Computer & Communications
Industry Association
Tech Advocacy Since 1972

August 21, 2020

*Via Email: DataPortability@ftc.gov*

Federal Trade Commission, Office of the Secretary
Constitution Center, 400 7th St., SW
5th Floor, Suite 5610
Washington, DC 20024

**Re: FTC Data Portability Workshop Comments**

Pursuant to the request for comments[1] issued by the Federal Trade Commission (FTC or the Commission), the Computer and Communications Industry Association (CCIA) submits the following comments on the subject of data portability, in preparation for the Commission's upcoming "Data to Go" public workshop.

CCIA is an international, non-for-profit association representing a broad cross section of computer, communications and Internet industry firms. CCIA remains dedicated, as it has for over 40 years, to promoting innovation and preserving full, fair and open competition throughout our industry. Our members employ more than 1.6 million workers and generate annual revenues in excess of $870 billion.[2]

CCIA commends the Commission for organizing the forthcoming workshop on data portability and for its deliberative framing of the topic. As the Commission's workshop announcement notes, data portability raises potential benefits and challenges to both consumers and competition.[3] Ensuring that data portability proposals maximize benefits to a broad range of stakeholders requires recognizing and balancing inherent trade-offs between intersecting interests. Therefore, voluntary, open-source, standards-based data portability initiatives focused on improving users' ability to access and transfer their information as they deem appropriate will provide the greatest benefit to consumers, service providers, and the wider digital ecosystem through improved convenience, competition, and innovation.

---

[1] Federal Trade Commission, "Data to Go: An FTC Workshop on Data Portability" (Mar. 31, 2020), https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.
[2] A list of CCIA members is available at http://www.ccianet.org/members.
[3] Federal Trade Commission, "FTC Announces September 22 Workshop on Data Portability" (Mar. 31, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/ftc-announces-september-22-workshop-data-portability.

The following sections respond to specific questions posed in the Commission's request for comments.

**Question #1: How are companies currently implementing data portability? What are the different contexts in which data portability has been implemented?**

Data portability tools exist on a spectrum of varying levels of coordination between the organizations transferring and receiving transferred data.[4] This is illustrated by the European General Data Protection Regulation (GDPR)'s right to data portability that includes both a data subject's "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 the "right to have the personal data transmitted directly from one controller to another, where technically feasible."[5] The broad spectrum of transfers that commonly fall under the umbrella term of "data portability" require different technical standards to implement and present unique risks and opportunities.

Transfers at the low end of the data portability complexity spectrum include providing a consumer with personal data in a machine-readable format for either their own use or for re-uploading to another service. Since the early 2010s, many data controllers have operated access portals that allow users to request and download their personal information.[6] In recent years, there has also been an increase in privacy technology vendors that market the ability to automate responses to data subject access requests by providing data mapping and discovery services.[7] For some organizations, adopting automated systems enabling data downloads may not be practical or efficient and instead these organizations elect to receive and respond to user data access requests through electronic communications and to manually process individual requests.

Data portability tools at the high end of the complexity spectrum include user directed, machine-to-machine transfers of information between services according to agreed-upon protocols and policies. In 2018, several companies launched the Data Transfer Project (DTP), an open-source effort to connect the APIs of different digital services to enable securely encrypted transfers of data initiated by users between participating organizations.[8] Through work with the DTP, Google and Facebook recently launched tools that allow users to direct the transfer of

---

[4] *See* Erin Egan, "Data Portability and Privacy: Charting a Way Forward," Facebook (Sept. 2019), at 9-13, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.
[5] General Data Protection Regulation, Art. 20, "Right to Data Portability."
[6] Anna Barker, "Consumer Data Rights and Competition," OECD (Apr. 29, 2020), at 44, https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.
[7] International Association of Privacy Professionals, "2020 Privacy Tech Vendor Report" (Apr. 15, 2020), at 27, https://iapp.org/media/pdf/resource_center/2020TechVendorReport.pdf.
[8] Data Transfer Project, "Overview and Fundamentals" (July 20, 2018), https://datatransferproject.dev/dtp-overview.pdf.

uploaded photos and videos to an associated account with another service (Facebook to Google, Google to Flickr).[9] This example demonstrates the potential for the technology underlying the DTP to enable data portability transfers across a wide array of use cases, although continued success will depend on adoption and good faith participation by services of all sizes.

**Question #2: What have been the benefits and costs of data portability? What are the benefits and costs of achieving data portability through regulation?**

Benefits of Data Portability

The users of data-enabled services stand to benefit from the balanced development of data portability mechanisms by enjoying reduced transaction costs to moving between services. Manually re-entering and re-uploading personal information, images, and content for each additional e-commerce site, streaming service, or fitness tracker that a consumer might be interested in using can be daunting and may contribute to 'lock-in' effects within a sector. An ecosystem of services that provides users with well-implemented tools for accessing and transferring personal data can ensure that consumers are able to use the services that are most appropriate for their needs. Data portability can also support individuals' data control and security by helping users organize and back up their personal information as well as recover in the event of a data breach or account takeover.

Balanced and reciprocal data portability mechanisms can also provide for economy-wide benefits to competition and innovation. Increasing the ease by which users can move between services promotes competition between businesses on attributes such as quality, cost, and availability of privacy-enhancing features. Furthermore, by enabling services to rapidly scale-up their user base through data transfers, portability mechanisms can encourage increased investment and market entry from both competitors and developers of complementary services. Finally, data portability can support innovation in a sector by enabling the development of new services or insights based on the analysis of ported data.[10]

Data Portability Risks

Without appropriate safeguards and flexibility in deployment, data portability requirements may increase risks of consumer harm. Any transfer of personal information, either to a user or between services, presents inherent privacy and security risks. Therefore, it is

[9] Steve Satterfield, "Driving Innovation in Data Portability With a New Photo Transfer Tool," Facebook (Sept. 2, 2019), https://about.fb.com/news/2019/12/data-portability-photo-transfer-tool.
[10] *See* datum future, "Data Portability: What is at stake?" (July 2019), at. 12, https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf.

necessary to develop standards for verifying the authenticity of transfer requests to prevent users' personal data from being stolen by scammers spoofing a legitimate service. If data is transferred pursuant to a fraudulent portability request, a user may be at risk of repeated breaches across accounts on separate services.

The potential privacy and security risks of data portability is broader than the facilitation of inappropriate access. Personal information sought by a user for transfer may relate to multiple additional individuals, implicating the privacy interests of third parties. Additionally, from an operational perspective, requirements to retain data in an identifiable format for the sole purpose of enabling future portability is contrary to the principle of data minimization and would raise security concerns.

The establishment of mandatory data portability frameworks may also negatively impact competition and innovation priorities. For example, obligations to develop and deploy portability mechanisms could create compliance costs that advantage incumbents over smaller competitors and establish new barriers to market entry.[11] Furthermore, if data transfer mandates were extended to analytic information and insights generated by an organization, portability could allow some companies to free ride on the efforts of others, thereby chilling the incentive to develop new innovative services.

Promoting Data Portability

The federal government has a significant role to play in supporting the development and implementation of data portability mechanisms that will benefit consumers while mitigating potential drawbacks. However, data portability mandates or regulations that attempt to set strict requirements and procedures for achieving data portability are likely to produce significant downsides. Furthermore, considerations of data portability as a remedy to promote competition should always be tailored to what is technically feasible, including the recognition that accurately incorporating new data sets into separate systems may not always be possible.[12] Recital 68 of the GDPR seeks to strike this balance by providing that "[d]ata controllers should be *encouraged* to develop interoperable formats that enable data portability" but that the right of data portability "should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible."[13]

[11] Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 Md. L. Rev. 335, 356 (2013).
[12] datum future, *supra* note 10, at 13.
[13] GDPR, Recital 68 "Right of Data Portability."

Data portability mandates that set overly prescriptive requirements could also preference particular technologies, protocols, and data formats, thereby hindering innovation and continued multi-stakeholder development of effective data portability tools.[14] A "one-size-fits-all" portability mandate would also be unable to account for differences in how data is maintained and managed in different sectors and between different companies, raising the prospect of increasing costs while failing to respond to the specific needs of a sector. Finally, rather than promote competition, mandatory data portability between services could increase the risk of collusion when competitors are required to collaborate and share information.

There are several concrete steps that the government can take to promote the development and adoption of balanced data portability mechanisms. For example, continuing to make open government data available will provide a template for data portability in the private sector in addition to spurring research and innovation.[15] Furthermore, the government can employ its power to raise public awareness and convene stakeholders to aid the development of industry-wide best practices. Ultimately, successful data portability tools are best developed through open, consensus-based standards in response to consumer interests and needs that (1) allow users to receive or transfer data that they have directly provided to a service, (2) afford consumers control over how and when portability tools are used, and (3) are tailored to the privacy and security expectations of specific products, services, and sectors.

**Question #3: To what extent has data portability increased or decreased competition?**

Research shows that facilitating users' access to their own data online can benefit consumers and the wider digital ecosystem through increased competition and innovation.[16] Prior data portability efforts in distinct sectors have produced positive effects on competition. For example, the Federal Communications Commission's Wireless Local Number Portability rules led to companies competing to offer deals on phones and services at lower prices.[17] In the United Kingdom where an Open Banking data portability initiative is currently underway, a 2019 industry survey of senior finance, payments, and product professionals found that 79% of

[14] *See* Michal Gal & Daniel Rubinfeld, "Data Standardization," 94 NYU L. Rev. 738, 753, (2019) (explaining the risks of lock-in to an inefficient data standard).
[15] *See, e.g.,* Executive Order 13642, "Making Open and Machine Readable the New Default for Government Information" (May 15, 2013), https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13642.pdf.
[16] *See* Barbara Engels, "Data portability among online platforms," Internet Policy Review (June 11, 2016), https://policyreview.info/node/408/pdf.
[17] *See* Nicole B. Stach, "Wireless Local Number Portability and Its Effect on Competition: Can There Be Too Much of a Good Thing?" 12 CommLaw Conspectus 223, 242 (2004).

respondents "were certain their company is planning to use Open Banking services and are ready to do so."[18]

For the reasons described, data portability initiatives have clear potential to increase competition among established players as well as support market entry. However, policymakers should not expect uniform competitive results from data portability initiatives across sectors. The competitive impact of increasing the availability and transferability of users' information is context-dependent, and will vary based on both the existing ease of switching services for consumers and the ability for receiving organizations to make use of ported data within a particular sector.[19]

Finally, data portability should not be considered solely as an external factor to competition in a sector, but also as a product of competition between firms.[20] Organizations compete to make their services more appealing to consumers by developing ways to give greater transparency and control over their personal data. Offering services with built-in portability options are likely to be more attractive to consumers and can help a service gain a competitive advantage in the marketplace.

**Question #4: Are there research studies, surveys, or other information on the impact of data portability on consumer autonomy and trust?**

CCIA is not aware of existing research on the specific impact of data portability on consumer autonomy and trust. However, data portability is often paired with additional information and choices for data subjects, such as processing transparency and the ability to access, correct, and delete personal information, that are aimed at giving consumers more control over their personal information.[21] Consumer surveys and research support the proposition that increasing user control with respect to data processing supports autonomy and can increase individuals' willingness to engage with a service.[22]

---

[18] Nuapay, "Open Banking World Series Edition 1: UK and Ireland" (June 2019), at 10, https://www.nuapay.com/wp-content/uploads/2019/09/OB-world-series.pdf.
[19] *See* Catherine Tucker, "Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility," 54 Rev. Ind. Organ., (2019), at 8-11.
[20] *See* Thomas M. Lenard, "If Data Portability is the Solution, What's the Problem?" Tech Policy Institute (Jan. 2020), at 3, https://techpolicyinstitute.org/wp-content/uploads/2020/01/Lenard_If-Data-Portability.pdf.
[21] *See* Laura Jehl & Alan Friel, "CCPA and GDPR Comparison Chart," Baker Hostetler LLP (2018), https://bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.
[22] *See, e.g.*, Timothy Morey, Theodore Forbath, & Allison Schoop, "Customer Data: Designing for Transparency and Trust," Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust; Jay Kesan, Carol Hayes, & Masooda Bashir, "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy" 91 Indiana L.J. 267 (2016).

The impact of increasing control over user data may also vary between different sectors, legal regimes, and across different cultural contexts.[23] For example, in the Europe, the right to data portability is often discussed in terms of user "empowerment,"[24] and "informational self-determination."[25] Therefore, it is important to develop data portability frameworks with a primary focus on user interests and practical use cases.

In order for data portability initiatives to best support user autonomy, data transfers should be explicitly directed by users on the basis of free and informed consent. Standards for providing transparent information and receiving consent may therefore vary between different data portability contexts. For example, informed consent for a one-time transfer of historic information between services may look different from consent for establishing periodic transfers as additional data is provided or collected. Another issue is the possibility that products or systems may be developed that include defaults in favor of portability or 'nudges' that pressure users to initiate transfers from other services.[26] Therefore, stakeholders should continue to explore how user autonomy can be supported in different data portability contexts.

**Question #5: Does data portability work better in some contexts than others (e.g., banking, health, social media)? Does it work better for particular types of information over others (e.g., information the consumer provides to the business vs. all information the business has about the consumer, information about the consumer alone vs. information that implicates others such as photos of multiple people, comment threads)?**

Portability in Different Contexts

It will not necessarily clear whether or not a data portability project is working in a particular context. As discussed, data portability initiatives can be taken in pursuit of a range of public policy outcomes including encouraging consumers to switch between services, promoting innovation in a sector, and encouraging market entry. Therefore, evaluating whether a data portability project is working requires stakeholders to have reached agreed-upon goals and metrics for measuring outcomes.

[23] *See* Vishal Midha, "Impact of consumer empowerment on online trust: An examination across genders" 54 Decision Support Systems 198, (Dec. 2012).
[24] Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" (Apr. 5, 2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[25] *See* Eva Fialová, "Data Portability and Informational Self-Determination" 8 Masaryk U. J.L. & Tech. 45 (2014).
[26] Anne Riechert,"Data Portability - Policy Paper" Stiftung Datenshutz (May 22, 2020), at 7, https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/SDS_Datenportabilitaet-PolicyPaper2020-05-22_EN.pdf.

Individual sectors of the economy have distinct characteristics that must be accounted for in the development of data portability proposals. For example, the extent to which data can be accurately received and utilized by an organization without the development of new data adapters and standards will vary based on existing data collection and management practices within an industry.[27] It is also important to consider consumer behavior and service provision in a sector in developing data portability goals, such as whether services are exclusive and rivalrous (such as in energy and telecommunications) or commodified and homogenous (such as financial services).

Specific considerations for encouraging data portability initiatives in particular contexts are included in the Australian Consumer Data Right, an ongoing process to introduce data portability to the banking, energy, and telecommunications sectors sequentially.[28] Under this framework, determinations of whether to introduce data portability to a sector have been based on an evaluation of a series of factors including likely impacts upon consumers, market efficiency, integrity and safety, and privacy for individuals and confidentiality for businesses.[29] Further, sector-specific rules governing transfers may be developed across a range of dimensions including consumer authorizations, safe and efficient data transfer, and the liability of participants.[30]

Types of Information

In considering data portability initiatives it is necessary to carefully scope the information subject to transfer. Ideally, transfers should cover information that a user has shared with a service that will be of greatest utility to the user. Expanding portability requirements to reach additional categories of information are likely to raise costs without corresponding benefits to consumers.

For example, providers regularly enrich existing data sets through complex analysis or the development of technological tools that rely on that data. Extending the scope of portability to such sensitive or proprietary business data would skew incentives to innovate. Additionally, many organizations maintain activity logs for security purposes that are unlikely to be of use to either a consumer or a legitimate recipient organization and would pose a significant operational burden to retain and process in a manner that enables portability. Therefore, providers should be

[27] Data Transfer Project, *supra* note 8, at 8 (noting that "Data Models have emerged organically in a largely disconnected ecosystem.").
[28] Office of the Australian Information Commissioner, "What is the Consumer Data Right?" last visited Aug. 21, 2020, https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right/.
[29] Australian Government The Treasury, "Consumer Data Right Overview" (Sept. 2019), at 11, https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf.
[30] *Id.* at 11-12.

encouraged to concentrate on building tools that easily and securely provide users access to the data they want to preserve or use elsewhere. This principle has been recognized by both the GDPR and California Consumer Privacy Act (CCPA) which limit their data portability rights to information that has been "provided to" or "collected" by a service respectively.[31]

Another consideration that should inform policymakers' approach to data portability initiatives is that certain data categories can pertain to multiple individuals, such as contact lists, photos, and social information.[32] When personal information sought by a user for transfer may relate to multiple additional individuals, those individuals are put at risk of having personal information transferred to an unknown third party without knowledge or consent. Consumer expectations of the availability of their information for third-party transfers may vary across services and types of information. Therefore, further multi-stakeholder engagement is appropriate to help evaluate relevant factors and reach a balanced approach to data transfers that implicate the privacy of multiple individuals. In some cases, transfers of information relating to multiple individuals may not be appropriate without the consent of all data subjects.[33]

**Question #6: Who should be responsible for the security of personal data in transit between businesses? Should there be data security standards for transmitting personal data between businesses? Who should develop these standards?**

Robust, risk-based data security standards for data portability transfers can mitigate threats of data leakage or access by harmful actors. Organizations' responsibility to apply reasonable protections for personal data extend to the data portability context and transferring entities should take steps to ensure that data is protected in transit between businesses and directed to the intended recipient.[34] Where user-directed transfers between organizations are technically feasible, common security standards for protecting data in transit should be developed and followed by both parties to the transfer. For example, the architecture of the DTP provides for the end-to-end encryption of data traveling between services and the revocation of authorization tokens following a data transfer to prevent the risk of subsequent misuse.[35]

---

[31] GDPR Art. 20; CCPA § 1798.100. (a).
[32] *See* Kevin Bankston, "How We Can 'Free' Our Facebook Friends," Techdirt (July 11, 2018), https://www.techdirt.com/articles/20180706/13460040185/how-we-can-free-our-facebook-friends.shtml.
[33] *See* Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" (May 22, 2019), at 135, https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf ("If the requested data has been provided to you by multiple data subjects (eg a joint bank account) you need to be satisfied that all parties agree to the portability request.").
[34] *See* Article 29 Working Party Guidelines *supra* note 24, at 19.
[35] Data Transfer Project, *supra* note 8, at 14-16.

Additional security safeguards should be considered for data portability transfers based on the nature and sensitivity of the transfer at issue. The DTP suggests possible protections such as minimizing data transferred, notifying users that a data portability request has been made, and limiting the number and frequency of transfers for a given user.[36] Finally, a common feature of digital systems is that security features designed to protect the privacy and autonomy of users can also negatively impact usability, therefore care should be taken in striking an appropriate balance in the data portability context.[37]

Policymakers should also consider standards for verifying the authenticity and data processing practices of individuals and organizations receiving data post-transit. There has been significant divergence on this topic in existing portability regimes. In the European Union, data protection obligations tend to follow information between organizations to the new data controller.[38] However, the Australian Consumer Data Right creates an accreditation system under which only entities that have been verified as meeting certain baseline privacy and information security requirements are permitted to be recipients of ported data.[39] Additional guidance is needed as to circumstances under which services may postpone or reject a portability request based on concerns about the validity of the request or the privacy and security practices of the recipient organization.[40]

**Question #7: How do companies verify the identity of the requesting consumer before transmitting their information to another company?**

Organizations should follow best practices for verifying and responding to data portability requests to ensure the legitimacy of requests. The privacy risk of lax verification practices was displayed in a 2019 study in which a security researcher who submitted GDPR data access requests in their fiancée's name received personal information in about 1 in 4 cases.[41] Strict requirements that place liability on organizations for not responding to portability requests in a particular time frame may create incentives for organizations to provide data access even in instances where the identity of the requestor is not verified with certainty.

Standards for verifying portability requests should be based on both the sensitivity of data at issue and the relationship that an organization has with a consumer. For example, it may be

---

[36] *Id*.
[37] *See* Article 29 Working Party Guidelines *supra* note 24, at 19.
[38] *Id*. at 6.
[39] Australian Government The Treasury, "Consumer Data Right Overview" (Sept. 2019), https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf.
[40] *See* Aysem Diker Vanberg, "The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience," J. Internet L. (2018), at 13.
[41] Leo Kelion, "Black Hat: GDPR privacy law exploited to reveal personal information," BBC (Aug. 8, 2019), https://www.bbc.com/news/technology-49252501.

easier for an organization to verify a consumer if the request is made through an existing, password-protected account.[42] Other services may require additional information in order to verify the identity of a data subject.[43] For direct portability between services, the DTP anticipates user authentication with both transferring and receiving entities prior to the initiation of a transfer.[44] Finally, some regimes provide for the appointment of "authorized agents" who may exercise rights on behalf of a data subject, which will require additional verification considerations and processes.[45]

**Question #8: How can interoperability among services best be achieved? What are the costs of interoperability? Who should be responsible for achieving interoperability?**

Interoperability, broadly defined as the ability for computer programs and systems of different vendors to exchange and make use of information, is the foundation of the open Internet.[46] Interoperability allows users to access websites and communications content consistently across different browsers and devices.[47] However, there are a range of technical features between systems that can be characterized as "interoperable," implicating different opportunities and risks. For example, an EU Commission report on Competition Policy for the Digital Era establishes a taxonomy for interoperability that covers "protocol interoperability," "data interoperability," and "full protocol interoperability."[48]

As with data portability, the risks and costs associated with requirements that businesses develop interoperable systems increase with the degree of interconnectivity between services. Mandates for interoperability that directly integrate features and functionality between complex digital services are likely to increase attack surfaces and heighten the potential for data exploitation and leakage.[49] Furthermore, rather than promote competition, mandated interoperability could increase the risk of collusion when competitors are required to share information and develop their systems in unison. Finally, interoperability requirements could limit innovation and consumer choice in services by restricting the ability of firms to

[42] Article 29 Working Party Guidelines *supra* note 24, at 14.
[43] *See* Information Commissioner's Office Guidance *supra* note 33, at 103.
[44] Data Transfer Project, *supra* note 8, at 6.
[45] *See* CCPA § 1798.185. (a)(7).
[46] *See, e.g.*, Chris Riley, "Unpacking interoperability in competition" 5, Journal of Cyber Policy, 94 (Mar. 15, 2020).
[47] *See* Urs Gasser, "Interoperability in the Digital Ecosystem," Berkman Klein Center for Internet & Society (Aug. 4, 2015) *available at* https://ssrn.com/abstract=2639210.
[48] Jacques Crémer, Yves-Alexandre de Montjoye, & Heike Schweitzer, "Competition policy for the digital era," European Commission (Mar. 29, 2019), at 59-60, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
[49] *See* Ben Thompson, "Open, Closed, and Privacy," Stratechery (Apr. 25, 2018), https://stratechery.com/2018/open-closed-and-privacy/.

differentiate services or develop new features due to the difficulties of working to maintain interoperability with competitors' products and services.

The United States legal system has a long history of setting conditions and legal certainty for developing interoperable systems, promoting both innovation and consumer choice in the technology sector. For example, in 1998 Congress included a carve-out in the Digital Millennium Copyright Act specifically directed at enabling software reverse engineering for the purpose of achieving interoperability between separate programs.[50] More recently, similar language permitting interoperability was included in the United States-Mexico-Canada trade agreement.[51] Going forward, policymakers should continue to ensure that user preferences and market forces can drive the development of greater interoperability between Internet-connected products, which will be especially important in the Internet of Things (IoT) context.

**Question #9: What lessons and best practices can be learned from the implementation of the data portability requirements in the GDPR and CCPA? Has the implementation of these requirements affected competition and, if so, in what ways?**

Both the GDPR and CCPA recognize important principles for data portability such as limiting the scope of information subject to transfer and adopting flexibility based on technical feasibility. At present, the deployment of the right to data portability under these frameworks is still developing. The European Commission's two-year implementation report of the GDPR notes that the "right to data portability has a clear potential, *still not fully used*, to put individuals at the centre of the data economy" (emphasis added).[52] Furthermore, although the CCPA entered into effect in January 2020, final implementing regulations were not approved until the fourteenth of August.[53] The ongoing implementation efforts under both regimes point to the need for developing data portability guidance, linked to clearly defined goals, extending beyond a bare obligation or right to portability.

---

[50] Digital Millennium Copyright Act Section 1201(f) (1998) specifically allows software developers to circumvent TPMs in a lawfully obtained computer program in order to identify the elements necessary to achieve interoperability of an independently created computer program with other programs.

[51] U.S.-Mexico-Canada Agreement, Art. 20.66.4(a) (Dec. 10, 2019), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/20-Intellectual-Property-Rights.pdf.

[52] European Commission, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation" (June 24, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

[53] California Attorney General, "Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act" (Aug. 14, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-final-regulations-under-california.

As described, data portability can support various public policy goals that are sometimes in tension and therefore require policymakers to establish clear guidance and expectations for managing. For example, while the Article 29 Working Party has provided important guidance on implementing the right to data portability under the GDPR, certain key issues are left open, such as balancing security risks and usability and considerations as to the rights of third-party data subjects in transfer requests.[54] Going forward, engagement on data portability initiatives should develop guidance and direction for resolving these key tensions at their outset.

Additionally, the GDPR and CCPA contain significant differences in requirements for exercising data portability controls including the scope of the right, covered entities, and the procedures for responding to requests.[55] These inconsistencies have created additional complications for organizations seeking to meet their data portability responsibilities under each framework and demonstrate the need for harmonized, multi-stakeholder approaches to developing the features and standards of data portability initiatives.

**Conclusion**

CCIA appreciates the opportunity to submit these comments in advance of the forthcoming workshop on data portability. As the Commission prepares for the workshop and future engagement on data portability, CCIA recommends considering the specific goals data portability initiatives can serve in discrete sectors. This approach will allow the Commission to evaluate and provide guidance to ensure that data portability efforts are appropriately balanced to best promote consumer welfare, competition, and innovation.

Respectfully submitted,

Keir Lamont
Policy Counsel
Computer & Communications Industry Association

[54] *See* Aysem Diker Vanberg *supra* note 40, at 6, 13.
[55] *See* clarip, "A DSAR Comparison Between GDPR and CCPA" last visited Aug. 12, 2020, https://www.clarip.com/data-privacy/dsar-gdpr-vs-ccpa/