6

Data Flows as Digital Trade

Privacy and Cybersecurity Governance in a Datafied World

6.1 Introduction

At a time when the global economy has become more digital and more datafied, data flows are becoming increasingly integral in all sectors. As illustrated in previous chapters, data flows, which are at the heart of the datafied economy, include complex types of information – from social media, video streaming, and health and financial data to other business services. Indeed, data flows literally constitute our social relations.[1] The so-called data explosion is real, and it is here. According to AmCham, more than 4 billion people spent a total of 3.7 trillion hours on social media in 2021.[2] In 2022 alone, 74 zettabytes of data were generated.[3] Labeled "the lifeblood of the modern economy," much of today's international trade in services would not exist without cross-border data flows – the movement of data between computer servers across national borders.[4]

Parts of this chapter are based on the author's previous work: Shin-yi Peng, "Public-Private Interactions in Privacy Governance" (Concept Paper) (2022) 11(6) MDPI-Laws Special Issue: International Law as a Driver of Internet Governance, at 80; Shin-yi Peng, "Private Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime" (2018) 51(2) Cornell International Law Journal 445.

[1] Salomé Viljoen, "An Argument for Positive Political Theories of Data Governance" (2022) 6 Georgetown Law Technology Review 464, at 466.

[2] Daniel S. Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2021: Annual Survey of Jobs, Trade and Investment between the United States and Europe" (2021).

[3] World Trade Forum, "How Industrial Data Can Help Unleash Productivity, Innovation and Sustainability" (May 13, 2022) <www.weforum.org/agenda/2022/05/industrial-data-can-unlock-our-sustainable-future-heres-how/>.

[4] OECD, "Fostering Cross-Border Data Flows with Trust" OECD Digital Economy Papers No. 343 (December 2022); The U.S. Congressional Research Service (CRS), "Data Flows, Online Privacy, and Trade Policy" (March 26, 2020).

It would be a misunderstanding if one were to think that cross-border data flows are less significant to the manufacturing sector. Data flows are now an integral part of almost all new technologies, including the IoT, AI, 3D printing, and cloud computing, etc.[5] More and more businesses depend on data flows for interconnected machinery and big data analytics. In particular, smart manufacturing – the application of digital technologies to manufacturing processes, from supply chain management to after-sales support – relies on cross-border machine-to-machine data flows.[6] Data-enabled goods and services require data and their flows across borders to support commercial activities, which generally include all of the stages of design, production, delivery, sales, and maintenance.[7] As a result, digital technologies are now connecting billions of people to one another, and they are also connecting those people to billions of devices. Furthermore, they are connecting all of those billions of devices.

In short, in terms of commercial aspects, cross-border data flows are central to the digital economy. Many sectors, including smart manufacturing, are highly reliant on digital trade and data flows. Cross-border data flows accelerate data-driven innovation and facilitate international trade in goods and services. More specifically, they enable smart manufacturing and global value chains and support cross-border services and platform activities.[8] At the same time, in terms of social aspects, the ubiquitous exchange of data across borders enables modern-day social interactions. Today's internationally connected social network is underpinned by the movement of data across borders.

Data flows connect the entire Internet ecosystem. As illustrated in Figure 0.1 of the Introduction of this book, horizontally, data flows across different servers, while vertically, data flows across different layers,

[5] See, for example, Zurich Insurance, "Cross-border Data Flows: Designing a Global Architecture for Growth and Innovation" (2022) <www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation>.

[6] Frontier Economics, "The Value of Cross-Border Data Flows to Europe: Risks and Opportunities" (June 2021) <https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf>, at 15.

[7] OECD, supra note 4, at 10–12.

[8] CRS, supra note 4. As illustrated in Section 1.4.4, the concept of "digital trade" is understood in a broad sense. The EU defines it as "commerce enabled by electronic means – by telecommunications and/or ICT services – and covers trade in both goods and services." EU, "Digital Trade" (2023) < https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en >.

including the network infrastructure and digital platforms. This final chapter, therefore, is somewhat of a cross-cutting, catch-all chapter that addresses the key challenges to cross-border data flows. In the wake of the datafied economy, should data be able to flow across borders by default? How can we safeguard privacy and security while reaping the economic and societal benefits of cross-border data flows? How can international trade agreements promote the movement of data while allowing states to ensure desired protections over data that crosses national borders? More importantly, how can we facilitate national regulatory approaches that work together on a global scale? These are the primary questions this chapter attempts to address.

6.2 Data Flow Restrictions as Trade Barriers

6.2.1 Cross-Border Data Flow Restrictions

In most situations, the "raw data" we generate in our daily lives crosses a number of national borders. As illustrated in Chapter 5, businesses process and compile individual profiles for many reasons, including targeted marketing. Data can also be sold or exchanged between businesses for such purposes. All of these scenarios bring significant challenges to data privacy and security, especially when personal data is transferred to other countries.[9] Disputes arise when personal data is safeguarded domestically but is less protected in another country. Conversely, it also poses a potential trade conflict when the flow of personal data is relatively free at home but is subject to strict restrictions abroad. Such international confrontations are now being amplified by new technologies such as the IoT and AI, simply because of the increasing reliance on cross-border data flows.

Much literature has documented national regulations that constrain the free flow of data across borders. According to studies conducted by the Information Technology & Innovation Foundation (ITIF), the number of countries that have adopted data localization measures has doubled in recent years, and the total number of data localization regulations around the world reached 144 in 2021.[10] In addition to

[9] OECD, supra note 4, at 10–12.

[10] A substantial body of literature exists on how states regulate cross-border data flows. See, for example, Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" Information Technology & Innovation Foundation (ITIF) (July 19, 2021) <https://itif.org/publica

explicit data localization measures that require data to be physically stored in the country where it originates, more and more *de facto* localization measures impose stringent and sometimes arbitrary data transfer requirements. As a result, businesses "choose" to store data locally to avoid complicated and costly pre-approval procedures for data transfers.[11] Taking a broader view, increasingly, states are deciding to regulate every stage of the data flow cycle in order to protect citizens' data privacy and security. Understanding what types of data are subject to which data regulations in the domestic context is complex enough. This problem can be made much more complex when data is transferred to other countries. Governments have been placing conditions on the movement of data across borders to ensure that data protections follow the individual; namely, when data is transferred outside a specific jurisdiction, the protections over it remain equivalent.[12] Consequently, data is subject to different rules depending on where it originated, where it is located, and the type of information it contains.

For businesses, overlapping or sometimes conflicting requirements create operational uncertainty surrounding which regulations apply to which data. This, in turn, can increase compliance costs.[13] Indeed, digital fragmentation is gearing up. When data crosses jurisdictions, regulatory harmonization becomes extremely challenging considering how individuals from different cultural and social backgrounds define the boundaries of their personal space, how people accustomed to different national conditions perceive appropriate limits on governmental surveillance, and what factors must be weighed and balanced when regulating cross-border data flows. In the context of international trade, businesses confront hurdles when attempting to comply with often conflicting requirements of diverse national regulations. Divergent national approaches raise costs and thereby direct resources away from more efficient operations, a phenomenon which eventually increases the price of goods and services offered to consumers. Notably, compliance costs stemming from conflicting rules may exceed what many SMEs can afford. In this regard, a fragmented data regulatory landscape creates

tions/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>, at 3.

[11] *Ibid.*, at 3–4.

[12] OECD, supra note 4, at 14.

[13] *Ibid.*, at 15.

the risk of squeezing out SMEs. At the end of the day, big tech can afford big legal departments and absorb the pain better than SMEs.

Whatever the different rationales behind the restrictions on cross-border data flows, these measures have affected global digital trade. Undeniably, free transborder data flows would enable services suppliers to build their commercial networks and data centers based on their business models, thereby increasing business efficiency.[14] Data localization requirements, when strictly enforced, would force companies to "build expensive and unnecessarily redundant data centers in every market they seek to serve."[15] Moreover, data centers are capital-intensive, which may bring substantial economic and social benefits for the host state, including job opportunities, increased taxes, and technological know-how. This may also bring about the cluster effect – the overall growth of the data-driven economy of a nation. To conclude, a more liberalized, less fragmented, and more harmonized international framework for data flows would bridge the differences among jurisdictions, diffuse the threat of legal uncertainty, reduce business costs, increase compliance, and therefore provide benefits to both industry and consumers – not to mention the potential for global economic growth if the origin and destination countries of data flows are mutually bound by common, agreed-upon standards. Accordingly, reaching an international consensus regarding how to balance free data flows and national policy objectives, especially data privacy and security, is key to advancing the digital economy.

6.2.2 *A Balkanized International Marketplace?*

That said, the road moving toward regulatory interoperability,[16] which may bridge regulatory disparities and thus facilitate transborder data flows, is far from well paved. At the regional level, states' international commitments are "soft" in the sense that most of them are subject to

[14] Joshua P. Meltzer, "The Internet, Cross-Border Data Flows and International Trade" (2015) 2(1) Asia & Pacific Policy Studies 90, at 91–92.

[15] USTR, "Chapter Summary of Electronic Commerce"<https://ustr.gov/sites/default/files/TPP-Chapter-Summary-Electronic-Commerce.pdf>, at 2.

[16] For a working definition of the term "privacy interoperability," see OECD, "Going Digital Guide to Data Governance Policy Making" (2022) <www.oecd.org/science/going-digital-guide-to-data-governance-policy-making-40d53904-en.htm>, at 45, in which "interoperability" is defined as the ability to "bridge any differences in approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data."

broad exceptions.[17] To be more concrete, although new generation FTAs more directly address data flows, they typically include general obligations to the free flow of data across borders, in conjunction with a commitment to maintain legal frameworks for personal data protection. In addition, they normally impose obligations to prohibit data localization, again, with accompanying exceptions. Taking the E-Commerce Chapter of the CPTPP as an example, Article 14.13 is the key provision that directly confronts data localization measures,[18] while Articles 14.8 and 14.11 lay down disciplines addressing personal data protection and cross-border data flows. Articles 14.11 (data flow) and 14.13 (data location) nevertheless recognize that the parties may impose regulatory requirements on "the transfer of information by electronic means,"[19] as well as requirements pertaining to "the use of computing facilities."[20]

More specifically, CPTPP allows parties to maintain data localization measures to achieve a legitimate public policy objective, as long as the measure "does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."[21] Note that, unlike GATT/GATS general exceptions, the exceptions to the free flow of data in the CPTPP contain an open-ended list of public policy objectives and require a trade tribunal's determination regarding whether an objective is legitimate.[22] Considering the political and economic sensitivity surrounding cross-border data flows, leaving the key element vague may make sense in terms of reserving parties' regulatory space. The question of how far such broad exceptions can go, however, will be interpreted by CPTPP tribunals when a real dispute occurs, triggering a high level of legal uncertainty about trade rules.[23]

[17] See generally Mark Wu, "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System" RTA Exchange, ICTSD and IDB (November 2017). See also Section 2.3.4.

[18] CPTPP, Article 14.13 (Location of Computing Facilities). See Section 2.3.3 for more discussion.

[19] CPTPP, Article 14.11 (Cross-Border Transfer of Information by Electronic Means).

[20] CPTPP, Article 14.13.

[21] *Ibid.*

[22] Note that with respect to data localization, the USMCA counterpart is stronger than the CPTPP, as the former is a straightforward ban, whereas the latter is linked to a loose exception. In this regard, the Coalition for App Fairness urged the Biden administration not to "make the same USMCA mistakes in the IPEF." Inside U.S. Trade, "New Tech Coalition Warns against USMCA Mistakes in IPEF Digital Rules" (May 18, 2023).

[23] This discussion draws upon materials in Shin-yi Peng and Han-Wei Liu, "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?" (2017) 51 (2) Journal of World Trade 183.

At the multilateral level, at the time of this writing, the WTO JSI on E-commerce had launched discussions on this most intense issue – data flows, with primary attention accorded to data localization measures.[24] In view of the "fundamental differences" among the major players – namely, the US, the EU, and China, all of whom are participants in the JSI e-commerce negotiations – it would be unrealistic to anticipate any high-standard agreement with deeper commitments. A less ambitious agreement incorporating the "common elements" of the three approaches, however, would only have a symbolic or nominal impact on cross-border data flows. After all, the fragmentation of national regulations and supervisions has transformed cyberspace into what the USTR coined "a balkanized international marketplace."[25] International arrangements that form like-minded states into coalitions may serve as an avenue through which to address such fragmentation, and in practice, several PTAs appear to be showing signs of convergence toward more similar data flow principles that employ identical or similar treaty language.[26] Nevertheless, substantial divides among the big players remain.[27]

In this context, transatlantic digital fragmentation has been the focal point of global data governance for years. In the Schrems I decision, which invalidated the US–EU Safe Harbor,[28] "adequate level of protection" was interpreted by the ECJ to require the third country to ensure "a level of protection of fundamental rights and freedoms" that is "essentially equivalent" to the EU data protection law.[29] Years later, in the

[24] Inside U.S. Trade, "WTO E-Commerce Leads 'Accelerating' Discussions on Data Flows, Privacy" (October 14, 2022).

[25] USTR, "What's Happening in the TPP on Twenty-first-Century Issues" <https://ustr.gov/about-us/policy-offices/press-office/blog/2013/march/tpp-21st-century-issues>.

[26] As explained by Mira Burri, there appear to be "path dependencies in the global digital trade rule-making." Mira Burri, "Trade Law 4.0: Are We There Yet? (2023) 26(1) Journal of International Economic Law 90.

[27] See, for example, USTR, "2023 National Trade Estimate Report on Foreign Trade Barriers" <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/march/ustr-releases-2023-national-trade-estimate-report-foreign-trade-barriers>, at 88 (pointing out that China's restrictions on cross-border data flows and the data localization requirements have severely restricted cross-border data flows and impaired US services suppliers' market access opportunities in China).

[28] Maximillian Schrems v. Data Protection Commissioner (Schrems I) C-362/14 (2015) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362_SUM&from=en>.

[29] *Ibid.*, paras. 6–7.

Schrems II decision, which invalidated the US–EU Privacy Shield,[30] the ECJ found that US surveillance laws do not afford EU data subjects adequate levels of protection equivalent to the EU's GDPR. Thus, transatlantic data flows became unlawful unless firms use standard contractual clauses or binding corporate rules.[31] The ECJ's invalidation of the two US–EU data transfer accords, that is, Safe Harbor in 2015 and the Privacy Shield Framework in July 2020, has threatened bilateral transatlantic trade and created legal uncertainty for businesses, which are primarily SMEs.[32] More than two years after Schrems II, the Trans-Atlantic Data Privacy (TADP) Framework represents a new effort between the two sides to facilitate transatlantic data flows and digital trade.[33] As phrased by Burri, the mutual recognition framework between the US and the EU, although the "second-best" of solutions, nevertheless fosters international cooperation on data flow policies.[34] In any event, the US and the EU are making progress in becoming more closely aligned, despite their obvious differences in terms of data protection. It remains to be seen to what extent the TADP can "strengthen the privacy and civil liberties protections," and, more importantly, whether there will be a Schrems III, IV, V, and so on.

Against this backdrop, this chapter attempts to examine the issues surrounding cross-border data flows from two angles: physical–digital convergence, and public–private convergence. In light of the physical–digital convergence, "industry 4.0" further integrates physical and digital activities. Privacy and cybersecurity paradigms are in flux, a fact which calls for innovative approaches. At the same time, in light of the public–private convergence, the increasing function of soft private law instruments in data governance underscores the need to reconfigure the roles of the public and private sectors in this datafied world. The following sections respectively tackle these two angles.

[30] Data Protection Comm'r v. Facebook Ire. Ltd. & Schrems (Schrems II) C-311/18 (2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&from=E%20N>.

[31] *Ibid.*, paras. 184, 191, 192.

[32] CRS, supra note 4.

[33] On March 25, 2022, the US and the EU jointly announced an "agreement in principle" to the new Trans-Atlantic Data Privacy Framework (TADP). On December 13, 2022, the EU launched the process toward the adoption of an adequacy decision for the TADP.

[34] Mira Burri, "Interfacing Privacy and Trade" (2021) 53 Case Western Reserve Journal of International Law 35, at 87.

6.3 Privacy Governance in a Datafied World

6.3.1 Physical–Digital Convergence: Ubiquitous Data Collection

6.3.1.1 Privacy Paradigm in Flux

For decades, privacy self-management based on informed consent, commonly known as notice-and-consent or "notice-and-choice," has been the key component of any privacy regulatory regime. As reflected in the privacy protection frameworks of the OECD, the EU, and the Asia-Pacific Economic Cooperation (APEC), concepts such as "purpose specification" and "use limitation," together with individuals' positive consent to personal data collection practices, legitimize almost all forms of the collection and use of personal data.[35]

Along the path of technological developments and market changes, this consent-centric regime is facing increasing challenges, primarily surrounding its feasibility. Among all of the critiques,[36] the central question is how to ensure that consent is meaningfully granted in a manner that serves the objective of giving people purposeful control over their data.[37] Commentators contend that the notice-and-consent mechanism may function well in situations where consumers always devote sufficient time and attention to their privacy choices, and where service providers completely adhere to their privacy terms.[38] In the real world, however, both the "notice" and the "consent" components are problematic in today's complex information society, where data collection from cameras, microphones, sensors, and new facial recognition technologies is too ubiquitous to be sufficiently described under meaningful "notice." Living in this datafied world, it is simply unrealistic to issue a notice and obtain consent from every individual whose images are captured by facial recognition cameras installed on sidewalks or in supermarkets. The

[35] See generally Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 Harvard Law Review 1879.

[36] See, for example, Joel R. Reidenberg et al., "Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards" (2019) 96 Washington University Law Review 1409, at 1414; United States President's Council of Advisors on Science and Technology (PCAST), "Big Data and Privacy: A Technological Perspective" ("the PCAST Report) (May2014) <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>; Cf., Mike Hintze, "In Defense of the Long Privacy Statement" (2017) 76 Maryland Law Review 1044.

[37] Hintze, *Ibid.*, at 1045.

[38] John A. Rothchild, "Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online or Anywhere Else" (2018) 66 Cleveland State Law Review 559, at 647.

reality is that more and more personal data is passively obtained,[39] and more and more of our movements are being sensed and datafied in ways that we are not aware of. For example, retail stores are increasingly using facial recognition systems in their stores for security and operational purposes. With facial recognition technology installed, retailers are able to bar people with criminal records from entering, recognize shoppers upon entry into the store, provide personalized information and services, monitor staff members who take too many breaks, and, more importantly, collect information for future targeted marketing.[40] To be sure, an increasing proportion of personal data is now being passively collected through constant surveillance and tracking.[41] In daily lives, our faces are often being scanned absent the provision of proper "notice." When data collection occurs passively through surveillance technologies, how can individuals be meaningfully informed and thus consent to it?

At the same time, the "consent" component is equally if not more troubling in our daily lives. It has been empirically proven that privacy policies are "notoriously" long.[42] Twitter's privacy policy, as an illustration, is literally nineteen pages in length.[43] There are endless examples of privacy statements that are impossible, or at least impractical, for consumers to read and comprehend their legal implications. In most cases, consumer consent is arguably illusory, with consumers allocating only a few seconds of very limited attention to quickly scan the "offer" and then "accept" it without an adequate understanding of the transaction.[44]

6.3.1.2 Informed Consent and Big Data Analytics

Big data analytics is now a popular tool through which businesses analyze high-volume and high-variety information assets from both physical and digital spaces. To realize the benefits of big data analytics, businesses must "collect as much data as possible ... from as many sources as

[39] McKay Cunningham, "Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm" (2014) 2(2) Groningen Journal of International Law 115, at 134.

[40] See, for example, Sergio Mannino, "How Facial Recognition Will Change Retail" (*Forbes*, May 8, 2020).

[41] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power* (2019), at 136, 139.

[42] Reidenberg et al., supra note 36, at 1412.

[43] Twitter Privacy Policy <https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-aug-19th-2021/Twitter_Privacy_Policy_EN.pdf>.

[44] Cunningham, supra note 39.

possible,"[45] simply because the more sophisticated and larger in scale the data set is, the more successful the big data analytics. In addition, businesses need to "store" the data so they can process and utilize it at a later stage. Throughout the entire big data analytics process, individuals' data privacy and security risk being misappropriated or breached if they are not well managed.

As discussed, the "notice" and "consent" components operate awkwardly in a datafied world. It must be stressed that big data analytics has intensified the dysfunction of the privacy informed-consent regime. The ubiquitous nature of data collection and the explosive volume and variety of data processed today render the "notice and consent" framework, which has been an important pillar of privacy regulation, more and more problematic in practice. Mundie observes that "[t]here is simply so much data being collected, in so many ways, that it is practically impossible to give people a meaningful way to keep track of all the information about them."[46] Even well-informed individuals who practice due diligence may not be able to meaningfully control their data usage. Privacy policies are growing longer and becoming more "all-encompassing" in response to the potential of big data analytics. Service providers tend to craft privacy statements that will cover every possible future use and reserve the maximum space for data aggregation. Written privacy policies, which contain information regarding how service providers will collect and share data with each other, are too vague to represent meaningful notice.[47] It goes without saying that blanket consent, which allows for an unlimited array of data aggregation, is socially undesirable.[48] How can we meaningfully consent to the use of raw data if the fruit of the analysis remains a mystery? In short, big data analytics has become such a common practice that it renders the informed-consent system

[45] Institute for Human Rights and Business (IHRB), "Data Brokers and Human Rights: Big Data, Big Business" (November 2016) <www.ihrb.org/focus-areas/information-communication-technology/data-brokers-big-data-big-business>.

[46] Craig Mundie, "Privacy Pragmatism: Focus on Data Use, Not Data Collection" (2014) 93 (2) Foreign Affairs 28.

[47] See, for example, WhatsApp Privacy Policy, which states "As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the other Facebook Companies. We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings" <www.whatsapp.com/legal/privacy-policy/?lang=en>.

[48] Solove, supra note 35, at 1881.

unworkable. It does not make legal sense to expect that a consumer can honestly and capably evaluate each privacy policy.

It should also be noted that the aggregation of personal data over a period of time by different service providers has brought privacy risks to a new level. Privacy harms might result from cumulative and holistic data usage. To illustrate, an individual consents to Service Provider A's use of his/her nonsensitive data at one point in time, and reveals other equally nonsensitive data to Service Provider B and Service Provider C at later points in time. Service Provider A, which has access to multiple sources of this individual's partial personal information, may be able to effectively piece together data (from Service Provider B and Service Provider C) and thereby analyze and profile sensitive information about this individual. Considering such an aggregation effect, managing personal data in every isolated transaction with separated service providers is no longer an effective way to prevent privacy harms, which may be the result of cumulative and holistic data usage.[49]

Altogether, new technological capabilities are accelerating the problems associated with privacy self-management as defined by Solove.[50] Datafication makes it possible for businesses to use data in ways that may have been technologically infeasible at the time of data collection and thus are beyond the original scope of informed consent. IoT devices, as an outstanding example, are becoming important components of the datafication process due to their ability to connect people at all times, continuously collecting and transmitting data. Sensors throughout a "smart house" track individual residents' behaviors and adjust the house conditions autonomously, including energy use and home security. Sensors in our cars gather real-time data on where the vehicle travels. Additionally, sensors at libraries "talk to" the books we borrow through the radio-frequency identification (RFID) affixed to the books. All of these sensors – at home, in our cars, and in public places – capture terabytes of data. The inevitable situation is that more and more everyday objects are connected to a network, and all of these devices constantly generate data and send it across borders. The expansion of new digital applications makes it even more unlikely that consumers will be able to precisely follow how their personal data is generated, for what purpose,

[49] *Ibid.*

[50] *Ibid.* See also Ari E. Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press 2018), at 83–85 (arguing that privacy policies are inadequate, confusing, and ineffective).

and by whom, as well as how much of their data is captured, sold, and ultimately used. A valid consent, however, must be "both specific and informed," providing the individual with precise details about the specific use.[51] Considering "the high threshold for a valid consent,"[52] the informed consent mechanism is gradually losing its function in today's technological and market environments.

On the other hand, privacy self-management based on informed consent may also constitute unnecessary barriers to the potential use of big data that could promote public interests and social values.[53] In the big data ecosystem, it is difficult for service providers, when providing services, to predict how the collected data might be aggregated in the future. As for the innovation sectors, a privacy regime that requires informed consent before data collection reflects an outdated technological landscape. Innovations in data aggregation and analysis are rapidly being introduced – a fact which may not be apparent when the data is collected.[54] Commentators therefore argue that the timing of consent should be more heavily focused on downstream uses rather than on the time of data collection.[55] Admittedly, the benefits of innovative and unexpectedly powerful uses of data enabled by big data analytics, to a certain extent, are defeated by the informed consent system. Bearing in mind that big data analytics has the potential to drive social benefits, from public infrastructure to medical innovations, the consent requirement at the time of data collection might serve as a *de facto* prohibition on potential big data applications.

6.3.2 *Public–Private Convergence: Privacy Regulatory Models*

6.3.2.1 Possible Roles of Private Actors

If the traditional "informed-consent" based, government-dominated approach has "lost much of its effectiveness"[56] and thus is ill-suited to the big data ecosystem, what should be the future direction of policy? Can private governance fill the gap created by state regulation? What

[51] The UK Information Commissioner's Office (ICO), "A Guide to International Transfer" <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-1–0.pdf>, at 11.
[52] *Ibid.*, at 12.
[53] Solove, supra note 35, at 1889.
[54] *Ibid.*, at 1895.
[55] *Ibid.*
[56] Melanie Hicken, "Big Data Knows You're Broke" (*CNN Money*, April 29, 2014).

about a hybrid governing framework in which the public and private sectors work together to reshape the landscape of the data protection regime? As a matter of fact, privacy certifications operated by the private sector have been developed to vouch for a service provider's compliance with certain privacy standards.[57] Over the past two decades, although notable attempts at privacy certification have not been popularly adopted on a global scale, certification has been gradually incorporated into the privacy practices of many transnational corporations.[58]

More importantly, innovative approaches have been proposed to enhance the role of private actors in privacy governance. Some policymakers became aware that the fundamental problem of the informed consent system is that it places the heavy burden of privacy protection on consumers.[59] To address the "non-level playing field in the implicit privacy negotiation between provider and user,"[60] substitutes for informed consent have been proposed to ensure that individuals have meaningful choices in managing their personal data. One direction is to empower individuals to "negotiate" with service providers with the assistance of a mutually accepted intermediary.[61] We need to create a new mechanism under which individuals can "delegate" their privacy preferences to a private actor they trust, such as an app store, industry organization, or private association.[62] Such a private actor would negotiate with other providers of similar services on behalf of consumers for a preferred level of privacy protection. In other words, individuals would delegate, on a commercial or noncommercial basis, the management of their personal data to a third party, which would then carefully read the service provider's privacy "offer," ensure that the privacy statement is sufficiently clear, negotiate the terms, formulate a meaningful consent to "accept" the transaction, and investigate the service provider's privacy practices. Ideally, such a third-party service would create a "privacy watchdog" marketplace for privacy negotiation and management.[63] Some policymakers are of the view that under the intermediation of the

[57] Reidenberg et al., supra note 36, at 1413.
[58] *Ibid*., at 1412. This raises the question of whether such attempts have effectively complemented state regulations. The case studies of APEC and the GDPR in the Section 6.3.2.3 will discuss the role of third-party privacy certification in existing legal frameworks.
[59] The PCAST Report, supra note 36, at 38.
[60] *Ibid*.
[61] *Ibid*.
[62] See generally Mundie, supra note 46.
[63] *Ibid*.

third parties, which represent critical masses of consumers, problems with the informed consent system can largely be solved. In such a marketplace, the third party would negotiate on behalf of its clients with service providers, including big tech, to adjust their offerings. Individuals could withdraw and delegate the work to different private actors in the market.[64]

In addition, from the angle of industry-specific techniques, privacy protection in this big data era requires a third party to carry out de-identification and re-identification tests. To illustrate, de-identification is an increasingly central technique that is being used in big data applications.[65] Netflix, as an example, has 125 million streaming subscribers worldwide. This large user base allows Netflix to gather a tremendous amount of data, analyze consumer behaviors, and then make business decisions accordingly. If Netflix saw that 75 percent of subscribers watched all available seasons of a TV show, there should be a good chance that subscribers will continue to watch the newest season. Amazon, as another example, collects data on how often customers shop on its website, how much they paid for a particular product, where these items were shipped, and how customers paid for the purchases. The variety, volume, and velocity of all of this information enable big data analytics.[66] At the crux of the matter is how this data is aggregated, as well as to what extent the data is de-anonymized. Equally importantly, how likely is it that the de-anonymized data will be re-identified? In real-world practices, as the amount and sources of data grow, the likelihood that individuals will be re-identified increases. Nonsensitive data might be re-associated into sensitive data or become identifiable information. Nonetheless, privacy regulations are generally considered technology neutral legislation, in that the law itself does not specify de-identification procedures and techniques. For example, the Recital of GDPR stipulates that "in order to determine whether a natural person is identifiable," consideration should be given to "all the means reasonably likely to be

[64] The PCAST Report, supra note 36, at 38.

[65] See, for example, US Department of Health and Human Services, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" (2010)<www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>.

[66] Institute for Human Rights and Business (IHRB), "Data Brokers and Human Rights: Big Data, Big Business" (November 2016) <www.ihrb.org/focus-areas/information-communication-technology/data-brokers-big-data-big-business>, at 8.

used."[67] In this regard, "all objective factors" should be taken into account to evaluate whether certain means are likely to be used to identify individuals, including "the amount of time required for identification, the available technology at the time of processing, and future technological developments."[68] Therefore, how to de-identify a particular segment of data in a particular context and better manage the risk of anonymized data being used to re-identify a natural person require sectoral technical standards.[69] Private actors, such as a certification body or industry association with the necessary technical expertise, can carry out de-identification assessments, apply state-of-the-art technology to maintain anonymization, and reduce the risk of re-identification.

6.3.2.2 Typologies: Public–Private Interactions

Private actors play an increasingly important role in global governance, in conjunction with state regulations. Private and public authority dynamics emerge in complex ways, and various efforts have been devoted to classifying them into types: namely, complement type and competition type.[70] As for privacy governance, it is important to identify how public authority and the private sector can simultaneously shape global privacy norms, as well as what type of public–private partnership (PPP) model is best suited for data governance given the technological uncertainty.

The analytical framework proposed by Cashore et al. emphasizes that the middle ground between complement and competition should be identified to capture complex PPP. They point out that the conceptualization of public and private authority as either complementary or competitive might be an oversimplified approach. They suggest that we should move beyond the complement/competition dichotomy and map "a fuller suite of mechanisms through which public and private governance interact."[71] Cashore et al. created more detailed subtypes of public–

[67] GDPR, Recital 26 (Not Applicable to Anonymous Data) <https://gdpr-info.eu/recitals/no-26/>.

[68] *Ibid.*

[69] Irene Kamara, "Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardization Mandate" (2017) 8(1) European Journal of Law and Technology 1, at 10.

[70] See, for example, Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability" (2019) 92 Southern California Law Review 1529, at 1557.

[71] See Benjamin Cashore et al., "Private Authority and Public Policy Interactions in Global Context: Governance Spheres for Problem Solving" (2021) 15 Regulation & Governance 1166.

private interaction.[72] In their view, "collaboration" and "coordination" are the primary forms of interaction within complementary-type PPP. Collaboration is an active partnership that is built upon effective communications. This type of PPP works better if both parties are on equal footing, namely, there is no clear hierarchy between them. Conceptually different from collaboration, coordination refers to the "delegation" of political authority to private actors, which in most cases involves hierarchy.[73] In their analytical framework, the main subtype within the competition-type PPP is "substitution," which generally describes the substitution effects of private governance.[74] In other words, private actors intend to displace state regulation by industry self-regulation, such as a Code of Conduct (CoC).

With respect to privacy governance, the public and private sectors can either "coordinate" or "collaborate" on governance, both of which fall in the center of the public versus private continuum. On one end of the continuum is top-down, government-dominated, command-and-control state regulation, and on the other end is bottom-up, voluntary-based self-regulation. Coordinative and collaborative governance, each with a different proportion of private governance, are hybrid approaches that rely on both governmental enforcement power and private participation. Depending on the degree of state involvement, the public and private sectors coordinate or collaborate in privacy governance. Under the form of coordinative governance, the government delegates oversight to private actors;[75] Under the form of collaborative governance,[76] the state works hand in hand with the private sector, remains involved as a dynamic facilitator to "nudge" private sector participation, and uses a traditional enforcement mechanism such as a penalty only when necessary to complement the governing framework. Under both forms of coordination and collaboration, traditional command-and-control regulation remains the backup authority in driving the governance

[72] *Ibid.* First, under the category of complement, Cashore et al. further divide the group into "collaboration," "coordination," and "isomorphism." Second, under the category of competition, they further distinguish the types into "substitution" and "cooptation." Third, they introduce a third main conceptualization: "coexistence," which contains two subtypes: "layered institutions" and "chaos."

[73] *Ibid.*, at 1172.

[74] *Ibid.*

[75] *Ibid.*, at 1563, 1596.

[76] Kaminski, supra note 70, at 1561–1563.

structure.[77] Finally, under the form of "substitutive" governance, private efforts such as industry self-regulation may in some situations "preempt" state regulations.[78] Private governance can also assume a "competitive role" in which it competes directly with and even attempts to replace government standards.[79] Substitution may lead to "chaos" – with overlapping or contradicting governance goals and strategies.[80]

6.3.2.3 APEC/CBPR: From Self-Regulation to "Collaboration"?

How is PPP being implemented in the privacy protection frameworks? Let us use cases from the APEC's Cross Border Privacy Rules (CBPR) and the EU's GDPR as models for exploration. The APEC CBPR system is a self-regulatory initiative designed to facilitate cross-border data flows while protecting consumer data privacy. To be brief, CBPR is a certification system of privacy protection that service providers can participate in to demonstrate compliance with privacy "principles" reflected in the APEC Privacy Framework ("Privacy Framework").[81] The Privacy Framework, as the title indicates, establishes the minimum standards for privacy protection. Led by the US as preferable to the EU's approach to data protection, it's not surprising that the CBPR system is now recognized in the USMCA as "a valid mechanism to facilitate cross-border information transfers while protecting personal information."[82] There are currently nine participating countries in the CBPR, each of which is at a different stage of implementing the CBPR System.[83]

Essentially, the CBPR is a voluntary scheme that requires acceptance at the state level, followed by certification of the service providers seeking to be part of the system.[84] Indeed, the key component of the CBPR is that third parties are to inspect and certify the privacy practices of service providers against the Privacy Framework, and to manage privacy-related

[77] *Ibid.*, at 1562–1564.
[78] Cashore et al., supra note 71, at 1172.
[79] *Ibid.*
[80] *Ibid.*
[81] APEC, "Privacy Framework" (2017) <www.apec.org/publications/2017/08/apec-privacy-framework-(2015) >; APEC "Cross-Border Privacy Rules System" (2020) <www.apec.org/publications/2020/02/apec-cross-border-privacy-rules-system-fostering-accountability-agent-participation>.
[82] USMCA, Article 19.8.
[83] Australia, Canada, Chinese Taipei, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, and the United States.
[84] APEC, "What is the Cross-Border Privacy Rules System?" <www.cbprs.org/>.

dispute resolution for certified service providers. A service provider applying to join CBPR must establish its privacy statement and practices to be consistent with either the basic standards in the Privacy Framework or domestic regulation. Following the assessment, service providers certified by an APEC-recognized Accountability Agent may display a seal or a trust mark or otherwise claim to qualify under the CBPR System.[85] To maintain the system in operation, the APEC economies should select and endorse the "accountability agents" who certify the privacy practices of service providers that wish to join the scheme. Currently, there are nine APEC-recognized accountability agents.[86] In practice, accountability agents, such as Schellman & Company in the US, typically provide certification services in accordance with APEC privacy standards. Schellman & Company, as an example, performs testing to evidence the certification's minimum requirements. The testing procedures include inquiries with relevant personnel of service providers wishing to join the CBPR, observation of the relevant process, and inspection of relevant records.[87] In addition, certified service providers are monitored throughout the certification period, including periodic reviews of the service provider's privacy policies, to ensure compliance with the Privacy Framework. Annual re-certification is required to update the CBPR Questionnaire. Certification will be suspended if the certified service provider is found to have violated the CBPR requirements, and if such a breach has not been resolved within certain time frames.[88]

In terms of PPP, several aspects deserve further exploration. First, in terms of the nature of the accountability agents, CBPR features a hybrid form of public and private organizations. While the five US-based accountability agents have private characteristics, other Asia-based agents are either government agencies or government-affiliated organizations: the Internet & Security Agency (KISA) is South Korea's Ministry of Science and ICT's suborganization;[89] the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is a public-interest corporation in Japan, which has long been in close cooperation with Japan's

[85] CBPR, "Interested in Becoming APEC CBPR Certified?" <http://cbprs.org/business/>.
[86] *Ibid.*, including TrustArc (US), Schellman (US), BBB National Program (US), HITRUST (US), NCC Group (US), JIPDEC (Japan), IMDA (Singapore), KISA (Korea), and III (Taiwan).
[87] Schellman & Company, "APEC Cross Border Privacy Rules (CBPR) Certification Process and Minimum Requirements" <www.schellman.com/apec/cbpr-process>.
[88] *Ibid.*
[89] The Internet & Security Agency (KISA) <www.kisa.or.kr/eng/main.jsp>.

Ministry of Economy, Trade and Industry;[90] and Singapore's ICT regulator, the Infocomm Media Development Authority (IMDA), is a statutory board under the Singapore Ministry of Communications and Information. While appointing an assessment body such as the BSI Group to determine whether a service provider's data protection practices conform to the CBPR requirements, the IMDA remains the Accountability Body under the Privacy Framework.[91] The Institute for Information Industry (III) in Taiwan is a nongovernmental organization that has long acted as an ICT "think tank" for the government.[92] Evidently, the degree of state involvement is more than nominal.

Another angle worth noting with regard to public–private interactions under the CBPR regime is the role of governmental enforcement authorities. By its very nature, the CBPR is an instrument of self-regulation. The main deficiency that hampers its overall effectiveness is the lack of sufficient governmental guidance and supervision. Nevertheless, there are some encouraging stories demonstrating that national regulators may sometimes act as "privacy cops" to sustain the integrity of the CBPR system. One striking example is the US Fair Trade Commission (FTC), which in 2014 fined TRUSTe (now TrustArc) for failing to timely re-certify participating companies on an annual basis, which violates its own certification policy.[93] In addition, the FTC in 2016 alleged that Vipvape had engaged in deception in its privacy statement. Vipvape had falsely advertised that it was a certified participant in the CBPR scheme, which it was not. The bilateral settlement between the FTC and Vipvape bans Vipvape from misleading the public about its certification status under the Privacy Framework. According to the FTC, "the governmental oversight and enforceability of the CBPR are mandated by the terms of the system itself."[94]

[90] The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) <https://english.jipdec.or.jp/>.

[91] The Infocomm Media Development Authority (IMDA). The certification application fee is payable to the IMDA. <www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification>.

[92] The Institute for Information Industry (III) < www.tpipas.org.tw/>.

[93] To date, the FTC has brought four actions to enforce companies' promises under APEC CBPR. See FTC, "Report to Congress on Privacy and Security" (September 13, 2021) <www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf>.

[94] "FTC Settles with Vipvape on CBPR Privacy Policy Deception" (*Data Protection Law & Policy*, June 2016).

Nevertheless, public enforcement under the CBPR remains limited. The low degree of state involvement has resulted in a lack of accountability. For consumers, there is no strong incentive to seek out those service providers that are CBPR certified. In turn, there are weak incentives for service providers to invest in and obtain CBPR certification. To conclude, the CBPR system falls between "collaborative governance" and "self-regulation" along the public versus private spectrum. Moving toward an accountable, collaborative form of governance, the future success of the CBPR depends on whether systemic and aggregate accountability over public–private interactions can be established.[95] Such accountability calls for a higher degree of state involvement and, in particular, requires national regulators to act as "privacy cops."

6.3.2.4 EU/GDPR: From State Regulation to "Coordination"?

The GDPR, on the other hand, is fundamentally a "hard law" by nature, backed by enforcement penalties.[96] Nonetheless, the regime seems to leave room for PPPs, namely, allowing private actors to complete the details of how to comply with the legal requirements through the CoC or certification mechanisms. Both the CoC and certification require an independent, third-party body to assess conformity with the normative documents, and they also require the assessor to be accredited. In addition, both the approved CoC and certification are recognized by the GDPR as factors when national regulators assess penalties for noncompliance.[97] Furthermore, both the CoC and certification, if coupled together with binding enforceable commitments to apply appropriate safeguards, can be used by controllers and processors in third countries as a legitimate basis for cross-border transfers of data.[98]

With respect to the CoC, associations or "other bodies representing categories of controllers or processors" are encouraged to draw up sector-

[95] Kaminski, supra note 70, at 1568–1580; Ira S. Rubinstein, "The Future of Self-Regulation Is Co-Regulation" in Evan Selinger et al. (eds) *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018), at 503.

[96] Kaminski, *ibid.*, at 1611.

[97] See generally Eric Lachaud, "What GDPR Tells about Certification" (2020) 38 Computer Law and Security Review 1, at 3–5; Clare Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era" (2019) 35(4) Computer Law & Security Review 380.

[98] *Ibid.*

specific CoC to "facilitate the effective application" of the GDPR.[99] The CoC may cover many aspects of the GDPR, such as "the pseudonymization of personal data" and "the transfer of personal data to third countries."[100] Wherever feasible, associations should consult stakeholders when preparing the CoC.[101] The monitoring of compliance with the CoC may be carried out by a body – including a private body – that is accredited by the national regulator.[102] Each regulator should "draft and publish the criteria for accreditation of a body for monitoring codes of conduct."[103] An accredited CoC monitoring body should "take appropriate action," for example, to suspend the controller or processor "in cases of infringement of the code by a controller or processor." A monitoring body should also report such actions to the regulator.[104] It should be noted that such an "action" from the accredited CoC monitoring body does not take the place of possible actions that can otherwise be activated by the authorities for noncompliance. Finally, in terms of service providers, "adherence to approved codes of conduct" is an element available to data controllers to demonstrate compliance with the GDPR obligations,[105] and it is also a factor when the regulator determines whether to impose an administrative fine, as well as the amount of the fine.[106]

With respect to certification,[107] the GDPR expressly recognizes data protection seals and/or marks as mechanisms for demonstrating compliance and enhancing transparency.[108] Certifications may be issued by either the European Data Protection Board, a national regulator, or a private third party that is an accredited certification body.[109] The certification bodies should conduct a "proper assessment leading to the

[99] GDPR, Recital 98.
[100] GDPR, Article 40.
[101] GDPR, Recital 99.
[102] GDPR, Article 41.
[103] GDPR, Article 57.
[104] GDPR, Article 41.
[105] GDPR, Article 24.
[106] GDPR, Article 83.
[107] Note that the European data processing board approved the very first European Data Protection Seal- Europrivacy. The Europrivacy certification can help data controllers and data processors certify privacy practices that demonstrate compliance with the GDPR. European Commission, "Shaping Europe's Digital Future" (October 17, 2022) <https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr>.
[108] GDPR, Recital 100.
[109] GDPR, Article 42.

certification," or the withdrawal of certification in the case of noncompliance.[110] The certification body should also inform the regulator and provide reasons for granting or withdrawing certification. More importantly, a certification does not "reduce the responsibility of the controller or the processor for compliance with this Regulation."[111] National regulators possess the investigative power to "order the certification body not to issue certification" when the requirements for the certification are not met. National regulators also retain the power to withdraw a certification, or to order the certification body to withdraw a certification "if the requirements for the certification are no longer met."[112] Finally, like the CoC, adherence to approved certification mechanisms is a key factor to consider when regulators impose administrative fines on certified service providers for noncompliance.[113]

At the crux of the matter is whether the GDPR relies on PPP in governing data. Can the CoC and certification systems work better under coordinative-type PPP? To what extent do EU member states delegate authority to private actors in terms of governance? Obviously, there is a hierarchical relationship between public and private actors in the GDPR framework. National regulators are entitled to approve or disapprove the certification requirements. Arguably, the accredited private bodies' certifying power is conditional,[114] as the certification can be withdrawn at any time by the regulator if the conditions of issuance are no longer met. Overall, the CoC and certification mechanisms under the GDPR remain in a top-down, command-and-control arrangement. Moreover, the GDPR has serious "teeth" with regard to an accredited private body's obligations. Infringements on the obligations of the CoC's monitoring body or the certification body will be subject to administrative fines of up to 10,000,000 EUR, or up to 2 percent of the "total worldwide annual turnover of the preceding financial year," whichever is higher.[115] This results in weak incentives for private actors to actively participate in the governing scheme. Additionally, the role of a certification body is further weakened by the GDPR certification's lack of presumption of conformity. GDPR certifications are not considered to offer a "presumption of

[110] GDPR, Article 43.
[111] GDPR, Article 42.
[112] GDPR, Article 58.
[113] GDPR, Article 83.
[114] Lachaud, supra note 97.
[115] GDPR, Article 83.

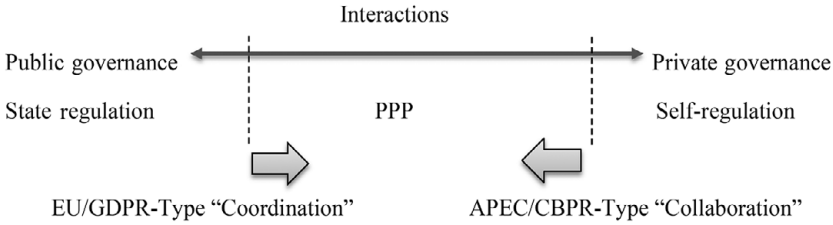

Figure 6.1 Public–private interaction in privacy governance

conformity" with the obligations under the GDPR.[116] In other words, the assessment by the certification body that a process is in line with the certification criteria merely grants a "stamp of approval" for the accountability of the certified service provider. The presence of such accountability, however, does not "reverse the burden of proof," and it does not indicate "presumed compliance" with the GDPR.[117] As such, GDPR certification does not entail *prima facie* full compliance with the GDPR. It does not act as a safe harbor from GDPR enforcement, nor does it provide the benefit of reduced regulatory scrutiny.[118] To conclude, the CoC and the certification systems rely too heavily on public governance and invoke private governance at a minimal level. The GDPR-type public–private "coordination" risks are too command-and-control oriented.[119]

The analysis above demonstrates the fluid interactions across public and private governance realms. As shown in Figure 6.1, self-regulation and state regulation are opposing ends of a regulatory continuum, with CBPR-type "collaboration" (moving from self-regulation to collaborative governance) and GDPR-type "coordination" (moving from state regulation to coordinative governance) falling somewhere in the middle. Turning to the question of how private actors can play more important roles when privacy paradigms are in flux, after assessing whether PPP is now being implemented in privacy protection, this section concludes that

[116] See Irene Kamara, "Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation" in Dara Hallinan et al. (eds), *Data Protection and Artificial Intelligence* (Hart Publishing 2021), at 83.
[117] Cf., Lachaud, supra note 97, at 7.
[118] See also Machiko Kanetake and André Nollkaemper, "The Application of Informal International Instruments Before Domestic Courts" (2014) 46 George Washington International Law Review 765.
[119] Kaminski, supra note 70, at 1599–1601.

there is an evident gap between private actors' potential governing functions and their current roles in privacy protection regimes. Looking to the future, technological developments and market changes call for further public–private convergence in privacy governance, allowing both the public authority and the private sector to simultaneously reshape global privacy norms.

6.4 Cybersecurity Governance in a Datafied World

6.4.1 Physical–Digital Convergence: Security in the Industry 4.0 Landscape

In a similar vein, physical–digital convergence posts unprecedented governance challenges to data security, which has been described by Weber as follows: "everything will inevitably be compromised at some point."[120] The core concept of Industry 4.0 is the connection of machinery to the Internet,[121] which encompasses many types of disruptive technologies.[122] The IoT applications, which feature the aggregation of many machine-to-machine connections, literally represent the penetration of the Internet into our everyday lives. It is now a regular occurrence in our daily experiences that IoT technologies tie together billions of devices, ranging from smartwatches, wearable sensors, and refrigerators to factories, cars, and drones.[123]

Industry 4.0 digitizes and integrates physical and digital activities. When everything can be connected to the Internet, everything can potentially be hacked. Consequently, the explosion of "smart" objects is causing unique security risks, which calls for a new security paradigm. It should be underscored that digital attacks on connected devices threaten both the physical and the digital world. For example, a connected car can be seen as a component of the entire IoT system. Depending on the level of automation, a connected car can interact with

[120] Rolf H. Weber and Evelyne Studer, "Cybersecurity in the Internet of Things: Legal Aspects" (2016) 32 Computer Law & Security Review 715.

[121] The Fourth Industrial Revolution refers to "the use of advanced digital technologies in industrial production and service delivery processes to enable new and more efficient processes for the production of goods and services combining traditional and digital technologies." See, for example, European Parliament, "Industry 4.0" (2016) <www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf>, at 20, 22, 83.

[122] *Ibid.*, at 22.

[123] Hamilton and Quinlan, supra note 2.

its users, other cars, the surrounding transportation infrastructure, and all other IoT devices. When a connected car communicates with other cars or infrastructure, risks arise from both physical and virtual sources. Hackers can control and damage the car itself, the Internet services supporting it, and the external systems that are digitally linked with the car. In short, security concerns surrounding connected devices are complex and relate to both mechanical safety and cybersecurity.[124] From an industrial perspective, such a physical–digital integration changes security practices, the most notable of which is the concept of "security by design," which generally indicates that "security should be built into a product by design" and "integrated at every stage of the product's development."[125] In doing so, security concerns can be addressed throughout "the entire product life cycle" – from its design to its disposal.[126] For example, connected car manufacturers are required to comply with the principle of security-by-design throughout the full life cycle of the cars so as to enhance the safety of the "cyber-physical vehicle system."[127]

Looking to the future, the emerging "digital twin" has enhanced smart manufacturing to another level, relying on "a virtual model designed to accurately reflect a physical object."[128] Updated from real-time data, digital twin technology allows for the remote monitoring of facilities

[124] Shin-yi Peng, "Autonomous Vehicle Standards under the Technical Barriers to Trade Agreement" in Shin-yi Peng et al. (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021), at 125–126.

[125] See, for example, European Commission, "Security by Design: Definition of the Principle" <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap/security-design>.

[126] Similarly, "Privacy by Design" means building privacy into the design, operation, and management of a given system, business process, or design specification. See Privacy Europe, "GDPR: Privacy by Design" <https://gdpr-info.eu/issues/privacy-by-design/>; Privacy measures are "embedded into the design and architecture of ICT systems and business practices." The World Bank, "Foundational Principles of Privacy by Design" <https://id4d.worldbank.org/guide/privacy-security>. The result is that privacy becomes "an essential component of the core functionality being delivered." Privacy is thus integral to the system; European Union Agency for Cybersecurity, "Privacy and Data Protection by Design" <www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

[127] Singapore Standard Council, "Technical Reference for Autonomous Vehicles" TR68. Part II: Safety. Part III (Cybersecurity Principles and Assessment Framework).

[128] See Gartner Glossary, "Digital Twin" <www.gartner.com/en/information-technology/glossary/digital-twin>.

and simulating processes.[129] Moving toward a Metaverse space, the sensors that consistently detect micro-level activities – including gestures, motions, and ambient conditions in virtual reality – can be seen as "physical extensions" of individuals' social identity: the "technological sense of self."[130] All of these emerging technologies, which further integrate and complement physical and virtual spheres, have their own privacy and security risks that must be managed.[131]

6.4.2 *Public–Private Convergence: Private Cybersecurity Standards*

6.4.2.1 Bottom-Up Approach to Cybersecurity Standardization

Cybersecurity risk management across all sectors, therefore, is more important than ever. Among all of the tools, cybersecurity standards contribute to risk management by establishing "common security requirements and capabilities needed for secure solutions,"[132] at least in reducing the effects of attacks if they occur.[133] Typically, cybersecurity standards, as "set forth in published materials that attempt to protect the cyber environment of a user or organization,"[134] define technical requirements, criteria for managing information and risk evaluation, techniques for handling security failures, and procedures following security breaches.[135] Cybersecurity standards are diverse and varied in scope and function, spanning the specifications of security features in web browsers, the mathematical definition of cryptographic algorithms, and other technical requirements.[136]

In terms of standards governance, there exists a spectrum of cybersecurity standardization models, ranging from more centralized, coercive, top-down governmental involvement to more decentralized, soft, bottom-up private initiatives. China's government-centered

[129] *Ibid.*
[130] Linda Tucci and Davie Needle, "What is the Metaverse? An Explanation and In-Depth Guide" (*TechTarget*, May 8, 2023).
[131] For example, informed consent for digital interactions in the Metaverse could be unprecedentedly challenging.
[132] See generally William Stallings, "Standards for Information Security Management" (2007), 10 Internet Protocol Journal 10.
[133] *Ibid.*
[134] Scholarly Community Encyclopedia, "Cybersecurity Standards" <https://encyclopedia.pub/entry/29282>.
[135] *Ibid.*
[136] *Ibid.*

standardization system represents the most outstanding case of a top-down regulatory approach. In the Chinese ICT market, the government assumes primary responsibility for standardization development, with the policy rationale that state-led standardization creates the most efficient national economy.[137] Conversely, there is a growing trend across the world toward a bottom-up approach to cybersecurity standardization.[138] Empirical studies demonstrate that more and more jurisdictions have been moving toward a bottom-up approach to cybersecurity standardization, which aims to minimize mandatory technical regulation and favors voluntary, private-sector standards to enhance cybersecurity.[139] Under the bottom-up approach, the business sector has actively taken on standardization initiatives, which they contend leads to more cost-effective rules than government regulation.[140] Behind the scenes, the privatization of governance has been driven, at least in part, by governments' lack of requisite technical expertise and the administrative flexibility to respond to rapidly changing regulatory needs.[141] The involvement of public and private sector actors working together has proven to be a more effective model than complete government control.

Emblematic of this movement with regard to the EU is the European Union Agency for Cybersecurity ("ENISA").[142] Mandated by the EU Cybersecurity Act as the hub in coordinating a cybersecurity certification framework throughout Europe, ENISA has actively contributed to cybersecurity standards, and thus, to the proper functioning of the internal market within the EU.[143] By working closely together with EU member states and the private sector, ENISA provides advice and solutions related to cybersecurity, supports policy implementation, and coordinates standardization activities.[144] As ENISA repeatedly stresses in its policy papers, it believes that enhancing the role of PPP should be emphasized in

[137] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions" (2016) Research Report Prepared on Behalf of the US–China Economic and Security Review Commission, at 2.
[138] Scott J. Shackelford et al., "Bottoms Up: A Comparison of 'Voluntary' Cybersecurity Frameworks" (2016) 16 U.C. Davis Business Law Journal 217, at 259.
[139] *Ibid.*
[140] Tim Buthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011), at 5.
[141] *Ibid.*, *at* 5–6, 9–10.
[142] The European Union Agency for Cybersecurity (ENISA) <www.enisa.europa.eu/>.
[143] *Ibid.*
[144] *Ibid.*

standardization processes.[145] Overall, a bottom-up approach to the creation of cybersecurity standards and strong representation from stakeholders are the key elements in ENISA decision-making procedures.[146] It can be said that the ENISA serves as an umbrella, under which a variety of certification schemes are encouraged to mutually recognize each other to mitigate potential fragmentation.[147] For instance, ENISA's Guidelines for Securing the Internet of Things,[148] which aims to provide security guidelines for IoT technologies, was created in conjunction with stakeholders involved in the supply chain of the IoT.

Similarly, the US National Institute for Standards and Technology Cybersecurity Framework (the "NIST Framework") was established to strengthen collaboration between the public and private sectors in their efforts to enhance cybersecurity.[149] In a series of multistakeholder meetings, international representatives across government, business, and civil society worked together to create the NIST Framework.[150] The NIST has been actively engaged with stakeholders through multiple avenues of communication.[151] Such a process demonstrates an active dialogue that relies on a bottom-up approach to cybersecurity regulation – building consensus across sectors and industries through a dynamic PPP. For example, together with stakeholders from government, industry, international bodies, and academia, the IoT Cybersecurity Program was established to develop standards and guidelines to improve the cybersecurity of connected devices.[152]

6.4.2.2 Cybersecurity Standards Chaos

Of course, the idea of governance through public-private networks is not at all new. The academic literature, including research in the field

[145] *Ibid.*
[146] *Ibid.*
[147] See generally Dimitra Markopoulou et al., "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation" (2019) 35(6) Computer Law & Security Review 2.
[148] ENISA, "Guidelines for Securing the Internet of Things" (2020) <www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.
[149] The National Institute of Standards and Technology (NIST) <www.nist.gov/about-nist>.
[150] *Ibid.*
[151] NIST, "Cybersecurity Framework" <www.nist.gov/cyberframework>.
[152] NIST, "Cybersecurity & Privacy Stakeholder Engagement" <www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement>; NIST, "Cybersecurity for IOT Program" <www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>.

of international economic law, has long examined the changing role of the state in market economies and the transformation of public functions.[153] In a world of high complexity, governments are delegating traditionally public functions to the private sector. Therefore, the world is increasingly governed through co-regulation by public and private actors.[154] With respect to cybersecurity, where public and private sectors attempt to adapt to rapid technological changes, it is particularly evident that governments must relax their regulatory power and shift responsibility through privatization.[155]

Nonetheless, bottom-up approaches generally lead to greater fragmentation than top-down approaches, simply because government-centered standardization systems have more influential positions in harmonizing the system. Indeed, cybersecurity standards are proliferating, exceeding 1,000 publications globally and resulting in a complex standards landscape.[156] This "mushrooms after rain" phenomenon surrounding private cybersecurity standards is now problematic in many ways. Although on the one hand it manifests the dynamics of the industry, it might also result in the danger of overlapping and even conflicting standards. From the perspective of international trade, the absence of a defined hierarchy over these private standards makes coordination challenging. The international "standards jungle" of cybersecurity, as a result, may lead to an uncoordinated set of standards and thus work as an impediment to free trade.

The IoT "standards chaos" serves as a strong example here.[157] The industry has been struggling to make sense of the IoT standards, which are currently moving in the opposite direction of the push toward universal standards for baseline security.[158] Dozens of organizations are currently developing various IoT cybersecurity standards and issuing IoT cybersecurity certifications. These disparate schemes, however, are

[153] See, for example, Gregory Shaffer, *Defending Interests – Public-Private Partnerships in WTO Litigation* (Brookings Institution Press 2003), at 12–14.

[154] Shackelford, supra note 138, at 219.

[155] Shin-yi Peng, supra note 124, at 130.

[156] PwC & The UK Department for Business, Innovation and Skills (BIS), BIS/13/1294, "UK Cyber Security Standards" (November 2013) <www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf>, at 4.

[157] Copper Horse, "Mapping Security & Privacy in the Internet of Things" <https://iotsecuritymapping.uk/by-sector-and-body>.

[158] Brian Buntz, "Amid IoT Standards Chaos, Put Business Matters First" (*IoT World Today*, April 20, 2019).

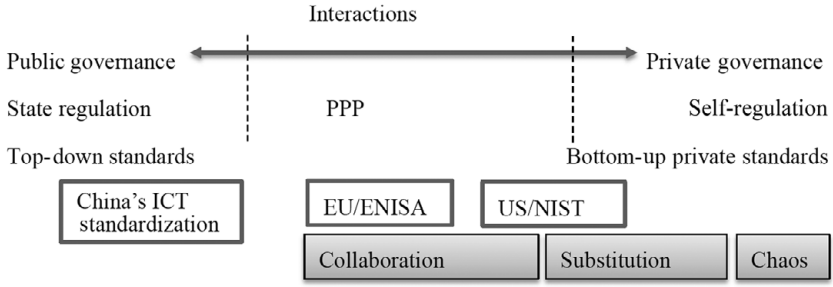

Figure 6.2 Public–private interaction in cybersecurity standardization

"nowhere near in sync" and can also be in conflict,[159] a fact which distorts the IoT value chain. Under such a fragmented landscape, IoT device manufacturers, sensor and chip suppliers, and software companies must manage all of these requirements and certify the security of their IoT products time and time again, with variants present around the world.[160] Evidently, the need to establish a global baseline for IoT cybersecurity is pressing. Turning back to the typologies framed above, public-private interactions in the realm of cybersecurity standards may be conceptualized as "chaos,"[161] as shown in Figure 6.2, in that they display no clear pattern and appear potentially contradictory.[162] From the aspect of international trade, a less fragmented standards regime can reduce barriers to entry into IoT markets. When ICT products are not manufactured with comparable cybersecurity standards, the need for interoperability will require extra gateways to translate one standard to another,[163] which will make it particularly difficult for SMEs to compete in the market.

To conclude, the implications of "standards" are unique in various contexts. Regardless, there is a strong link between technical standards and an efficient international trading system. In a globalized world, standards provide information about goods and services to ensure

[159] Copper Horse, supra note 157.
[160] Connectivity Standards Alliance (CSA), "Now is the Time for a Global Approach to IoT Cybersecurity" (September 12, 2022).
[161] See supra notes 72 and 80.
[162] See Cashore et al., supra note 72, at 1175.
[163] Bruce Sinclair, *IoT Inc.: How Your Company Can Use the Internet of Things to Win the Outcome Economy* (McGraw Hill Education 2017), at 194.

technical compatibility.[164] By sharing a common standard, anonymous manufacturers and services suppliers in markets all over the world can communicate, establish common expectations about one another's products, and evaluate the compatibility of their joint productions.[165] Any innovator in the market can develop new applications with the commercial certainty that an international market for their products will exist.[166] More harmonized cybersecurity standards, therefore, can facilitate "trade flows" from the aspects of both the demand and the supply of digital goods and services.

6.5 Global Architecture for Cross-Border Data Flows

6.5.1 *The Reconfiguration of Governance: A Holistic Approach and Hybrid Structure*

Taken as a whole, data flow governance is evolving into a debate over the roles of international organizations (IOs), sovereign states, private sectors, civil societies, and other stakeholders. We are facing a crossroads, where (Internet) multistakeholderism meets (trade) multilateralism.[167] This friction is evident. The former features more inclusive and transparent processes, under which public authorities govern alongside private and civic sectors, while the latter is inherently characterized as a series of top-down processes, in which states play central roles (and, in most cases, are the only actors).[168] Should global governance in the cyberspace context follow a multistakeholder approach that is premised on the broad participation of private actors, or move toward a more traditional,

[164] Xiaomeng Lu, "Standards-Related Barriers to Trade in Chinese ICT Market" (2008) Monterey Institute of International Studies, at 7.

[165] *Ibid.*

[166] *Ibid.*; Baisheng An, "Institutional Governance for ICT Standards at the International Level: Within the WTO and Beyond" (2012) World Trade Institute Series Paper.

[167] The term "multistakeholderism" refers to "two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature." In practice, there are various types of multistakeholder governance, produced by variations in the types of actors involved and the nature of authority. See generally William H. Dutton, "Multistakeholder Internet Governance?" (2016) World Bank Background Paper: Digital Dividends, at 2–5; Kal Raustiala, "Governing the Internet" (2017) 110 American Journal of International Law 491; Stefaan G. Verhulst, "The Practice and Craft of Multistakeholder Governance: The Case of Global Internet Policymaking" (2016) Global Partners Digital, at 8–9.

[168] Burri, supra note 26, at 10–11.

multilateral approach through treaty-based international arrangements with greater government oversight?[169]

Considered alone, however, neither approach suffices. On the one hand, the world today tells us that multilateralism has its limits. The analyses above, and throughout this book, reveal and confirm that international economic law alone may not be able to produce significant results to effectively address concerns surrounding datafication. The divergent regulatory goals and approaches of states – in particular, among the US, the EU, and China – render it a "mission impossible" for the WTO JSI on E-commerce to conclude a high-standard, broad agreement with deeper commitments that meaningfully tackle the important issues of cross-border data flows. A governance framework of modesty, as proposed by Shaffer,[170] with limited coverage and obligations that accommodate the divergent regulatory schemes of WTO members, might be the result of political reality.[171]

On the other hand, multilateralism, to which states consent, remains the key source of legitimacy in global trade governance. Controversies over cross-border data flows are at the heart of the digital economy and beyond. In this regard, states' digital policies and data regulations are playing, and will continue to play, a key role in shaping the global rules of the game. As demonstrated in the case studies of CBPR and IoT standards, state involvement and coordination remain significant in addressing problems arising from private regulations, such as the CBPR's lack of accountability and IoT cybersecurity standards chaos.[172] In any event, the role of multilateralism is indispensable in holding states accountable when they impose unjustified barriers to digital trade.

[169] See Joost Pauwelyn, "Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties" (2014) 17 Journal of International Economic Law 739, at 745; Urs Gasser et al., "Multistakeholder as Governance Groups: Observations from Case Studies" (2015) The Berkman Ctr. for Internet & Society Research Publication Series; Petros C. Mavroidis and Robert Wolfe, "Private Standards and the WTO: Reclusive No More" (2017) 16 World Trade Review 1, at 2–3.

[170] Gregory Shaffer, "Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience" in Shin-yi Peng et al. (eds) *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021), at 29, 42–52.

[171] At the same time, the fragmentation and uncertainties brought about by the FTAs further challenge international economic legal order. See Section 2.3.4 and Section 5.4.1.

[172] See Sections 6.3.2.3 and 6.4.2.2.

Accordingly, a holistic approach to, and the hybrid structure of, global governance, where the two approaches somehow merge and operate together, may be capable of striking a balance between decentralized, multifaceted initiatives and centralized decision-making.[173] Such a "blended governance regime," as advocated by Gasser,[174] can more proactively coordinate the various elements and actors of both multistakeholderism and multilateralism.[175] In the spheres of privacy and cybersecurity regulations, industry-driven soft standards and state-centered international rules can be employed as complements in a strategic and dynamic manner, and the two regimes can be linked and build upon each other. The potential role of each is explored below.

6.5.2 *The Role of (Internet) Multistakeholderism*

We have witnessed the difficulties and complexities associated with concluding digital trade rules through formal international treaties. In this context, the soft law nature of private initiatives can fill the gap left by international trade agreements, regardless of whether it is due to the "thin" obligations of, or the "vague" exceptions to, the trade rules. This book argues that the greater the legal uncertainty surrounding international law, the more critical the soft law norms that should be developed. Pauwelyn observed that the phenomenon of multistakeholderism incorporates not only informal actors and processes, but also soft law output.[176] The "products" of a multistakeholder process are often in the form of nonbinding soft law norms, that is, guidance, best practices, and codes of conduct. These soft private norms may, through various means and under different degrees, emerge and evolve into public regimes.[177] The softness of these informal regulations, although of a voluntary nature, can be linked to state-imposed standards or requirements in terms of both administrative and judicial organs.

[173] See Ayelet Berman et al., "Rethinking Stakeholder Participation in Global Governance" in Joost Pauwelyn et al. (eds), *Rethinking Participation in Global Governance: Voice and Influence after Stakeholder Reforms in Global Finance and Health* (Oxford University Press 2022), at 10–13.

[174] Urs Gasser, "Futuring Digital Privacy: Reimaging the Law/Tech Interplay" in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press 2021), at 195, 211.

[175] *Ibid.*

[176] Pauwelyn, supra note 169, at 742.

[177] Enrico Partiti et al., "Evolutionary Dynamics of Transnational Private Regulation" (2023) Transnational Legal Theory 1, at 7.

From the aspect of administration, cybersecurity standards are increasingly referred to by relevant regulators, to the degree that compliance with such standards becomes a core requirement in the "duty of care." For example, the US FTC has brought actions against companies whose cybersecurity practices it deemed had failed to take appropriate action in terms of "cybersecurity due diligence."[178] In these cases,[179] the FTC consistently relies on industry experts to prove whether the cybersecurity practices at issue are fully compatible with the NIST Framework.[180] In a broader context, by heavily referring to the NIST Framework established under multistakeholderism, the FTC signals to companies that the "soft, voluntary" nature of the NIST Framework has been recognized by the FTC as the "reasonableness standard for cybersecurity."

Likewise, from the aspects of judicial proceedings and litigation, private standards under multistakeholderism often give meaning to concepts in law, specifically when evaluating the duty of care in negligence cases.[181] Such judicial recognition can extend a binding effect to otherwise "voluntary" private standards.[182] In other words, even though the court does not (and cannot) apply private standards as such, private standards nevertheless serve as guidelines when it comes to the determination of the required standard of care. Compliance with these standards may not be a sufficient defense, but it does have evidentiary value when establishing cybersecurity due diligence requirements.[183] Specifically, the industry-led soft norms provide a baseline for judges in the evaluation of "reasonable care." Considering this, manufacturers may be able to partially mitigate the legal risk by demonstrating conformity to industry standards. Consequently, concerns about legal liability gradually become incentives for companies to comply with the soft law norms, which are

[178] Under its general statutory authority, Section 5(a) of the Federal Trade Commission Act addresses "unfair or deceptive acts or practices in or affecting commerce." Bruce Heiman et al., "The FTC Has Already Set Cybersecurity Standards" (*Law360,* March 5, 2015).

[179] See, for example, *Federal Trade Commission v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602 (2014).

[180] Vladimir J. Semendyai, "Due Process and the FTC's Fair and Reasonable Approach to Data Protection" (2016) 84 George Washington Law Review 51, at 66.

[181] Buthe and Wattli, supra note 140, at 205.

[182] *Ibid.*

[183] *Ibid.*; Katja Creutz, "Law versus Codes of Conduct: Between Convergence and Conflict" in Jan Klabbers and Touko Piiparinen (eds), *Normative Pluralism and International Law: Exploring Global Governance* (Cambridge University Press 2013), at 190–191.

not legally mandated, but which define best practices.[184] In this regard, soft private law instruments should not be seen merely as self-imposed corporate obligations. Rather, they can be a source of law in court proceedings.

It should be noted, however, that the increasing influence of soft private norms introduces new risks to big tech's dominant position in private norm-settings. Much like the well-organized industry lobbies in the multilateral treaty-making process, the multistakeholder process may become another effective vehicle for private actors with the greatest resources to press their cases. Large companies and well-funded industry groups are more likely to actively participate in multistakeholder processes. The description of multistakeholderism indicating that "everyone can have an equal seat at the table" may be true in theory but not necessarily in practice.[185] This is in addition to the insights of Raustiala, who posited that "U.S. interests in the Internet have in fact been well served by multistakeholder governance ... in which the key actors are disproportionately U.S.-based."[186]

Nevertheless, the multistakeholder process, or even "polycentric" governance, which is generally defined as multiple governing authorities with less hierarchical structure and a high degree of autonomy toward a variety of non-state actors,[187] marked a shift away from the top-down governance architecture toward a bottom-up approach that largely relies on voluntary commitments.[188] This trend toward greater polycentricity is primarily attributable to the need to respond to rapid technological changes. For the digital sectors, governments must govern alongside the private sector in a proactive manner in order to adequately drive cross-industry cooperation. As the ICT industry advocated, "polycentric partnerships" should represent the constituency of global governance in

[184] Shackelford, supra note 138, at 225–226, 256.

[185] Aleecia M. McDonald, "Stakeholders and High Stakes Divergent Standards for Do Not Track" in Evan Selinger et al. (eds) *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018), at 262.

[186] In Raustiala's view, "multistakeholder governance over the Internet has triumphed in large part because it reflects hegemonic power, not in spite of it." Kal Raustiala, supra note 167, at 502.

[187] See generally Rüdiger Wurzel et al., "Pioneers, Leaders and Followers in Multilevel and Polycentric Climate Governance" in Rüdiger Wurzel et al. (eds), *Pioneers, Leaders and Followers in Multilevel and Polycentric Climate Governance* (Routledge 2020), at 2–3.

[188] *Ibid.*

the digital sphere.[189] Individual states, although they continue to be functional components, do not play an exclusively dominant role when governing cyberspace. The reality is that cybersecurity certifications are becoming attractive mechanisms to promote a trustworthy digital ecosystem. In Japan, for example, the NIST Framework and the International Organization for Standardization (ISO) 27001 are complementary tools in governing cybersecurity,[190] with more and more companies turning to the NIST best practices as their cybersecurity standards.[191] The fact that the NIST Framework is globally applied indicates its potential to become a recognized baseline standard under international trade agreements and thus serve as an interoperability mechanism that facilitates cross-border data flows between divergent regulatory systems.

6.5.3 *The Role of (Trade) Multilateralism*

The ongoing shift to multistakeholderism raises pivotal questions concerning international norms development, namely: What is the appropriate role of states-based multilateral norm-setting in Internet governance? How can the WTO's governing function be sustained in the age of datafication? Can international trade agreements provide venues for digital trade dispute settlements regarding soft private standards created through multistakeholder mechanisms, especially the government-backed "voluntary" standards and certifications? More concretely, how can states be held accountable for unjustified barriers to digital trade when multilateralism and multistakeholderism combined shape the regulatory landscape of the digital economy?

To be sure, multilateral governance remains alive as the primary actor in world politics. The WTO has played and is expected to continue to play a useful role in international economic legal order. First, it is more empirically reasonable and economically justifiable to rely on multilateral approaches to safeguard the balance between the free flow of data and other legitimate public policies. On that premise, the role of the WTO in tackling excessive privacy standards or arbitrary cybersecurity risk

[189] The Internet Governance Forum (IGF), for example, brings various stakeholder groups together "as equals" to discuss Internet policy issues.

[190] Inside Cybersecurity "Japanese Industry Leader on Cyber: NIST Framework Increasingly Embraced Overseas" (July 25, 2017).

[191] NIST, "Cybersecurity Framework Success Story: Japan's Cross-Sector Forum" (2020).

assessment procedures would not be easily replaced. Ideally, a "blended governance regime" might occur when WTO trade tribunals exercise the power of review in the case of "unnecessary trade barriers." Certain industry-driven best practices or codes of conduct may be used as baselines in determining whether "less trade-restrictive measures" exist. As illustrated in the previous chapters, the necessity test – especially when operating in the context of "general exceptions"[192] – functions as the key mechanism in distinguishing between protectionist and non-protectionist trade-restrictive measures. In this context, soft private norms can be considered alternatives to state regulations under the necessity test. A trade tribunal can decide, for example, if certain privacy certifications are "less trade-restrictive measures" when compared with "hardish" state privacy laws. Toward that goal, a trade tribunal must consider if alternative, less trade-restrictive measures proposed by the complaining party are reasonably available and can achieve the desired policy goal of the responding party. Here, a complaining party might argue that an anonymization/de-identification certification granted by a trusted certification body or other credible industry self-regulating association is a less trade-restrictive alternative to data-restrictive measures. A complaining party might also propose self-certification programs as a feasible, less trade-restrictive alternative.[193] The responding party, on the other hand, may argue that private governance cannot achieve the equivalent level of protection that state regulation achieves.

Along this line of arguments, private cybersecurity standards appear to have the potential to compete with state regulations and thus constitute "less trade-restrictive alternative measures" in a trade dispute. Considering the global popularity of some cybersecurity certifications, it is not unimaginable that a trade tribunal might find certain information security testing and certifications representative of WTO-consistent measures which are reasonably available to the responding party and less trade restrictive than the state measures in dispute, and

[192] See Section 1.4.3 for more discussions. Note that some of the more recently concluded FTAs specifically record in the digital trade chapter that the general exceptions shall be interpreted "in a manner that takes into account the evolutionary nature of digital technology." See, for example, the EU–NZ FTA, Article 12.4 (Cross-border data flows).

[193] TADP, supra note 33. Like its predecessors, the Privacy Shield and Safe Harbor provisions, the new TADP Framework requires companies to self-certify their adherence to the Principles through the US Department of Commerce. See European Commission, "Trans-Atlantic Data Privacy Framework" (March 25, 2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100>.

which could also achieve an equal or higher level of contribution to the objective of protecting cybersecurity. In this way, soft private law norms visibly compete with state regulations – fighting for legitimacy under the multilateral regime.[194] Through multilateralism, the challenged protectionist measures of the responding party might eventually be substituted by "private norms" that are less trade restrictive.[195] In the long run, voluntary private schemes can serve as practical instruments for governments to "assure" compliance with trade rules.

Moreover, multilateral organizations such as the WTO can engage in the coordination of privacy and cybersecurity "international standards." Certain private schemes are highly influential and thus may constitute a "relevant international standard" within the meaning of WTO law. In terms of WTO litigation, technical standards are "rebuttably presumed" not to be more trade restrictive than necessary when they are in accordance with relevant "international standards" within the meaning of TBT Articles 2.4 and 2.5[196] or GATS Article VI:4/5.[197] In practice, when assessing whether a responding state's privacy or cybersecurity regulations constitute unnecessary barriers to trade, a trade tribunal should consider "international standards" established by "relevant international organizations."[198] Taking TBT Article 2.4 as an example, in *U.S. – Tuna II (Mexico)*, the Appellate Body confirmed that by virtue of Article 2.4, if a standard is found to constitute a "relevant international standard," WTO members are required to use it, or its relevant parts, as a basis for their technical regulations.[199]

It should be noted, however, that while the heart of the TBT Agreement is the adoption of international standards for the sake of trade liberalization, the TBT Agreement does not define the term

[194] Partiti et al., supra note 177, at 7.
[195] *Ibid.*
[196] According to Article 2.4 of the TBT Agreement, technical regulations that use international standards are presumed, subject to rebuttal, to be consistent with WTO obligations; on the other hand, the use of a standard that differs from the pertinent international standard may be challenged as an unnecessary trade barrier.
[197] See Aik Hoe Lim, "Trade Rules for Industry 4.0" in Shin-yi Peng et al. (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021), at 112.
[198] TBT Agreement, Article 2.4; GATS, Article VI:4/5.
[199] Appellate Body Report, *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products (US – Tuna II)*, WT/DS381/AB/R, May 16, 2012, para. 348.

"international standards" per se. The Appellate Body, in *U.S. – Tuna II*, stated that in order to constitute an "international standard," a standard must be adopted by an "international standardizing body" for the purposes of the TBT Agreement.[200] A "standardizing body" does not need to have standardization as its principal function, or even as one of its principal functions, as long as WTO members "have reason to expect that the international body in question is engaged in standardization activities."[201] In other words, such a "body" simply has to be "active in standardization," and WTO members are aware of the body's standardization activities.[202] One tricky issue here, under TBT Article 2.4 and GATS Article VI:4/5, is the requirement that the membership of the standardizing body must be open to "the relevant bodies of at least all Members of the WTO"[203] – which may be at odds with the characteristics of the multistakeholder process. It is worthy of special note that such a requirement has been reinforced in the recently developed WTO rules, including the "Six Principles"[204] created by the TBT Committee and the DR JSI. With respect to the former, international standards that are developed in line with the "Six Principles" are more likely to be considered "relevant international standards" within the meaning of the TBT Agreement.[205] However, the "Six Principles" explicitly indicate that "[m]embership of an international standardizing body should be open on a non-discriminatory basis to relevant bodies of at least all WTO Members." Similar wording can be found in the DR JSI.[206] If we follow the reasoning of the Appellate Body in *U.S. – Tuna II,* a body is "open" if membership to the body is not restricted; and it is not "open" if membership is *a priori* limited to the relevant bodies of only some WTO members.[207] On this point, it would be interesting to see whether the dispute settlement mechanism of the WTO provides sufficient incentives

[200] *Ibid.*, paras. 355–359.
[201] *Ibid.*, para. 362.
[202] *Ibid.*, paras. 360, 362.
[203] GATS, footnote 2: "The term "relevant international organizations" refers to international bodies whose membership is open to the relevant bodies of at least all Members of the WTO."
[204] WTO, "Principles for the Development of International Standards, Guides and Recommendations" <www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm>.
[205] Lim, supra note 197, at 112.
[206] WTO, "Declaration on the Conclusion of Negotiations on Services Domestic Regulation" WT/L/1129 (2 December 2021), at footnote 15.
[207] Appellate Body Report, *U.S. – Tuna II*, para. 364.

for multistakeholder bodies to be fully open to broader public actors, including state membership and ICT sectoral regulators.

In addition to international trade litigation, a more ambitious path is to incorporate multistakeholder standards into international economic law through trade negotiations. In light of this, leading scholars in the field have different candidates in mind. Chander and Schwartz advocate that the Global Privacy Assembly[208] should be able to develop substantive international standards including a set of global privacy norms, just as the Codex Alimentarius Commission set the international standards for food safety.[209] Kulesza and Weber, however, are of the view that among the existing venues, the Internet Corporation for Assigned Names and Numbers (ICANN) seems best equipped to fuel further discussion on relevant standards and offer possibilities for a more harmonized international framework.[210]

6.6 Conclusion

Admittedly, international economic law alone is not adequate in light of concerns surrounding privacy and cybersecurity governance. The global governance architecture of cross-border data flows therefore calls for the "variable geometry" model, which integrates different components of approaches and instruments. Multistakeholderism and multilateralism – at least when it comes to data flow governance – do not have to be two parallel paths. A "right" balance between the free flow of data and other legitimate objectives might never be found, but a more properly balanced approach may be possible if each role and its momentum in the public and private sectors can be reconfigured and restored.

[208] Global Privacy Assembly (GPA) <https://globalprivacyassembly.org/>.
[209] Anupam Chander and Paul Schwartz, "Privacy and/or Trade" (2023) 90(1) University of Chicago Law Review 49.
[210] Joanna Kulesza and Rolf H. Weber, "Protecting the Internet with International Law" (2021) 40 Computer Law & Security Review 1, at 4.