their data.[95]

Neither the Australian Constitution nor existing human rights law delineates such a right. However, as Leonard notes, a right to data portability could serve "as a lever for competition between service providers in industry sectors where complexity of data impedes product comparisons and switching between service providers."[96]

As the US internet activist group EFF notes, on its own, data portability cannot magically improve competition, create viable competitors, or fend off data oligopolies. But it can facilitate users' power over these platforms.[97]

The Australian Government expects that "the Consumer Data Right will lead to new and innovative products and services as consumer data becomes more widely available throughout the economy. It will also increase competition in the marketplace. This means there will be more products and services for you to choose from."[98]

[90] https://www.cdr.gov.au/how-it-works
[91] https://www.cdr.gov.au/what-is-cdr
[92] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0
[93] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0
[94] Leonard, "Is Data your most?" p. 3.
[95] Gennie Gebhart, Bennett Cyphers, and Kurt Opsahl, What we mean when we Say "Data Portability", September 13, 2018, https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability
[96] Leonard, Is Data your Most? pp 3-4.



Why is this Innovative data governance?

While Australia was not the first government to enact data portability into law, it used data portability to bridge competition policy, personal data protection, and consumer regulation.

Case 5: India weaves together domestic regulation and data localization to attempt to achieve data sovereignty

India is one of the largest and fastest-growing markets for digital consumers, with 560 million internet subscribers in 2018. India's data governance is guided by a vision that the Indian government has sovereignty over the data generated by its citizens within its borders.

India is one of the largest and fastest-growing markets for digital consumers, with 560 million internet subscribers in 2018 (second only to China).[97] Government officials have carefully planned India's data driven growth. On July 1, 2015, Prime Minister Narendra Modi launched the Digital India Programme. The Programme aims to transform India into a digitally empowered knowledge economy by providing a digital infrastructure that the government should provide and regulate and by using technology to transform public services.[98]

A 2019 McKinsey study of India's digitalization found that the public and private sectors are both propelling digital consumption growth. "The government has enrolled more than 1.2 billion Indians in Aadhaar, its biometric digital identity programme, and "brought more than 10 million businesses onto a common digital platform through a goods and services tax." Meanwhile telecommunications firms have "turbocharged internet subscriptions and data consumption, which quadrupled in both 2017 and 2018 and helped bridge a digital divide."[99]

But India's data governance may hobble its digital progress. India's data governance is guided by two philosophies: 'data sovereignty', which posits that the Indian government has sovereignty over the data generated by its citizens within its borders," and a vision of 'data colonialism',[100] that the big platforms seek to extract data from developing county citizens and use it to control the internet.[101]

While big firms are certainly taking advantage of the personal data of Indians, the data giants use the same business model of extracting data in developing countries as they do in high income countries. However, high income nations have an advantage in this situation. Nations such as Australia or the UK may be more experienced at data governance and better placed to supplement it with tax or competition policies to challenge the business models of these firms. Hence, data sovereignty gives Indian officials a justification for protecting the data of the Indian people.

---

[97] McKinsey Global Institute, Digital India: Technology to transform a connected nation, McKinsey, 2019, . https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.pdf

[98] https://www.digitalindia.gov.in/content/introduction; https://www.digitalindia.gov.in/content/vision-and-vision-areas

[99] McKinsey Global Institute, Digital India: p. 8. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/digital-india-technology-to-transform-a-connected-nation-full-report.pdf

[100] Nilma Elmi, Is Big Tech Setting Africa Back?, Foreign Affairs, November 11, 2020, https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/

[101] Vindu Goel, India Pushes Back Against Tech Colonialism by Internet giants, The New York Times, August 31, 2018, https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html

However, critics of India's approach argue that while Indian officials claim that they are protecting Indian users, India's approach may undermine the human rights of its citizens. Thus far, India has not clarified what information belongs to the individual and what to the state. Without such clarification, Indians' personal data could be seen as a sovereign asset of the state rather than accruing to individuals.[102] Moreover, critics also argue that by treating data as a sovereign asset, India cannot develop a rights-based approach to personal data protection.[103]

India, like the US, lacks a clear data protection law, although Indian civil society groups, firms and officials have been trying to govern personal data since 2000. In the absence of clear law, Indian policies have vacillated.[104] Hence, while Indian officials have a clear vision of how data should be governed, they have not evolved a consistent strategy or effective policy framework. India has however made progress in data sovereignty by weaving domestic regulation and data localization.

India has long planned to leverage data to develop by means of two tactics. At home, India has developed policies to regulate the practices of multinationals, while at the same time it has worked internationally to slow the adoption of rules governing cross-border data flows at the WTO and regionally.[105] At the WTO, India and South Africa argued that developing countries need trade rules requiring special and differential treatment. They also demanded the ability to utilize customs duties to finance digital development if they are to build data-driven economies.[106] Consequently, India refuses to negotiate digital trade at the WTO until it has clarified its own data governance rules.[107] In 2019, India's information technology and telecom minister Ravi Shankar Prasad said that Indian data sovereignty is "non-negotiable." He acknowledged that while a degree of data circulation is important in a digital world, it must be based upon reciprocity and understanding."[108]

India first outlined minimal data protection rules in its basic e-commerce law. The Information Technology Act of 2000[109] contains a number of provisions that can, in some cases, safeguard online privacy, including penalizing child pornography hacking and fraud. However, the Act does not address issues covered in

[102] Centre for Internet and Society, "Internet Privacy in India, ND, https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india

[103] Jyoti Panday, Tracking India's Approach to Data Governance: From Localization to Stewardship of Data, February 9, 2021, https://www.internetgovernance.org/2021/02/09/tracking-indias-approach-to-data-governance-from-localization-to-stewardship-of-data/ and Anja Kovacs and Nayantara Ranganathan . Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India. Data Governance Network Working Paper 03, https://datagovernance.org/files/research/IDP_-_Data_sovereignty_-_Paper_3.pdf

[104] Kovacs and Ranganathan . Data sovereignty, of whom?

[105] Arindrajit Basu, Sovereignty in a 'datafied' world: A framework for Indian diplomacy, Observer Research Foundation, https://www.orfonline.org/expert-speak/sovereignty-datafied-world-framework-indian-diplomacy/#_ednref27

[106] Susan Ariel Aaronson and Thomas Struett, Data Is Divisive: A History of Public Communications on E-commerce, 1998–2020, CIGI Paper No. 247, https://www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020/. See TO, Work Programme on Electronic Commerce, The E-Commerce Moratorium: Scope and Impact, Communication from India and South Africa, WTO Doc WT/GC/W/798, online: WTO <docs.wto.org> [Scope and Impact]

[107] Susan Ariel Aaronson and Thomas Struett, Data Is Divisive: A History of Public Communications on E-commerce, 1998–2020, CIGI Paper No. 247, https://www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020/. See TO, Work Programme on Electronic Commerce, The E-Commerce Moratorium: Scope and Impact, Communication from India and South Africa, WTO Doc WT/GC/W/798, online: WTO <docs.wto.org> [Scope and Impact]

[108] NA, India will allow data mobility only if reciprocated: Ravi Shankar Prasad, The Economic Times, June 15, 2019, https://economictimes.indiatimes.com/tech/internet/india-will-allow-data-mobility-only-if-reciprocated-ravi-shankar-prasad/articleshow/69796915.cms

[109] https://www.meity.gov.in/content/information-technology-act-2000

broader general data protection laws such as data portability, or if users have the right to be notified of the presence of cookies and do-not track options. The act has been amended several times.[110] However, according to the Centre for Internet and Society in India, business, government and civil society pushed for clarification and in 2011 the Ministry of Communications and Information Technology issued regulation outlining such rules.[111] These rules define 'sensitive personal information' and require that any corporate body must publish an online privacy policy, provide individuals with the right to access and correct their information, obtain consent before disclosing sensitive personal information except in the case of law enforcement, provide individuals the ability to withdraw consent, establish a grievance officer, require companies to ensure equivalent levels of protection when transferring information, and put in place reasonable security practices. The rules apply only to private firms and not to the government and cover only some types of sensitive personal information. Finally, no one knows if companies are really adhering to these rules.[112]

Policymakers and activists kept trying to clarify the responsibilities of firms and the government regarding personal data protection. In 2017, India's Supreme Court ruled that under the Constitution, Indians have a fundamental right to privacy.[113] In July 2018, India's Ministry of Electronics & Information Technology released an initial version of its Draft Personal Data Protection Bill. The objective was to develop legislation to "ensure growth of the digital economy while keeping personal data of citizens secure and protected."[114] After extensive public comment, the Indian Parliament prepared the first iteration of the 2019 Personal Data Protection Bill.[115] The bill merged India's desire for data sovereignty with provisions for data localization, requiring certain types of data be stored in local servers. The bill has not yet been approved by Parliament and it has been revised several times.[116] The current draft of the Bill prescribes compliance requirements for all forms of personal data, broadens the rights given to individuals, introduces a central data protection regulator, and institutes data localization requirements for certain forms of sensitive data. The Bill applies extra territorially to non-Indian organizations in the event that certain nexus requirements are met, and also imposes hefty financial penalties in case of non-compliance.[117] These provisions have led to international concerns about protectionism, but in August 2019, the law and technology minister Prasad noted that India would not compromise on data sovereignty.[118] Nonetheless, foreign companies and human rights activists continued to worry that the law does not clarify whether government can

[110] https://www.meity.gov.in/content/notifications

[111] Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[112] https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india#fn8

[113] Privacy International, 1.3 Billion People's Right To Privacy Upheld Following Historic Judgement By India's Supreme Court, December 1, 2017, https://privacyinternational.org/blog/768/13-billion-peoples-right-privacy-upheld-following-historic-judgement-indias-supreme-court

[114] https://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited

[115] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[116] NA, "India will Allow," 2019. https://economictimes.indiatimes.com/tech/internet/india-will-allow-data-mobility-only-if-reciprocated-ravi-shankar-prasad/articleshow/69796915.cms

[117] NA, Privacy and Data Protection – India Wrap 2020, The National Law Review, January 15, 2021, https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020

[118] NA, PM Modi won't compromise on data sovereignty' The Times of India, August 29, 2019, https://timesofindia.indiatimes.com/business/india-business/pm-wont-compromise-on-data-sovereignty/articleshow/70812638.cms

control and utilize personal data without the direct consent of citizens.[119]

Foreign companies have viewed much of India's approach to digitalization and data governance as protectionist and unfair. First, many foreign firms are already subject to data localization. In April 2018, the Reserve Bank of India issued a directive to all companies to store data related to payments systems in India.[120] Since then there have been eight sectoral notifications mandating data localization in some form, including in sectors like insurance, healthcare, and e-commerce.[121] These remain in force.[122] These provisions allow the state to obtain greater control of personal data which could be problematic for Indian citizens. In addition, India banned 59 Chinese mobile apps in June 2020, taking a cue from the US. However, India asked the companies creating the apps to explain whether they censored content, worked on behalf of foreign governments or lobbied influencers. The bans remained in place in January 2021.[123]

Meanwhile, some Indians argue that other nations/trade blocs are also using data sovereignty to ensure that their companies and people flourish with data.[124] They cite as example, the GAIA X project (the European plans for a single European cloud).[125] They maintain that "more data located and harnessed in India equals higher levels of economic growth"[126] However, other Indians argue data protectionism will reduce foreign investment. "Rising protectionism, arbitrary taxation, and excessive regulation that target foreign investment do not project the image of an India that is open and welcoming. These factors could limit India's potential and hinder growth."[127]

India has made data sovereignty a key rationale for data protection. In February 2019, the Government of India released the Draft National E-Commerce Policy. It stated, "it is important to protect data, prevent its misuse, regulate the use and processing of data, and address the concerns related to privacy and security. The policy recognizes the importance of data while enabling the domestic industry to benefit from the advantages and opportunities created by electronic commerce."[128] Firms from Amazon to Walmart viewed the potential approach as discriminatory and unfair. They argued it could stimulate disinvestment or less investment and could undermine India's plans for digital led growth.[129] Some of these firms also argued that their business models were overregulated in India. In 2018, the Ministry of

[119] Manasi Gopalakrishnan, India's personal data privacy law triggers surveillance fears, Deutsche Welle, November 11, 2020, https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949

[120] https://src.bna.com/D5n?_ga=2.123343947.1131408265.1575749815-1922557974.1575749815

[121] https://www.lawfareblog.com/indias-role-global-cyber-policy-formulation

[122] Arindrajit Basu, The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam, The Diplomat, January 10, 20210, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/

[123] https://www.reuters.com/article/us-india-china-apps/india-retains-ban-on-59-chinese-apps-including-tiktok-idUSKBN29U2GJ

[124] Rudra Chaudhuri, the era of data-globalism is over. Where does this leave India? December 4, 2019, https://theprint.in/opinion/the-era-of-data-globalism-is-over-where-does-this-leave-india/329687/

[125] https://ec.europa.eu/digital-single-market/en/european-cloud-initiative

[126] Chaudhuri, The Era,"

[127] Aparna Pande, India's Protectionism Might Hinder Its Economic Growth — and Affect Global Partnerships, The Diplomat, November 4, 2020, https://thediplomat.com/2020/11/indias-protectionism-might-hinder-its-economic-growth-and-affect-global-partnerships/

[128] Draft National E-Commerce Policy India's Data for India's Development, p8, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

[129] https://www.businesstoday.in/current/corporate/india-s-e-commerce-rules-regressive-not-good-for-global-business-walmart-to-us-government/story/363708.html; https://www.business-standard.com/article/companies/dpiit-meet-foreign-vs-indian-war-of-words-over-e-commerce-fdi-policy-121032501465_1.html

Electronics and Information Technology demanded that WhatsApp create a way to track and stop mass messages, such as a series of false items about child kidnappers that led to the murder of two dozen innocent people by angry mobs. After the company refused, saying that building such technology would break the encryption that keeps messages private, Indian officials said the company was not complying with local law and delayed approval of a new payments service from WhatsApp until it complies with local laws, including a new rule that requires Indian financial data be stored only in India[130]

In 2021, the Ministry issued a revised draft of the e-commerce strategy, which was supposed to curb alleged circumvention of foreign direct investment (FDI) norms and anti-competitive activities by foreign tech platforms. The draft, which has not been released publicly, supposedly clears up some of the confusion the previous draft had created over data sharing and consumer protection. Allegedly, the data localization provisions remain in the e-commerce policy. [131] Moreover, the draft supposedly states that "E-commerce operators shall ensure that algorithms used are not biased and that no discrimination due to digitally induced biases is prevalent,"[132]

The e-commerce policy proposed a separate class of data called “community data". Although the country innovated in defining this class, it remains unclear whether community data belongs to the country, the community, and/or the people whose data are aggregated to make it a community. [133] There is also uncertainty regarding what kind of groups can form a ‘community.’ In short, it did not clarify data protection rules for various communities.

But in July 2020, a government expert committee released a report on a Non-Personal Data (NPD) governance framework for India.[134] This framework aimed “to tap into data as an economic asset, incentivize start-ups by correcting the imbalance established by a few dominant players and use data for public good and economic benefits of citizens while protecting collective community interests over such data.”[135] The government asked for public comment and received and incorporated many of the comments into a new draft published by the government in December 2020.[136]

The new draft builds on the notion of community data first delineated in the 2019 draft e-commerce strategy.[137] It is designed to give some control and ownership rights over data to communities and mandates that such data be stored locally. However, critics argue that it “risk[s] eviscerating competition and innovation in India to the detriment of Indian consumers, undermining consumer privacy, spurring mistrust of companies and the government, and fostering a regulatory regime that is unclear, overly burdensome, and lacks nuance, all outcomes that are starkly opposed to the report’s noble intentions.” [138] Many

[130] Vindu Goel, India Pushes Back. https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html

[131] https://economictimes.indiatimes.com/tech/tech-bytes/indias-new-draft-e-commerce-policy-to-rein-in-related-parties/articleshow/81502310.cms?from=mdr

[132] Priyanka Sahav, Explained: India's new draft e-commerce policy and how it will impact the e-tail space, MoneyControl, March 16, 2021, https://www.moneycontrol.com/news/business/explained-indias-new-draft-e-commerce-policy-6648901.html

[133] Nayantara Ranganathan, The Seduction of Data Sovereignty in India, Hindustan Times, August 26, 2019, https://www.hindustantimes.com/analysis/the-seduction-of-data-sovereignty-in-india/story-iOS8cVKxstIIgJLy47Iy0J.html

[134] https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

[135] https://www.financialexpress.com/opinion/can-we-have-one-data-policy-for-india/2218836/

[136] https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

[137] https://www.thehindubusinessline.com/opinion/for-a-robust-data-protection-regime/article34551998.ece

[138] https://www.medianama.com/2020/07/223-five-key-concerns-with-indias-non-personal-data-report/,

stakeholders are also saying that it is premature to set out a regulation for non-personal data before citizens are given a baseline privacy right with an adoption of the PDP.[139]

Taken in sum, India has articulated a clear vision for data governance built on its desire to empower Indians through digital sovereignty. But its plans may make it harder to achieve trusted personal data governance.[140] India has adopted several regulations that appear to favor domestic providers and discriminate among foreign providers of data driven services. At the same time, India has also refused to negotiate international rules on data until it has clarified its domestic rules. Yet data governance in India is a work in progress: India lacks a data protection law, e-commerce policy, and clear rules to govern cross-border data flows.

Foreign investors and citizens alike see contradictions in India's approach. They note India has addressed personal data protection for firms but not for the government and note that data localization and other regulatory policies could impede investment and digital progress. Nonetheless, by issuing drafts of these policies, frameworks, laws and strategies, India has ignited a broad debate among domestic and foreign market actors about how personal and non-personal data should be regulated by a developing country.

Why is this innovative data governance?

India used plans for data protection, ecommerce, and data-driven development to further its goal of data sovereignty.

[139] https://indianexpress.com/article/business/non-personal-data-framework-premature-startups-tech-groups-to-govt-committee-6596268/, https://www.financialexpress.com/opinion/non-personal-data-norms-too-much-too-soon/2183383/, https://www.medianama.com/2021/02/223-india-revised-personal-data-report-shortcomings, https://www.internetgovernance.org/2021/02/09/tracking-indias-approach-to-data-governance-from-localization-to-stewardship-of-data/

[140] Divij Joshi, Interrogating India's quest for data sovereignty, Seminar Magazine, July 31, 2020, https://www.india-seminar.com/2020/731/731_divij_joshi.htm

Food For Thought

Herein, we delineated how nations are innovating in various aspect of personal data governance. We chose our 5 cases because they had a divergent approach to personal data protection. While the cases differed in what and how they innovated, we found some convergence on motivations (the why).

In thinking about data governance, we note that nations have not only evolved different approaches to personal data governance, but they also have different definitions of personal data as it is transformed into input for data driven services. Some have set up a dialectic where data can be divided into personal and non-personal data, whereas others have created additional categories of data types. We also note that when firms use proprietary processes (such as algorithms) to transform aggregated personal data, that data becomes proprietary and is controlled by the firm. We will closely monitor how nations define and develop policies to govern personal, non-personal, proprietary, and aggregated personal data.

FOOD FOR THOUGHT