August 2019

The Data Portability Act: 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).