The Do-Not-Track Act of 2019

Section 1. Short Title

(a) SHORT TITLE.—This Act may be cited as "The Do-Not-Track Act of 2019."

Section 2. Definitions

(a) "Anonymous Data" means data which does not relate to an identified or identifiable User. Identifiable Data may be rendered Anonymous Data if it has been De-Identified to an extent that no User can be singled out or identified, either directly or indirectly, (e.g., via association with an identifier, User Agent, or device), by that data alone or in combination with other data. To determine whether a User can be identified from the data, account should be taken of all the means reasonably likely to be used by any Party to identify the User. Data that has been re-identified, is shown to be capable of re-identification, or that is capable of being used for Personalization or profiling a User or a device used by a User is not Anonymous Data.

(b) "Collect" means to receive Identifiable Data in a Network Interaction and to retain that data after the Network Interaction is complete.

(c) "Commission" means the Federal Trade Commission.

(d) "Context" means a website or similar online Resource, or a connected set of such Resources. A connected set of Resources that are controlled by the same Party or jointly controlled by a set of Parties can constitute a single Context if a User would reasonably expect them to form a single Context. Factors relevant to determining whether such a reasonable expectation exists include, but are not limited to, whether they share prominent branding, provide connected and integrated User-facing features, are offered under the same domain name or through a single app, use the same sign-in credentials, and are marketed or sold as a single product or service.

(e) "De-Identify" means to alter data such that the likelihood of identifying a User from the data is reduced. De-Identification includes a range of techniques and differing levels of re-identification risk. Data that is fully De-Identified such that it becomes Anonymous Data is no longer Identifiable Data. Data that is De-Identified to a lesser extent remains Identifiable Data.

(f) "Do-Not-Track Signal" means a signal sent by a web browser or similar User Agent that conveys a User's choice regarding online Tracking, reflects a deliberate choice by the User, and otherwise complies with the latest Tracking Preference Expression (DNT) specification published by the World Wide Web Consortium (W3C) [available at https://www.w3.org/TR/tracking-dnt/].

(g) “First Party” means, with respect to a given User Action, a Party with which the User intends to interact, via one or more Network Interactions, as a result of that action.

(1) Typically, when a User visits a website, the First Party is the Organization identified in the website URL and/or whose branding is most prominent on the website.

(2) More than one Party can be a First Party with regard to a given User Action. For example, when a User visits a website with prominent co-branding identifying two Organizations such that the User would reasonably expect to be communicating and interacting with both Organizations when accessing the website, both Organizations can be First Parties.

(3) Conversely, the mere presence on a First Party’s website of embedded content from another Party does not make that other Party a First Party, and merely hovering over, muting, pausing, or closing a given piece of content does not constitute a User's intent to interact with a Party. When a User visits an Organization’s website that displays advertisements from a third-party ad network, the Organization is a First Party and the ad network is a Third Party. When a User signs into an Organization’s website using a sign-in method provided by another Party, the Organization is a First Party and the sign-in provider is a Third Party with respect to User Actions in that website.

(h) “Identifiable Data” means data from which the User can be singled out or identified, directly or indirectly (e.g., via association with an identifier, User Agent, or device), by that data alone or in combination with other data. Identifiable Data includes, but is not limited to, a User’s contact information (such as email addresses and phone numbers), unique persistent identifiers (such as IP addresses, cross-session cookie IDs, and device identifiers including those derived through device fingerprinting and probabilistic techniques), and any other data associated with such identifiers. Identifiable Data does not include Anonymous Data.

(i) “Network Interaction” means an online connection consisting of an HTTP[S] request and as many corresponding response(s) as are necessary to respond to a single User Action. A User interaction or session with a website or other Resource frequently consists of many Network Interactions.

(j) “Organization” means a legal entity. Such term does not include government agencies or Users.

(k) “Party” means a User, an Organization, or a group of legal entities that share common ownership and control, operate as an integrated enterprise, and have a group identity that is easily discoverable by a User. Common branding or publishing a list of affiliates that is readily available online via a prominent link from a Resource where a

party describes its DNT practices are deemed easily discoverable. With respect to a User Action, a Party is either a First Party or a Third Party (but not both).

(l) "Personalize" means to use Identifiable Data to alter the experience of a User, including but not limited to the content or advertising displayed to the User.

(m) "Process" means to Collect, use, or Share data.

(n) "Resource" means a single online destination or experience, such as a website, streaming service, online game, digital assistant, or other online service, accessed by a User through the use of a User Agent.

(o) "Service Provider" means an Organization that Processes Identifiable Data on behalf of another Organization. A Service Provider has no right to use any Identifiable Data for its own purposes.

(p) "Share" means, with respect to Collected data, to transfer or provide a copy of such data to any Third Party.

(q) "Third Party" means, for any User Action, any Party other than the User, a First Party to that User Action, or a Service Provider acting on behalf of either the User or a Frist Party.

(r) "Tracking" or "Track" means to (a) Collect data regarding a User Action of a particular User, (b) Process such data outside the Context in which the User Action occurred, (c) facilitate the creation of a User profile; or (d) Personalize that User's online experience. For the purposes of this definition, Processing data related to a device used by a User or the User's household shall be considered Processing data related the User.

(s) "User" means a natural person who uses the Web.

(t) "User Action" means a deliberate online action by the User, via configuration, invocation, or selection, to initiate a Network Interaction. Selection of a link, submission of a form, and reloading a page are examples of User Actions.

(u) "User Agent" means any of the various client programs capable of initiating Network Interactions, including but not limited to browsers, spiders (web-based robots), command-line tools, native applications, mobile apps, or Internet-connected devices.

Section 3. Response to Do-Not-Track Signals

(a) IN GENERAL.—Except as permitted below, a Party to a User Action that receives a Do-Not-Track Signal indicating a User preference not to be Tracked shall not Track.

(b) EXCEPTIONS.—

(1) FIRST PARTY.—A First Party to a User Action within a Context to which the User has affirmatively signed in may Process data received from such User Action (including for Personalized content, services, and advertising) within that Context. However, a First Party shall not Share such data with a Third Party. For the purposes of this paragraph, a User is signed into a Context when the User has affirmatively authenticated and identified oneself by entering a username and password, or similar credentials.

(2) ANONYMOUS DATA.—Data that has been sufficiently De-Identified such that it is rendered Anonymous Data may be Processed for any purpose, including outside of the Context of the User Action(s) from which it originates, or across multiple Contexts.

(3) CONSENT.—A Party may disregard a User's Do-Not-Track Signal when the User has given express affirmative consent to Track. A User may give consent through a technical means defined in the Tracking Preference Expression (DNT) specification published by the World Wide Web Consortium (W3C) or through a separate mechanism such as an online or offline consent form that demonstrates a specific and voluntary choice of the User. For instance, accepting a general or broad terms of use document that contains a clause regarding Tracking does not constitute express affirmative consent for the purposes of this Act. Likewise, agreement obtained through a user interface designed or manipulated with the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice does not constitute consent for the purposes of this Act. When relying on consent from a User given through a separate mechanism, a Party must provide notice in accordance with Section 5 below.

(4) PERMITTED USES.

(A) IN GENERAL.—An Organization may Process data for the uses specified below, provided the Organization:

(i) limits the amount of Identifiable Data Collected to that which is strictly needed for the permitted use(s);

(ii) limits the retention of Identifiable Data to no longer than is reasonably needed for the permitted use(s);

(iii) uses Anonymous Data to the extent the permitted use(s) can be achieved with such data, or otherwise De-Identifies the Identifiable Data to the greatest extent that is compatible with the permitted use(s);

(iv) Processes the data separately from systems that are used for purposes other than the permitted uses specified in this section; and

(v) does not Process the data beyond the permitted use(s).

(B) PROVIDING A SERVICE.—An Organization may Process data to the extent necessary to effectuate a transaction with the User, or to provide a product or service to a User, provided the User has consented to or authorized the transaction or the provision of the product or service and any Tracking, including Personalization, that is a necessary or inherent part of that transaction, product, or service would have been clear to the User at the time of such consent or authorization. If such Processing requires Sharing data with a Third Party, such Third Party may not Process the data for any other purpose.

(C) SECURITY.— An Organization may Process data to the extent reasonably necessary to detect security incidents, protect the website or other Resource accessed by the User against malicious, deceptive, fraudulent, or illegal activity, and prosecute those responsible for such activity.

(D) DEBUGGING.—An Organization may Process data for debugging purposes to identify and repair errors that impair existing functionality of the website or other Resource accessed by the User.

(E) FINANCIAL LOGGING.— An Organization may Process data for billing and auditing related to Network Interactions and related transactions.

(F) RESEARCH.— An Organization may Process data to conduct security research.

(G) JOURNALISM.— An Organization may Process data as necessary for news gathering purposes by journalists or other purposes protected by the First Amendment to the United States Constitution.

(5) TECHNICAL ERRORS.—Data that is Processed by a Party due to a technical error does not violate this Act if such error is unintentional and unexpected, and within 30 days of the Party discovering or receiving a report of the error: (i) the error is corrected, (ii) any Processing by the Party that is otherwise prohibited is stopped, and (iii) the Party deletes any data that should not have been Collected.

Section 4. Contractual Obligations and Liability.

(a) A First Party that enables or permits a Third Party to engage in Tracking on or through the First Party's website or other Resource:

(1) must require the Third Party, through a contract, terms of service, or similar binding and enforceable legal agreement, to comply with this Act;

(2) shall be liable for the Third Party's non-compliance with this Act if the First Party knew or could have upon the exercise of due diligence known of the Third Party's non-compliance and failed to take adequate corrective action.

Section 5. Transparency.

(a) IN GENERAL.—An Organization that engages in Tracking shall describe, in understandable language and syntax such that an ordinary User can comprehend, its practices with respect to Do-Not-Track Signals in its privacy statement or similar notice, available through a clear and prominent link on the home page of its website(s). The description required under this paragraph must include at least the following information:

(1) the exceptions or permitted uses under this Act under which the Organization Processes data;

(2) the effects on the User, if any, resulting from a Do-Not-Track Signal, including if any webpages, features, or services are not available, or reduced in functionality;

(3) if the Organization obtains out-of-band consent to disregard the Do-Not-Track Signal, a description of how a User may give and revoke consent, and the scope of any such consent, and the anticipated effect of consent or revocation on the User;

(4) the time period or periods for which Identifiable Data Collected by the Organization is retained or the criteria used to determine such time periods, and whether such Identifiable data is rendered Anonymous Data in lieu of being deleted; and

(5) how a User may contact the Organization with any inquiries or complaints regarding the Organization's Do-Not-Track practices.

Section 6. No Circumvention

A Party shall not block or take similar actions to avoid receiving a User's Do-Not-Track Signal. Nor shall any Party take other actions to circumvent the effectiveness of Do-Not-Track Signals.

Section 7. Report to Congress

Not later than five years after the effective date of this Act, the Commission shall review the effectiveness of this Act and submit a report to Congress. The report shall include information on the number of FTC personnel working on enforcement of the Act, the number of matters investigated, a description of enforcement or other actions taken as a

result of such investigations, and an evaluation of whether complaince with the Act aligns with reasonable expectations of Users enabling the DNT Signal, the Act's impact on consumer privacy generally, and any demonstrable influence on innovation and the availability of consumer services.

Section 8. Enforcement

(a) DE FACTO AND DE JURE HARM.—Users from whom Identifiable Information has been Processed in violation of this Act shall be deemed to have been harmed by such violations.

(b) ENFORCEMENT BY THE COMMISSION.—The Commission is authorized to enforce this Act.

(1) ACTIONS BY THE COMMISSION.—Except as provided in this Section, the Commission shall have the authority to prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(2) STATUTORY DAMAGES.—The Commission may bring a civil action in United States district court to obtain damages for violations of this Act in an amount no less than $50,000 and no more than $10,000,000 or 2% of an Organization's annual revenue, whichever is greater. In determining the appropriate amount, the court shall take into account the criteria set out in 15 U.S.C. 45(m)(1)(C).

(3) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.— Notwithstanding Sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) and otherwise applicable jurisdictional limitations, the Commission is authorized to enforce this Act with respect to any Organization engaged in Tracking, including:

(A) Common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and

(B) Organizations not organized to carry on business for their own profit or that of their members.

(4) COMMISSION AUTHORITY.— Nothing contained in this Act shall be construed to limit authority provided to the Commission under any other law.

(c) ENFORCEMENT BY STATES.—

(1) CIVIL ACTION.— A State is authorized to enforce this Act with respect residents of that State that have been affected by any violation of this Act. The State may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

(A) to enjoin further violation of this Act by the defendant; or

(B) to obtain damages on behalf of residents of the State, in the amount authorized under state law or as permitted under federal law, whichever is greater.

(2) RIGHTS OF FEDERAL REGULATORS.— The State shall serve prior written notice of any action under paragraph (1) upon the Federal Trade Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Federal Trade Commission shall have the right--

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein;

(C) to remove the action to the appropriate United States district court; and

(D) to file petitions for appeal.

(3) CONSTRUCTION.— Nothing in this Act shall be construed to prevent a State from exercising the powers conferred on the attorney general or applicable agency by the laws of that State.

(4) PREEMPTIVE ACTION BY THE COMMISSION.— If the Commission has filed a civil action for violation of this Act, no State shall file a civil action during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act as alleged in the complaint.

(d) ENFORCEMENT BY USERS.— Users from whom Identifiable Information has been Processed in violation of this Act may bring a civil action in a district court of the United States of appropriate jurisdiction—

(1) to enjoin further violation of this Act by the defendant; or

(2) to obtain damages, in the amount of $1000 or actual damages shown, whichever is greater.

(e) ATTORNEY FEES.— In the case of any successful action under this section, the court, in its discretion, may award the costs of the action and reasonable attorney fees to the Commission, the State, or the User.

Section 9. Severability of Provisions.

If any provision of this Act, or the application thereof to any person or circumstance, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons and circumstances shall not be affected thereby.

Section 10. Effective Date.

This Act shall enter into effect one year after the date of its enactment.