Portable Trust: Fostering Both Autonomy and Privacy in Data Portability Mechanisms

Cobun Zweifel-Keegan[1]

February 27, 2024

I. Introduction

This policy brief provides an examination of the principle of data portability, a data protection right that has been increasingly recognized and codified in privacy laws worldwide. While not universally mandated, data portability is a critical tool for empowering individuals by giving them control over their personal data. However, achieving true portability is not without its challenges, as it can introduce significant privacy, security, and integrity risks. To mitigate these risks and foster trust in the process of data portability, the implementation of consistent operational, technical, and legal safeguards is essential. This requires prioritization of this data right within privacy programs—a portability by design approach—as well as collaborative engagement between platforms as opportunities for portability mature. This brief delves into each of these aspects, providing an overview of the complexities of achieving the promise of data portability from a privacy perspective, along with best practices to meet the challenge.

II. Data portability is a longstanding principle of data privacy.

The idea of data portability as a privacy right is often portrayed as a relatively recent innovation. This is mostly true. The European Union's General Data Protection Regulation (GDPR) was the first, in 2016, to add this right among the bundle of data protection rights data subjects enjoy across the EU.[2] But data portability has its roots in fundamental principles of data privacy going back to the first codes of practice.

More than fifty years ago, the Fair Information Practice Principles (FIPPs) were the first attempt to capture the principles and processes that should be supported when creating computerized

---

[1] Cobun Zweifel-Keegan is a privacy lawyer who serves as the Managing Director, Washington, D.C. for the International Association of Privacy Professionals. This policy brief is an individual research project and does not reflect the opinions of the IAPP or any other organization. This paper was produced with the support of the Data Transfer Initiative: https://dtinit.org/.

[2] The GDPR reflected a similar right to data portability that was incorporated into France's Digital Republic Act of 2016. As early as 2011, the U.K. government pioneered its "midata" program to encourage the development of intra-company portability standards and processes. *See,* Kaori Ishii, Discussions on the Right to Data Portability from Legal Perspectives, IFIP ADVANCES IN INFO. & COMM'N TECH. VOL. 537 (2018), https://link.springer.com/chapter/10.1007/978-3-319-99605-9_26.

systems storing the personal data of many individuals.[3] That is, they were the first attempt to promulgate best practices for the nascent field of data privacy, known in other jurisdictions as data protection. Over the years, many different versions of the FIPPs have been put forward, but even the first report by the U.S. Department of Health, Education, and Welfare included among its principles the idea that "there must be a way for an individual to find out what information about him is in a record and how it is used."[4] In other versions of the FIPPs, this principle was broadened and referred to, generally, as "individual participation" or—perhaps more generously—"individual control."[5]

Control and participation privilege the idea of consent, when relevant, but also provide an umbrella under which the broad rights of access, correction, and redress are captured. All these separate rights are commonly reflected across privacy laws and codes—and have been continuously and with increasing sophistication for five decades.

To understand the unique elements of the right to data portability, one must first understand the much older right of access to personal data. The two rights bear much in common. (See *Figure 1*, below, for a comparison.) After all, they are both designed to empower individuals to exercise control over their personal data by receiving a copy of their data from an organization. Some privacy and data protection laws consider portability a special type of access, while others treat it separately as a standalone right.

FIGURE 1: ACCESS AND PORTABILITY AT A GLANCE

	Access	**Portability**
Definition	Allows individuals to obtain a copy of their personal data held by an organization.	Enables individuals to receive their data in a structured, machine-readable format and transfer it to another service provider.
Purpose	Helps individuals understand data processing, verify accuracy, and exercise other rights.	Facilitates switching services, promoting user autonomy and a competitive marketplace.

[3] For a brief overview of the history and importance of the FIPPs to the field of data privacy, see Cobun Zweifel-Keegan, *A view from DC: Celebrating privacy's 50th birthday*, IAPP: U.S. PRIVACY DIGEST, June 30, 2023, https://iapp.org/news/a/a-view-from-dc-celebrating-privacys-50th-birthday/.

[4] U.S. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), https://aspe.hhs.gov/reports/records-computers-rights-citizens.

[5] *See, e.g.*, U.S. DEPARTMENT OF HOMELAND SECURITY, THE FAIR INFORMATION PRACTICE PRINCIPLES (2015), https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

Scope	Pertains to the individual's own data within a specific organization.	May extend beyond individual access, allowing data to move directly between services on request.
Example	Requesting medical records from a hospital.	Transferring contact lists from one social media platform to another.

In addition to encouraging respect for consumers' requests to access personal data in codes like the FIPPs, the right of access is enshrined in the Charter of Fundamental Rights of the European Union, which lies at the foundation of EU law. Access and rectification are the only practical rights related to personal data explicitly listed in the Charter. Access is often described as the "gateway" to other privacy rights. Requesting access to one's personal data enables an individual to better understand the extent to which an organization is processing information about them, which can enable further requests, such as correcting an incorrect record or deleting it entirely.

Portability goes one step farther, enabling the individual to exercise their autonomy over their own personal data, including in ways that do not serve the interests of the platform with which they are interacting. It is not by accident that portability requirements include language about the usability of data. When fully achieved, data portability empowers individuals to make use of their own data without regard to the whims of platforms. It thus could be considered the culmination of rights related to the autonomy of the data subject.

III. Data portability is widely—but not universally—required under privacy law.

It is important to stress the fact that data portability is an independent data protection right, separate and apart from its operation as a pro-competitive regulatory measure. In fact, in its guidance on the subject, the European Data Protection Board takes pains to highlight this fact: "Whilst the right to personal data portability may also enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition. In particular, article 20 does not limit portable data to those which are necessary or useful for switching services."[6]

Though data portability is brought up most frequently in the context of social media, communications, or personal tracking data, the right is not explicitly limited to any personal data types.[7] However, the right to data portability is not universally applicable under data protection or consumer data privacy laws.

---

[6] Article 29 Data Protection Working Party, Guidelines on the right to data portability at 4, 13 Dec. 2016, https://ec.europa.eu/newsroom/article29/items/611233.

[7] Sasha Hondagneu-Messner, *Data Portability: A Guide and a Roadmap*, 47 RUTGERS COMPUTER & TECH. L.J. 240, 249 (2021).

Artful legal drafting limits the obligation to respect data portability requests to those situations where it is already "technically feasible" to provide a structured, commonly used, machine readable format. This is the case in most U.S. state privacy laws, which recognize the right alongside the simple right of access.[8] (See *Figure 2*, below, for example language from California and Colorado.) Although the GDPR's recitals includes lofty language that companies "should be encouraged to develop interoperable formats that enable data portability," it also limits portability to what is technically feasible, but only for the component of the regulation that requires direct transfer of data between controllers.[9] The technically feasible exception does not apply to individuals' direct download requests under GDPR.

***FIGURE 2:** COMPARING PORTABILITY RIGHTS ACROSS A SELECTION OF PRIVACY LAWS*

	Legal Text	**Primary Guidance**
EU General Data Protection Regulation	**Article 20:** ***Right to data portability*** 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and b. the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public	**Recital 68:** To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract.… The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in

[8] For an up-to-date listing of U.S. state privacy laws tracking their inclusion of portability requirements, see International Association of Privacy Professionals (IAPP), U.S. State Privacy Legislation Tracker, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. For an in-depth comparison of the portability requirements across U.S. states (and beyond), see Delara Derakhshani, *Global developments in data portability law*, Data Transfer Initiative, Oct. 25, 2023, https://dtinit.org/blog/2023/10/24/global-developments.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such
data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, at Recital 68.

	interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	accordance with this Regulation.… Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.
California Consumer Privacy Act, *as amended by* California Privacy Rights Act	**Calif. Civil Code Sec. 1798.130** (a) … a business shall, in a form that is reasonably accessible to consumers: … (3)(B) For purposes of [the business's obligation to disclose information about a consumer in response to a verifiable consumer request under the Right to Access] (iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.	**CPPA Regulations Section 7024** (g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.
Colorado Privacy Act	**C.R.S. § 6-1-1306** (1)(e) *Right to data portability.* When exercising the right to access personal data pursuant to subsection (1)(b) of this section, a consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year. Nothing in this subsection (1)(e) requires a controller to provide the data to the consumer in a manner that would disclose the controller's trade secrets.	**CPA Rule 4.07** A. To comply with a data portability request, a Controller must transfer to a Consumer the Personal Data it has collected and maintains about the Consumer through a secure method in a commonly used electronic format that, to the extent technically feasible, is readily usable and allows the Consumer to transmit the Personal Data to another entity without hindrance. B. Pursuant to C.R.S. § 6-1-1306(1)(e), a Controller is not required to provide Personal Data to a Consumer in a manner that would disclose the Controller's trade secrets. When complying with a request to access Personal Data in a portable format, Controllers must provide as much data as possible in a portable format without disclosing the trade secret.

The GDPR further limits the applicability of the right to data portability in three ways. First, the right is limited to those situations where data is processed subject to the legal bases of consent or contract. This leaves four other legal bases, including the widely used "legitimate interests" basis, under which an organization may legally process personal data without any obligation to respect individual requests for a portable copy of personal data. In contrast, U.S. state laws do not reflect this same limitation.

In addition, the GDPR generally limits the operation of data protection principles if they conflict with other fundamental rights or interests. Risks to the privacy or other rights of the requesting individual or others could override the right to data portability in certain circumstances.[10]

Finally, the GDPR and some—but not all—of the laws it inspired limit the scope of the right to data portability to data collected from the individual. That is, personal data about an individual that is not directly collected from them may not be required to be included in a portable form, whether collected from another source, created through the operation of the service, or inferred from other data. Such data may be worth considering as includable in portability requests, however, if the individual is likely to expect its inclusion. Furthermore, some U.S. state privacy laws do not include limiting language about the source of the data (see, e.g., Colorado above).[11]

IV. Portability supports individual empowerment.

European jurisprudence considers the framing of "informational self-determination" as core to data protection rights. In 1983, the German Constitutional Court ruled that whoever "cannot survey with sufficient assurance the information concerning himself known in certain areas of his social surroundings, and whoever is not in a position to assess more or less the knowledge of possible partners in communication, can be essentially obstructed in his freedom to make plans or decisions on the basis of his own self-determination."[12]

Whether framed in language about participation, agency, control, or autonomy, data rights like the right of access help to empower individuals to gain knowledge about the spread of their personal data and power over how it is collected, used, and shared. The right to data portability relies on this same philosophical underpinning.

As the EDPB explains in its portability guidance, "This right… supports user choice, user control and user empowerment.… By affirming individuals' personal rights and control over the personal data concerning them, data portability also represents an opportunity to 're-balance' the relationship between data subjects and data controllers. The primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem."[13]

---

[10] *See*, *id.*, Section III.

[11] For other states, see also IAPP, *supra* note 8.

[12] For an explanation of the importance of the *Karlsruhe* case and the reasoning behind data portability in the European context generally, *see* Gabriela Zanfir-Fortuna, *The right to data portability in the context of the EU data protection reform*, INT'L DATA PRIVACY L. (May 11, 2012) at 149, https://ssrn.com/abstract=2215684.

[13] Article 29 Data Protection Working Party, *supra* note 6 at 3-4.

Nevertheless, portability has to date been the least exercised and developed right under the GDPR.[14] This is evidenced by the lack of notable developments regarding the right to data portability, such as supervisory enforcement or case law. Most jurisdictions reported no significant developments, and data portability rarely seems to be used by data subjects or debated before a court. Research also shows confusion and a lack of regularity in responses to portability requests.[15] This contrasts with other rights, such as the right to access, which data subjects have frequently relied on, resulting in a broad catalog of jurisprudence. As for case law in the EU about the right to data portability, there have been very few, if any, cases.

V. Porting data has inherent privacy, security, and integrity risks.

The philosophy of individual empowerment undergirds the right to data portability whether it is exercised by an individual requesting direct access to machine-readable data (a "direct-download scenario"), or via a controller-to-controller transfer request. However, these two distinct methods of exercising portability may both present privacy and security risks to individuals, organizations, and third parties (see *Figure 3*, below). In fact, some scholars have critiqued the right to data portability as inherently not worth the risks and drawbacks.[16]

When an individual exercises their right to direct access to machine-readable data, they may encounter security and privacy risks. Securely transferring large volumes of data can be a complex task, and any breach during this process could expose sensitive information. Individually processing or accessing the requested data may require users to download software, a further security threat. Ongoing risks of breach from improper storage or re-upload to unverified destinations make the direct download scenario riskier for individuals.

Conversely, when data portability is exercised via a transfer request, where data is transferred directly from one controller to another, a different set of risks emerges. The primary risks for controllers sharing data include the failure to inform individuals about how their data will be processed, collecting personal data for one purpose and subsequently sharing or using it for another incompatible purpose without the data subject's consent, and the inability within receiving platforms to maintain the integrity and security of the data. Moreover, cross-border data transfers can introduce complexities.

---

[14] Jurre Reus & Nicole Bilderbeek, Data portability in the EU: An obscure data subject right, IAPP: PRIVACY PERSPECTIVES, Mar. 25, 2022, https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/.

[15] *See, e.g.*, Janis Wong and Tristan Henderson, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, INT'L DATA PRIVACY L. (July 6, 2019) at 173, https://academic.oup.com/idpl/article-abstract/9/3/173/5529345.

[16] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD L. REV. 335 (2013), https://fpf.org/wp-content/uploads/2013/07/Swire-Lagos_Why-the-Right-to-Data-Portability-Likely-Reduces-Consumer-Welfare1.pdf (exploring a variety of critiques of the idea data portability before passage of the GDPR, including the lack of focus on market power and inherent privacy and security risks from operationalizing the right).

Only by considering these concerns and implementing appropriate safeguards throughout the data lifecycle can portability mature as a practice and earn the trust of consumers. Trust in the process of exercising portability requires efforts to build trusted privacy practices within individual companies, but efforts must not stop there. Multi-party efforts must also be made, within domains of specific data uses (e.g., fitness trackers, social graphs), to build trust in the general process of portability. Truly portable trust, as this could be called, is an ideal that has yet to be realized in most domains.

FIGURE 3: RISK CONSIDERATIONS FOR DATA PORTABILITY			
	Risk to Organization	**Risk to Individual**	**Risk to Others**
Verification	Misidentification of data subject can result in exposure.	Verification often requires sharing of personal information, plus exposure risk.	
Scope	Over- or under-inclusion of personal data.	Mismatch between expectation and reality for extracted data. Usability concerns may vary.	Other individuals may have personal data included.
Transfer	Security risks of extracting and transferring a large file. Compliance risks for cross-border transfer.	Higher risk of exposure during transfer, whether through direct download or B2B.	Receiving platform may take control of data at a high-risk time, integrating datasets can cause corruption.
Storage	Duplicated dataset is outside of scope of control for privacy and security safeguards.	Ill-equipped to store data in a secure and privacy-preserving way.	Receiving platform may have different privacy / security posture with incompatible fields.
Re-use	Purpose limitations and sharing provisions of privacy policy may not be met for ported data.	When porting to new platform, may not be aware of different privacy considerations.	Receiving platform may not be aware of limitations or irregularities in dataset, can fail to maintain integrity.

VI. Portable trust and privacy require consistent safeguards.

Though portability has not been top-of-mind for regulators since its introduction as a privacy right, the tide is already shifting as data protection standards continue to mature—and other regulatory frameworks draw attention to data portability.[17] As with any privacy practice, organizations that under-invest in portability processes now may find themselves paying higher costs to adjust systems later.

[17] *See*, Chris Riley & Delara Derakhshani, *Future Horizons for Data Portability Research*, TECH POL. PRESS, Sept. 28, 2023, https://www.techpolicy.press/future-horizons-for-data-portability-research/.

Unlike the closely linked idea of interoperability, portability can be initiated on a unilateral basis.[18] But unilateral mechanisms, such as portals and direct downloads, bring with them the heightened risks to the security and privacy of the data explored above. On the other hand, bilateral and multilateral efforts to build uniform standards and technical systems for translating datasets between platforms can be expensive without eliminating risks.

Nevertheless, a principles approach to data privacy should encourage organizations to consider portability measures, especially for data types for which user autonomy and empowerment are most likely to be reflected. For example, today's computer users have come to expect the ability to maintain control over their communications, their social graph, the content they produce, and longitudinal insights about themselves driven by sensors such as fitness monitors. When physical analogues exist over which consumers are familiar taking an ownership interest, their privacy expectations around the portability of their data away from platform control are likely to be correspondingly high.

Organizations are well advised to consider both compliance and consumer trust goals in developing robust portability mechanisms. Achieving such measures first requires internal investment, even before multilateral challenges are addressed. Thus, privacy programs should implement operational, technical, and legal safeguards that consider portability throughout the data lifecycle. The costs of re-architecting systems to allow for portability can be much higher than designing them with portability in mind from the beginning. A much-cited example is the $3 billion price tag that U.S. telephone carriers spent in re-architecting systems to allow for phone number portability between operators.[19]

For those systems that users are likely to view through a lens of their own autonomy as stewards of their data, and those systems that users invest significant time or energy in curating, organizations should consider portability as early as possible in the design and engineering process. This "portability by design" approach should embrace efforts across operational, legal, and technical controls.

Portability by design involves architecting systems from the outset to support data portability, thereby embedding this right into the very fabric of the system's design and operation. Doing so ensures that data portability is not an afterthought but a fundamental aspect of the system, thereby reducing potential risks and enhancing the security and privacy of data subjects. This proactive approach can help mitigate potential vulnerabilities, enhance data integrity, and foster greater trust among data subjects.

---

[18] Sukhi Gulati-Gilbert and Robert Seamans, Data portability and interoperability: A primer on two policy tools for regulation of digitized industries, Brookings, May 9, 2023, https://www.brookings.edu/articles/data-portability-and-interoperability-a-primer-on-two-policy-tools-for-regulation-of-digitized-industries-2/.

[19] Joshua Gans, Stephen King, and Graeme Woodbridge, *Numbers to the people: regulation, ownership and local number portability*, 13 INFO. ECON. POLICY 167 (2001).

Operational and legal safeguards are the first line of defense. These are the written policies, procedures, and practices that organizations put in place to ensure secure and efficient data portability. For instance, organizations need to establish clear protocols for recognizing and processing data portability requests, and for determining the scope of the data that will be subject to each type of portability request.[20] User education is another vital operational concern, especially when providing users with an opportunity to download large quantities of raw data. Warnings about the security and privacy risks should be coupled with information about properly vetting third-party platforms and securely storing data.

Fully implementing operational controls also requires technical expertise. Technical safeguards include those mechanisms that enable trusted verification of data requestors, secure transmission of personal data, and encrypted file types to facilitate secure storage. In its portability guidance, the EDPB provides an overview of a lengthy but non-exhaustive list of possible technical mechanisms to consider in facilitating portability, including "secured messaging, an SFTP server, a secured WebAPI or WebPortal" in addition to the possibility of facilitating data subjects in their use of a "data store, personal information management system or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required."[21]

The last factor to consider when embracing data portability—but far from the least important—is participation in multilateral mechanisms to support safe and trustable transfers of data in ways that reduce friction, increase usability, and mitigate user-driven risks. Like other systems that benefit from, but do not require, multi-party collaboration, portability mechanisms can be more trusted and long-lasting through intervention by trusted third-party actors.

Multilateral mechanisms can take a variety of forms with various levels of formality. Associations or other independent intermediaries can encourage or even directly shape the continued investment in portability resources and interoperable systems. Governmental and non-governmental actors can craft standards and protocols for nascent technical systems to move beyond proprietary, siloed mechanisms. Independent bodies can also serve as outside verifiers of portability, through the creation of recognized trust marks or certifications that would verify compatibility with best practices.[22] At the far end of formalized mechanisms,

[20] See the guidance from the U.K. data protection authority for a detailed description of some of these measures. U.K. Information Commissioner's Office, *Right to data portability*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/.

[21] Article 29 Data Protection Working Party, *supra* note 6 at 16.

[22] For a review of the factors that contribute to robust independent accountability mechanisms, see BBB National Programs, filed comment in response to NTIA request for comments on artificial intelligence system accountability measures and policies, FR Doc # 2023-07776, June 12, 2023, https://www.regulations.gov/comment/NTIA-2023-0005-1158.

multilateral governance structures can facilitate ongoing interoperable frameworks for portability, which can have knock-on effects for driving value in the marketplace.[23]

VII. Conclusion

Much work is still needed to achieve the goals of autonomy, consumer empowerment, and self-determination that lie beneath the privacy interests in data portability.

The successful implementation of data portability hinges on a concerted effort from companies to invest resources in internal portability initiatives. This includes the development of robust systems and processes that facilitate secure and efficient data transfer consistent with a holistic privacy program. However, internal efforts alone are not sufficient. Companies must also actively engage in multilateral or multistakeholder mechanisms that foster collaboration, standardization, and mutual understanding among different actors in the data ecosystem. Furthermore, companies that support the goals of portability should support the creation of new mechanisms that address emerging challenges and opportunities—or incorporate new technical modalities—while fostering trust in the broader portability landscape.

A multifaceted approach is crucial for overcoming the complexities of data portability and for realizing its full potential in empowering individuals and fostering a competitive user-centric marketplace.

[23] For a discussion of multilateral governance structures, *see* Sukhi Gulati-Gilbert and Robert Seamans, *supra* note 18.