SB3081

LRB10223767SPS32958b

102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

SB3081

Introduced 1/11/2022, by Sen. Thomas Cullerton

SYNOPSIS AS INTRODUCED:

New Act

Creates the Do Not Track Act. Prohibits a party to a user action from tracking another user whenever the party receives a do-not-track signal indicating a user preference not to be tracked, with some exceptions. Provides that data that has been sufficiently de-identified such that it is rendered anonymous data may be processed for any purpose. Provides that a party may disregard a user's do-not-track signal when the user has given express affirmative consent to track. Provides that an organization may process data for specified uses if the organization: (i) limits the amount of identifiable data collected; (ii) limits the retention of identifiable data to no longer than what is reasonably needed for the permitted uses; (iii) uses anonymous data; (iv) processes the data separately from systems that are used for purposes other than the permitted uses; and (v) does not process the data beyond the permitted uses. Requires an organization that engages in tracking to 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. Prohibits a party from blocking a user's do-not-track signal. Provides that the Attorney General shall enforce the Act. Permits a user whose identifiable information has been processed in violation of the Act to bring a civil action in any court of competent jurisdiction. Preempts home rule powers. Effective January 1, 2023.

LRB102 23767 SPS 32958 b

A BILL FOR

AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Do Not Track Act.

Section 5. Definitions. As used in this Act:

"Anonymous data" means data which does not relate to an identified or identifiable user. Identifiable data may be rendered anonymous data if it has become de-identified to an extent that no user can be singled out or identified, either directly or indirectly, 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 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.

"Collect" means to receive identifiable data in a network interaction and to retain that data after the network interaction is complete.

"Commission" means the Federal Trade Commission.

"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.

"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 or 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.

"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) specifications published by the World Wide Web Consortium.

"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 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.

(3) The mere presence of 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.

"Identifiable data" means data from which the user can be singled out or identified, directly or indirectly, 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 derived through device fingerprinting and probabilistic techniques), and any

other data associated with such identifiers. Identifiable data does not include anonymous data.

"Network interaction" means an online connection consisting of an HTTP or HTTPS request and as many corresponding responses 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.

"Organization" means a legal entity. Such term does not include government agencies or users.

"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 Tracking Preference Expression (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.

"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.

"Process" means to collect, use, or share data.

"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.

"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.

"Share" means, with respect to collected data, to transfer or provide a copy of such data to any third party.

"Third party" means, for any user action, any party other than the user, a first party to that user action, or a service provider action on behalf of either the user or a first party.

"Tracking" or "track" means to (i) collect data regarding a user action of a particular user, (ii) process such data outside the context in which the user action occurred, (iii) facilitate the creation of a user profile, or (iv) 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 to the user.

"User" means a natural person residing in this State who uses the Internet.

"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.

"User agent" means any of the various client programs capable of initiating network interactions, including, but not

limited to, browsers, web-based robots, command-line tools, native applications, mobile apps, or Internet-connected devices.

Section 10. Response to do-not-track signals.

(a) In general. Except as permitted in this Section, 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 the context of the user actions 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 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 tracing does not constitute express affirmation consent for the purposes of this Act. Likewise, agreement obtained through a user interface designed or manipulated with the purpose of 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 20.

(4) Permitted uses.

(A) In general. An organization may process data for the uses specified in subparagraphs (B), (C), (D), (E), (F), and (G), provided the organization:

(i) limits the amount of identifiable data collected to that which is strictly needed for the permitted uses;

(ii) limits the retention of identifiable data to no longer than what is reasonably needed for

the permitted uses;

(iii) uses anonymous data to the extent the permitted uses can be achieved with such data, or otherwise de-identifies the identifiable data to the greatest extent that is compatible with the permitted uses;

(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 uses.

(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 the 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 of 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 15. Contractual obligations and liability. 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 20. Transparency. 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. 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 the 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 25. 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 30. 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 Attorney General. Whenever the Attorney General has reasonable cause to believe that a party or organization has engaged in a violation of this Act, the

Attorney General shall enforce the provisions of this Act by bringing a civil action on behalf of the people of this State in a court of competent jurisdiction:

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

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

(c) A user from whom identifiable information has been processed in violation of this Act may bring a civil action in any court of competent jurisdiction:

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

(2) to obtain damages, in the amount of $1,000 or actual damages shown, whichever is greater.

(d) 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 State or the user.

Section 35. Home rule preemption. Except as otherwise provided in this Act, the regulation of the activities described in this Act are the exclusive powers and functions of the State. Except as otherwise provided in this Act, a unit of local government, including a home rule unit, may not regulate the activities described in this Act. This Section is

a denial and limitation of home rule powers and functions under subsection (h) of Section 6 of Article VII of the Illinois Constitution.

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

Section 99. Effective date. This Act takes effect January 1, 2023.