August 2019

The Data Portability Act: More User Control, More Competition

For twenty years, the United States' approach to protecting privacy has relied primarily on notice and consent. As U.S. policymakers work to develop legislation to protect users' privacy, however, it is time to move away from that regime. Users want more control over the data they provide companies, and granting users certain rights over their data can facilitate increased control. Data portability is one such user right.[1]

Data portability allows users to take the data that a company has collected about them and move it to another service. Moving data in such a way has significant benefits. It helps users make informed decisions about who has access to their information by empowering them to switch services. Currently, large companies enjoy a huge advantage—massive data sets collected over years, if not decades—that new players cannot hope to compete with. Allowing users to port their data from one service to another promotes competition and gives new entrants access to data they otherwise would not have.[2]

After the 2018 Facebook–Cambridge Analytica scandal prompted a #DeleteFacebook movement, the ultimate question was where could users go? Without data portability, competitors to Facebook and other data-dependent companies are unlikely to become viable. Users of certain services may spend years developing a social following and creating content; the inability to transfer that work to another service likely serves as a significant switching cost that a data portability right could alleviate.

Data portability is already a requirement in some laws. Both the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Protection Act ("CCPA") grant users a right to data portability. Both require the information to be in a usable format that allows for easy transmittal, and information must be transmitted "without hindrance."[3] Many companies, including Google and Facebook, now allow users to download their data, often in a machine-

[1] User rights typically include the right for users to access, correct, and delete data, and to move their data from one service to another ("data portability").

[2] Another step in pro-competitive policy would be encouraging platform interoperability, meaning that different services (especially social networks) allow communication and functionality across platforms so, for instance, a Facebook user could directly communicate with a Twitter user. *See* OTI Comments to FTC, at 7-13, https://newamericadotorg.s3.amazonaws.com/documents/OTI_Final_FTC_portability_comments_Question_4_fixed.pdf.

[3] GDPR, Art. 20, Sec. 1, https://gdpr-info.eu/art-20-gdpr; California Consumer Privacy Protection Act of 2018, AB-375, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375, *as amended by* SB 1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 ("CCPA").

readable format that can be used to transmit their data to another service. Google and Microsoft recently teamed up to launch the Data Transfer Project, an open source software project designed to facilitate data transmittals, that now counts Facebook, Twitter, and Apple as contributors.[4]

Data portability will encourage online competition, and any U.S. privacy legislation should include a right to data portability. Below, we present the Data Portability Act, which provides strong, clear draft bill language that should serve as a model for Congress as it deliberates how to protect privacy and encourage competition in a privacy law.

The Data Portability Act

The Data Portability Act (the "Act")[5] builds on and improves the provisions contained in the GDPR and CCPA and encourages the free flow of data between online services. The Act would grant a "customer, subscriber, or user" (the "rightsholder") a right to portability over many types of data, including social graph[6] and address book data, going into more detail than the GDPR or the CCPA. The data requested must be provided to the rightsholder in a standard format and secured, and the mechanism must be prominently available and provided free of charge. Transmitting companies must follow special privacy and security requirements, such as authenticating the requesting rightsholder, and must not transmit data if the company cannot meet those requirements. The Act would not require companies to collect more data than they normally would, or to identify unidentified data. It also grants the Federal Trade Commission (FTC) rulemaking authority under the Administrative Procedure Act to promulgate regulations, and requires the FTC to define specific terms in the statute once every five years.

We envision that the Data Portability Act will most likely be incorporated into a more comprehensive privacy bill. This premise has three primary impacts on the Act. First, we did not try to draft language aimed at providing other rights, even those that are conceptually similar to portability, such as access, correction, and deletion. Second, while we thought it was important for our language to include authorization for FTC enforcement and rulemaking as part of the text, our expectation is that such language would be subsumed into broader rulemaking authorization in the comprehensive bill. Third, some terms are not fully defined within the confines of this bill, because they would likely be defined in a comprehensive privacy bill.

Below is a section-by-section explanation of the Act.

[4] Data Transfer Project, https://datatransferproject.dev.

[5] Full text in Appendix A.

[6] Facebook's social graph is Facebook's way of tracking your friends and how you interact with others on its platform. Boonsri Dickinson, *So What the Heck Is the 'Social Graph' Facebook Keeps Talking About?*, Business Insider (Mar. 2, 2012), https://www.businessinsider.com/explainer-what-exactly-is-the-social-graph-2012-3.

> ***Section 1. User right to data portability.***
> *(a) In General.—Where technically feasible, a customer, subscriber, or user of a covered entity shall have the right to receive, and the right to transmit directly from that covered entity to another covered entity of their choosing, a copy of any data within the possession or control of the covered entity that*

The first section of the Act sets out the basic right to data portability. Any customer, subscriber, or user of a service has the right to receive (download) and transmit a copy of their data directly to another company of that person's choosing. The list of types of data is further explained below.

The language aims to capture and improve upon other portability requirements. As noted above, at least two laws currently require data portability. The GDPR grants "data subjects" the right to transmit data from one "data controller" to another whenever technically feasible.[7] The CCPA requires a "business" to deliver "portable" data to "consumers" requesting access.[8] Both require the information to be in a usable format that allows for easy transmittal, and information must be transmitted "without hindrance." Further, the Dodd Frank Wall Street Reform and Consumer Protection Act provides an analogous right to portability of consumer financial data.[9]

In the Data Portability Act, the data portability requirement applies to "covered entities" (or "companies" herein) broadly. Like in the GDPR and the CCPA, a federal data portability requirement should apply to all online companies that process (collect, use, or otherwise handle) personal data. If a company collects data about its customers, subscribers, or users, those people should be able to port that data to another service. This requirement should also apply to small businesses, though the Act incorporates a safety valve in its list of exceptions that would not impose the requirement on small companies that collect and store data, but do not attribute that data to a particular customer, subscriber, or user.

Our definition of the rightsholder, while drafted broadly, is narrower than that of other laws. The CCPA grants portability to the "consumer," meaning every natural person in California. The GDPR grants portability to the "data subject," meaning any identified or identifiable natural person. The Data Portability Act grants the right to the "customer, subscriber, or user," which requires that the person exercising the right has some kind of relationship with a certain company. Having a broader definition of user or applying the right to all natural persons may create more privacy problems—the law should not force a company to attach identifying information to data that it would not otherwise identify simply to facilitate its portability (see further discussion in the exceptions section below).

---

[7] GDPR, Art. 20, Sec. 1, https://gdpr-info.eu/art-20-gdpr.
[8] CCPA, *supra* note 3, Sec 1(d).
[9] Dodd-Frank Wall Street Reform and Consumer Protection Act, Section 1033 "Consumer Rights to Access Information," https://www.govtrack.us/congress/bills/111/hr4173/text/enr#link=X_C_1033&nearest=H5003C7E8716F46EBA98F9F8AC7DD9B71.

This definition of rightsholder will likely mean that data brokers, because they collect data about people from other sources, will not have to comply with the portability requirement as written. We do not intend to downplay the unique concerns associated with data brokers—in fact, data brokers should be subject to their own privacy obligations beyond a mere registry. But given a data broker's increased difficulty in authenticating identity and concerns related to a company potentially having to attach an identity to unidentified data, the Act requires rightsholders to have a relationship with the company before they have a right to transmit data.[10]

Within the data portability right is the right to "receive," or download, data. The Act, in general, requires that companies establish a mechanism to export data, but does not require a company to import data or impose any requirements on importing data. One service may require a person to download a copy of their data from another service rather than allow for direct transmittal between services. In this way, the right to "receive" data in this Act could be viewed as a right of access (a different user right) to data held by a company about a rightsholder. The proper scope of a right of access is beyond the subject matter of this memo, except to say that data that is portable should also be accessible to the rightsholder. Therefore, in addition to a direct transmittal to another service, the data portability right allows for a direct download.

The Act requires that a "copy" of the data be downloaded or transmitted to another company. The transmitting company is not required to delete the data it holds on the rightsholder when it transmits that data. That said, in comprehensive privacy legislation, a person would likely also have the right to have their information deleted from the transmitting service if they so desire, which could be encapsulated in a separate "right to deletion" of data.

Last, by default the Act assumes that any data "within the possession or control" of the company is portable. Thus, any data stored on a company's servers, or stored in a way that the company has the ability to process that data, regardless of the source of that data, is susceptible to the portability right.

Covered types of data

The Act broadly defines the five types of data that should be portable: data the rightsholder provides to the company, data the rightsholder has access to and was collaboratively or jointly created, data about the rightsholder that was collected by the company through the normal use of the company's service, data inferred about the rightsholder through analyzing other information, and data about the social connections (if any) that the rightsholder has accumulated through their use of the service.

> *(1) the customer, subscriber, or user affirmatively provided to the covered entity,*

[10] OTI would welcome increased regulations on data brokers.

Ensuring portability of data provided to the company by the rightsholder is non-negotiable. If a person provides data to company, that company must make that data portable. For instance, a person who uses a social network may upload myriad documents, posts, and media to the site, and all that data should be portable to another company. The GDPR already requires such data to be portable.[11]

> *(2) that was created in whole, in part, or collaboratively by the customer, subscriber, or user using the covered entity's service or functionality provided by the covered entity's service, and to which the customer, subscriber, or user has authorized access at the time the data is requested,*

Similarly, data created on the service provided by the company, and in collaboration with others, should be portable by the relevant rightsholders. The most obvious examples are Google Docs or shared word processing documents that were created and maintained by multiple people. That said, this provision raises the question of people interacting and responding to other people's content. For instance, is a post collaboratively created when a person retweets another tweet and responds with a comment? What about comments or replies in response to another person's post? These are good questions for the FTC to address in its rulemaking, further discussed below.

The rightsholder must still have authorized access to the data at the time of the transmittal request. Those who have lost access to a particular document or piece of media should not be able to access it circuitously through their data portability right.

> *(3) concerns or pertains to the customer, subscriber, or user, and was collected through the customer, subscriber, or user's use of the covered entity's service or functionality provided by the covered entity's service,*

Data that a company passively collects and processes about its customers, subscribers, or users (often called "observed data") should be portable. Data in this category would include heart rate information on a health device, location data collected by a map program, or activities on a site such as ads clicked on or terms searched for.

Not only does access to these types of data benefit rightsholders (who may monitor their health or want to know the geographic locations they have visited), but allowing their portability could provide competitive benefits. Transmitting data to other companies would help level the competitive playing field by allowing new companies to bypass the significant hurdle posed by the need to invest time and resources into accumulating their own data to become a real, feasible alternative for users. For instance, it could help competing health apps or map programs better understand new users and better provide their own service or potentially serve

[11] GDPR, Art. 20, Sec. 1, https://gdpr-info.eu/art-20-gdpr ("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….").

ads. Transmitting this data could also foster innovation by providing inputs for competing services to make their own inferences about customers, subscribers, or users for their own benefit, potentially leading to new services and more viable business models.

In Europe, observed data has been considered portable. The Article 29 Working Party of the European Commission (now part of the European Data Protection Board[12]) concluded in its guidelines on data portability that "observed data provided by the data subject by virtue of the use of the service or the device," such as the subject's search history, traffic data, and location data, and even "raw data such as the heartbeat tracked by a wearable device" is covered by GDPR's portability requirement.[13]

> *(4) was inferred by the covered entity about the customer, subscriber, or user,*

Data that companies have inferred about rightsholders from their collection of other types of data should be portable. Inferred data is data that the company did not directly collect, but learned through analysis of other data the company has access to. For instance, a company may learn that a person enjoys bicycling given recent clicks on ads for helmets, or a company may learn that a person works a 9-to-5 job given the times that the person logs into the service. Often, these inferences are used to categorize people and serve ads, and such information would be highly useful to a new service.

Information that a company infers about a rightsholder can have important portability value. For the rightsholder, it allows them to move to a different service while still making use of the results of the analysis of their own data. The company to which the data is being transmitted will have access to data, it would not otherwise have, which could help it develop a more viable business model, much like with passively collected data. However, making this sort of data portable will be challenging and we expect that the FTC will exempt data that clearly would not be useful or practical to transmit (see description of FTC rulemaking below).

> *(5) consists of address books, directories, friends lists, social graph data, or any other data regarding the customer, subscriber, or user's contacts that is necessary and sufficient to connect with, communicate with, or re-identify those contacts on another covered entity's service.*

Perhaps the most difficult—but in some cases, the most important—type of data that should be portable is address books and social graphs. Recreating a social network is often the highest

[12] European Data Protection Board, https://edpb.europa.eu/.

[13] Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (April 5, 2017), at 10, https://www.ec.europa.eu/newsroom/document.cfm?doc_id=44099. That view has been criticized by the European Commission. David Meyer, *European Commission, Experts Uneasy over WP29 Data Portability Interpretation*, Privacy Advisor - IAPP (Apr. 25, 2017), https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1.

barrier for users to changing services—assuming there is a viable competing service. If a person is to create a new network on a competing social network, that person needs to be able to recreate their friends list on the new service without undergoing an onerous and burdensome process. Some users of large social networks have thousands of friends or connections, and recreating that network manually would be nearly impossible, and therefore, impedes effective competition.

OTI and others[14] have called on Facebook, Twitter, and other companies to "free the social graph," and make it easy to replicate networks on other social services. But meaningful social graph portability raises privacy issues. Portability of your social graph requires moving personal data about all of your friends that is sufficient to reliably re-identify and reconnect with them on another service. Your friends, however, may not want or expect you to move that data about them to another platform, or they may not have ever shared such contact details with you in the first place. The FTC should address this issue in its rulemaking, as discussed below, to ensure that social graph portability does not undermine privacy. It may not be an easy task, but the competitive benefits will be significant.

How to transmit data

> *(b) Format.—The data made available under subsection (a) shall be provided in a machine-readable format, using an industry standard or commonplace format or, where such a standard or commonplace format is not available, in a reasonably consistent and stable publicly-defined and publicly-documented format.*

Key to a robust data portability right is ensuring that data is transmitted in a standardized and machine-readable format that follows industry standards. Common formats are necessary to ensure seamless data portability between different companies. Such a requirement is also included in similar forms in the GDPR[15] and CCPA.[16] Our language goes somewhat further by requiring that, if there is no existing standard, data must be organized in a consistent and publicly defined format such that other companies can design systems to make use of ported data. This helps to protect against companies transmitting data in incomprehensible formats that change arbitrarily, making portability nearly impossible.

[14] Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (June 28, 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends; Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, EFF (July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine.

[15] GDPR, Art. 20, Sec. 1, https://gdpr-info.eu/art-20-gdpr ("in a structured, commonly used and machine-readable format").

[16] CCPA, *supra* note 3, Sec. 1(d) ("in a readily useable format that allows the consumer to transmit this information to another entity").

> *(c) Mechanism.—The mechanism that effectuates the right in subsection (a) shall be made available prominently and free of charge, and the transmission of requested data shall be provided without hindrance.*

A data portability right is most useful and effectual when the mechanism is prominent and provided free of charge. Companies should not be able to hide or monetize their portability mechanism. If rightsholders must navigate through multiple policies or down many levels of menus to find the mechanism, or must purchase access to the mechanism, that will impede competition and reduce the effectiveness of the data portability right.

> *(d) Security and Privacy.—A covered entity providing or transmitting data under Section 1*
> *(1) must take reasonable steps to authenticate the requesting user, and must provide or transmit the requested data to the new entity requested, or the user themselves, in a reasonably secure manner, and*
> *(2) must not allow the provision or transmission of data if it has a good faith belief or is aware of substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent.*

In storing and transmitting data, security is extremely important. Companies handling data portability requests have an obligation under this statute to authenticate the requesting user before allowing any transmittal of data, and the transmittal must be handled securely. These are straightforward requirements for any portability right.

Subsection 1(d)(2) requires companies to refuse to transmit data to other companies when they have a legitimate concern that the requesting party is not authorized to access the data or is acting with malicious intent. This section could be misused by companies that do not wish to share their data with other companies. However, the requirement that a refusal be based on “a good faith belief” or an awareness of “substantial indicators” should limit any potential misuse of this authentication safeguard. The FTC has rulemaking authority to define these terms (discussed below), which should provide clarity and a sufficient deterrent to prevent companies from engaging in this behavior.

Relatedly, rightsholders should be able to try out (and thus port data to) multiple different services in a short period of time. Thus, multiple data portability requests within a short period of time on their own should not be sufficient for a “malicious intent” finding.

> *(e) Exceptions.—Nothing in this section shall be construed to require an entity to*
> *(1) collect information it does not otherwise collect,*
> *(2) maintain or retain information about a customer, subscriber, or user when it otherwise would not,*
> *(3) create new records that are personally identified or identifiable to particular customers, subscribers, or users,*
> *(4) personally identify records that were not previously personally identified to particular customers, subscribers, or users, or*
> *(5) import data from another entity.*

A right to data portability should be enacted carefully, and steps should be taken to avoid inadvertently creating more privacy problems. For instance, a company may hold data in a scattered, unidentified format, or it may affirmatively delete data when it no longer serves a purpose. That company should not have to undertake more data collection, or identify unidentified data, just to meet the data portability requirements. Thus, the Act attempts to protect privacy by not requiring the creation of new personal data or personally identifiable data.[17]

Without the need to collect or analyze more data than a company otherwise would, this provision should help alleviate the burden on small companies that may not have sophisticated databases where all data is tied to a particular user. A company that does not already have those databases set up would be exempt from this Act's requirements. Such an exception avoids a situation in which a small company would be forced to recreate a purchase history based on credit card numbers. Given the presence of these exceptions, there is no need for a separate "small business" exemption nor a need to define the contours of a "small business."

The last exception makes clear that the Act does not require a company to import data from another company. However, there should be sufficient incentive for companies to create import mechanisms, because such mechanisms will allow them to access data without having to invest significant time and resources into collecting it.

[17] This section was inspired by Dodd-Frank's financial data portability provision, which affirmatively states that it does not create a duty to maintain or keep records, just that the records they do maintain or keep need to be portable. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Section 1033 "Consumer Rights to Access Information," https://www.govtrack.us/congress/bills/111/hr4173/text/enr#link=X_C_1033&nearest=H5003C7E8716F46EBA98F9F8AC7DD9B71.

> ***Sec. 2. Immunity for services.—****Notwithstanding any other provision of law, covered entities shall not be held liable for*
>
> *(a) the act of providing or transmitting data in compliance with the requirements of this Act,*
>
> *(b) the acts of third parties that arise from the provision or transmission of data that is done in compliance with the requirements of this Act, or*
>
> *(c) failure to provide or transmit requested data if it has a good faith belief or is aware of substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent.*

As seen with the Data Transfer Project, there are already efforts to build platforms that allow seamless data transmittal. When these companies follow the Data Portability Act, particularly in regard to data security and authentication requirements, they should not be held further responsible for the behavior of potential bad actors. A transmitting company is unlikely to know exactly how a receiving company will use data transmitted to them, and any subsequent privacy violations or data breaches should be the responsibility of the relevant company, not the transmitting company. That said, similar to subsection 1(e)(2), companies should not be held liable for refusing to transmit data when they rely on a good faith belief that the parties involved are not able to be authenticated or are otherwise acting maliciously. The particulars of immunity are to be determined by the FTC under subsection 3(c)(1).

> ***Sec. 3. Enforcement.*** *Enforcement by Federal Trade Commission.—*
> *(a) Unfair and deceptive practices.—A failure to comply with the requirements of Section 1 by an entity shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).*
> *(b) Rulemaking authority.—The Commission shall promulgate regulations under this Act in accordance with section 553 of Title 5, United States Code.*
> *(c) As a part of its rulemaking, the Commission shall determine within one year of enactment of this Act, and at least once every five years thereafter,*
> *(1) What constitutes "reasonable steps to authenticate," a "reasonably secure manner" of data delivery, and "a good faith belief or awareness" of "substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent."*
> *(2) What specific types of data are included in the categories of data subject to the user right in Section 1. In making this decision, the Commission shall balance the following elements:*
> *(A) the utility of each type of data to requesting customers, subscribers, or users,*
> *(B) the competitive benefits of requiring the provision or transmission of each type of data,*
> *(C) the privacy or security risk to parties other than the requesting customer, subscriber, or user from the provision or transmission of each type of data, and*
> *(D) whether requiring the provision or transmission of each type of data would create an unreasonable or undue burden on covered entities compared to the utility and benefits of requiring the portability of that data.*

The FTC should enforce the user right to data portability. The FTC has extensive privacy and competition expertise, and it recognizes the importance of employing technologists who will be able to understand the underlying systems the Act will require.

Granting authority to the FTC under this Act is standard. Subsection 3(a) states that violating the Data Portability Act constitutes a violation of a rule promulgated under the rulemaking provisions of the FTC Act. Subsection 3(b) states that the FTC shall also have general rulemaking authority to further define and clarify any provisions of the Act.

The Data Portability Act, however, adds another element: periodic review of pertinent parts of the Act that will likely need updating. Subsection 3(c) requires the FTC to define certain terms, and define what types of data are portable, within one year of enactment, and then again every five years thereafter.[18] These time restrictions are necessary to ensure that the Act continues to

[18] This requirement is a modified version of the five year review timeline contained in the Children's Online Privacy Protection Act, 15 USC § 6506.

reflect the technology available at the time and ensure that rightsholders have the broadest possible portability rights without overburdening the online ecosystem.

The Act requires the FTC to engage in a balancing test when determining whether certain types of data shall be portable. Essentially, the FTC would have to balance the benefits of making the data portable, both to rightsholders and to competition, against the potential harms to privacy and to the relevant companies. Though, to most effectively promote rightsholders' control over their data and increase competition, data should be portable by default.

> ***Sec. 4. Effective Date.—***
> *(a) In General.—This Act shall take effect upon enactment.*
> *(b) Applicability of Specific Provisions Within Section 1.—*
> *(1) With respect to Section 1(a)(1), covered entities must comply within one year of enactment of this Act.*
> *(2) With respect to Section 1(a)(2)-(6), covered entities must comply within 180 days of a final FTC decision pursuant to notice-and-comment rulemaking under Section 3(b)-(c).*

The effective date of most of the Act is upon enactment. There are special provisions with respect to Section 1. Because portability of data that users provide to a company is so straightforward, companies must comply with the data portability requirement within one year of enactment. On the other hand, the types of data in the remaining part of Section 1 are not as immediately clear. Therefore, companies must come into compliance with those requirements within 180 days of the FTC providing further clarity and guidance on what specific types of data must be portable under each subsection.

Appendix A

Section 1. User Right to Data Portability.

(a) In General.—Where technically feasible, a customer, subscriber, or user of a covered entity shall have the right to receive, and the right to transmit directly from that covered entity to another covered entity of their choosing, a copy of any data within the possession or control of the covered entity that
   (1) the customer, subscriber, or user affirmatively provided to the covered entity,
   (2) that was created in whole, in part, or collaboratively by the customer, subscriber, or user using the covered entity's service or functionality provided by the covered entity's service, and to which the customer, subscriber, or user has authorized access at the time the data is requested,
   (3) concerns or pertains to the customer, subscriber, or user, and was collected through the customer, subscriber, or user's use of the covered entity's service or functionality provided by the covered entity's service,
   (4) was inferred by the covered entity about the customer, subscriber, or user, or
   (5) consists of address books, directories, friends lists, social graph data, or any other data regarding the customer, subscriber, or user's contacts that is necessary and sufficient to connect with, communicate with, or re-identify those contacts on another covered entity's service.

(b) Format.—The data made available under subsection (a) shall be provided in a machine-readable format, using an industry standard or commonplace format or, where such a standard or commonplace format is not available, in a reasonably consistent and stable publicly-defined and publicly-documented format.

(c) Mechanism.— The mechanism that effectuates the right in subsection (a) shall be made available prominently and free of charge, and the transmission of requested data shall be provided without hindrance.

(d) Security and Privacy.—A covered entity providing or transmitting data under Section 1
   (1) must take reasonable steps to authenticate the requesting user, and must provide or transmit the requested data to the new entity requested, or the user themselves, in a reasonably secure manner, and
   (2) must not allow the provision or transmission of data if it has a good faith belief or is aware of substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent.

(e) Exceptions.—Nothing in this section shall be construed to require an entity to
   (1) collect information it does not otherwise collect,
   (2) maintain or retain information about a customer, subscriber, or user when it otherwise would not,
   (3) create new records that are personally identified or identifiable to particular customers, subscribers, or users,
   (4) personally identify records that were not previously personally identified to particular customers, subscribers, or users, or
   (5) import data from another entity.

Sec. 2. Immunity for Services.—Notwithstanding any other provision of law, covered entities shall not be held liable for

(a) the act of providing or transmitting data in compliance with the requirements of this Act,
(b) the acts of third parties that arise from the provision or transmission of data that is done in compliance with the requirements of this Act, or
(c) failure to provide or transmit requested data if it has a good faith belief or is aware of substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent.

Sec. 3. Enforcement.—Enforcement by Federal Trade Commission.—

(a) Unfair and Deceptive Practices.—A failure to comply with the requirements of Section 1 by an entity shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).
(b) Rulemaking Authority.—The Commission shall promulgate regulations under this Act in accordance with section 553 of Title 5, United States Code.
(c) As a part of its rulemaking, the Commission shall determine within one year of enactment of this Act, and at least once every five years thereafter,
    (1) What constitutes “reasonable steps to authenticate,” a “reasonably secure manner” of data delivery, and “a good faith belief or awareness” of “substantial indicators that the requesting party or the requested new entity is not authorized to access the data or is otherwise acting with malicious intent.”
    (2) What specific types of data are included in the categories of data subject to the user right in Section 1. In answering this question, the Commission shall balance the following elements:
        (A) the utility of each type of data to requesting customers, subscribers, or users,
        (B) the competitive benefits of requiring the provision or transmission of each type of data,
        (C) the privacy or security risk to parties other than the requesting customer, subscriber, or user from the provision or transmission of each type of data, and
        (D) whether requiring the provision or transmission of each type of data would create an unreasonable or undue burden on covered entities compared to the utility and benefits of requiring the portability of that data.

Sec. 4. Effective Date.—

(a) In General.—This Act shall take effect upon enactment.
(b) Applicability of Specific Provisions Within Section 1.—
    (1) With respect to Section 1(a)(1), covered entities must comply within one year of enactment of this Act.

(2) With respect to Section 1(a)(2)-(6), covered entities must comply within 180 days of a final FTC decision pursuant to notice-and-comment rulemaking under Section 3(b)-(c).