STATE OF NEW YORK

8149--A

2023-2024 Regular Sessions

IN ASSEMBLY

October 13, 2023

Introduced by M. of A. ROZIC, REYES, SHIMSKY, MAGNARELLI, HEVESI, BUTTENSCHON, FAHY, DICKENS, McMAHON, GLICK, DE LOS SANTOS, DURSO, McDONOUGH, GANDOLFO, SIMON, ZACCARO, DeSTEFANO, WALLACE, BERGER, BURDICK, SEAWRIGHT, McDONALD, BEEPHAN, SMULLEN, MANKTELOW, J. A. GIGLIO, SLATER, ARDILA, SILLITTI, DARLING, K. BROWN, EPSTEIN, LEVENBERG, WEPRIN, BICHOTTE HERMELYN, LUPARDO, MIKULIN, PAULIN, SOLAGES, SANTABARBARA, L. ROSENTHAL, DAVILA, BURGOS, CHANDLER-WATERMAN, TAYLOR, ZEBROWSKI, JENSEN, KIM, RIVERA, ZINERMAN, MAHER, WALKER, CUNNINGHAM, CONRAD, CLARK, JACKSON, DAIS, RAJKUMAR, FALL, LUNSFORD, FORREST, LEE, GIBBS, ANDERSON, LAVINE, STERN, BRAUNSTEIN, DINOWITZ, JEAN-PIERRE, SEPTIMO, KELLES, CARROLL, MAMDANI, HUNTER, BARRETT, BRONSON, PHEFFER AMATO, O'DONNELL, COOK, GUNTHER, BURKE, AUBRY, JONES, STIRPE, SAYEGH, RAGA, GALLAHAN, TAPIA, THIELE, GALLAGHER, ALVAREZ, SIMONE, EICHENSTEIN, PRETLOW, MORINELLO, SHRESTHA, EACHUS, MEEKS, JACOBSON, BRABENEC -- Multi-Sponsored by -- M. of A. GONZALEZ-ROJAS, WOERNER -- read once and referred to the Committee on Science and Technology -- recommitted to the Committee on Science and Technology in accordance with Assembly Rule 3, sec. 2 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to establishing the New York child data protection act

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The general business law is amended by adding a new article 39-FF to read as follows:

ARTICLE 39-FF
NEW YORK CHILD DATA PROTECTION ACT
Section 899-ee. Definitions.
899-ff. Privacy protection by default.
899-gg. Processors.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD13150-12-4

899-hh. Ongoing coverage.
899-ii. Respecting user-provided age flags.
899-jj. Protections for third-party operators.
899-kk. Rulemaking authority.
899-ll. Scope.
899-mm. Remedies.

§ 899-ee. Definitions. For purposes of this article, the following terms shall have the following meanings:

1. "Covered user" shall mean a user of a website, online service, online application, mobile application, or connected device, or portion thereof, in the state of New York who is:

(a) actually known by the operator of such website, online service, online application, mobile application, or connected device to be a minor; or

(b) using a website, online service, online application, mobile application, or connected device primarily directed to minors.

2. "Minor" shall mean a natural person under the age of eighteen.

3. "Operator" shall mean any person who operates or provides a website on the internet, online service, online application, mobile application, or connected device, and who, alone or jointly with others, controls the purposes and means of processing personal data. A person that acts as both an operator and processor shall comply with the applicable obligations of an operator and the obligations of a processor, depending on its role with respect to each specific processing of personal data.

4. "Personal data" shall mean any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person or device.

5. "Process" or "processing" shall mean an operation or set of operations performed on personal data, including but not limited to the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, modification, or deidentification of personal data.

6. "Primarily directed to minors" shall mean a website, online service, online application, mobile application, or connected device, or a portion thereof, that is targeted to minors. A website, online service, online application, mobile application, or connected device, or portion thereof, shall not be deemed directed primarily to minors solely because such website, online service, online application, mobile application, or connected device, or portion thereof refers or links to any other website, online service, online application, mobile application, or connected device directed to minors by using information location tools, including a directory, index, reference, pointer, or hypertext link. A website, online service, online application, mobile application, or connected device, or portion thereof, shall be deemed directed to minors when it has actual knowledge that it is collecting personal data of users directly from users of another website, online service, online application, mobile application, or connected device primarily directed to minors.

7. "Sell" shall mean to share personal data for monetary or other valuable consideration. "Selling" shall not include the sharing of personal data for monetary or other valuable consideration to another person as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which that person assumes control of all or part of the operator's assets or the sharing of personal data with a processor.

8. "Processor" shall mean any person who processes data on behalf of the operator. A person that acts as both an operator and processor shall comply with the applicable obligations of an operator and the obligations of a processor, depending on its role with respect to each specific processing of personal data.

9. "Third-party operator" shall mean an operator who is not the operator:

(a) with whom the user intentionally and directly interacts; or

(b) that collects personal data from the direct and current interactions with the user.

§ 899-ff. Privacy protection by default. 1. Except as provided for in subdivision six of this section and section eight hundred ninety-nine-jj of this article, an operator shall not process, or allow a processor to process, the personal data of a covered user collected through the use of a website, online service, online application, mobile application, or connected device, or allow a third-party operator to collect the personal data of a covered user collected through the operator's website, online service, online application, mobile application, or connected device unless and to the extent:

(a) the covered user is twelve years of age or younger and processing is permitted under 15 U.S.C. § 6502 and its implementing regulations; or

(b) the covered user is thirteen years of age or older and processing is strictly necessary for an activity set forth in subdivision two of this section, or informed consent has been obtained as set forth in subdivision three of this section.

2. For the purposes of paragraph (b) of subdivision one of this section, the processing of personal data of a covered user is permissible where it is strictly necessary for the following permissible purposes:

(a) providing or maintaining a specific product or service requested by the covered user;

(b) conducting the operator's internal business operations. For purposes of this paragraph, such internal business operations shall not include any activities related to marketing, advertising, research and development, providing products or services to third parties, or prompting covered users to use the website, online service, online application, mobile application, or connected device when it is not in use;

(c) identifying and repairing technical errors that impair existing or intended functionality;

(d) protecting against malicious, fraudulent, or illegal activity;

(e) investigating, establishing, exercising, preparing for, or defending legal claims;

(f) complying with federal, state, or local laws, rules, or regulations;

(g) complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(h) detecting, responding to, or preventing security incidents or threats; or

(i) protecting the vital interests of a natural person.

3. (a) For the purposes of paragraph (b) of subdivision one of this section, to process personal data of a covered user where such processing is not strictly necessary under subdivision two of this section, informed consent must be obtained from the covered user either through a device communication or signal pursuant to the provisions of subdivision

two of section eight hundred ninety-nine-ii of this article or through a request. Requests for such informed consent shall:

(i) be made separately from any other transaction or part of a transaction;

(ii) be made in the absence of any mechanism that has the purpose or substantial effect of obscuring, subverting, or impairing a covered user's decision-making regarding authorization for the processing;

(iii) clearly and conspicuously state that the processing for which the consent is requested is not strictly necessary, and that the covered user may decline without preventing continued use of the website, online service, online application, mobile application, or connected device; and

(iv) clearly present an option to refuse to provide consent as the most prominent option.

(b) Such informed consent, once given, shall be freely revocable at any time, and shall be at least as easy to revoke as it was to provide.

(c) If a covered user declines to provide or revokes informed consent for processing, another request may not be made for such processing for the following calendar year, however an operator may make available a mechanism that a covered user can use unprompted and at the user's discretion to provide informed consent.

(d) If a covered user's device communicates or signals that the covered user declines to provide informed consent for processing pursuant to the provisions of subdivision two of section eight hundred ninety-nine-ii of this article, an operator shall not request informed consent for such processing, however an operator may make available a mechanism that a covered user can use unprompted and at the user's discretion to provide informed consent.

4. Except where processing is strictly necessary to provide a product, service, or feature, an operator may not withhold, degrade, lower the quality, or increase the price of any product, service, or feature to a covered user due to the operator not obtaining verifiable parental consent under 15 U.S.C. § 6502 and its implementing regulations or informed consent under subdivision three of this section.

5. Except as provided for in section eight hundred ninety-nine-jj of this article, an operator shall not purchase or sell, or allow a processor or third-party operator to purchase or sell, the personal data of a covered user.

6. Within thirty days of determining or being informed that a user is a covered user, an operator shall:

(a) dispose of, destroy, or delete and direct all of its processors to dispose of, destroy, or delete all personal data of such covered user that it maintains, unless processing such personal data is permitted under 15 U.S.C. § 6502 and its implementing regulations, is strictly necessary for an activity listed in subdivision two of this section, or informed consent is obtained as set forth in subdivision three of this section; and

(b) notify any third-party operators to whom it knows it disclosed personal data of that covered user, and any third-party operators it knows it allowed to process the personal data that may include the personal data of that user, that the user is a covered user.

7. Except as provided for in section eight hundred ninety-nine-jj of this article, prior to disclosing personal data to a third-party operator, or permitting a third-party operator to collect personal data from the operator's website, online service, online application, mobile

application, connected device, or portion thereof, the operator shall disclose to the third-party operator:

(a) when their website, online service, online application, mobile application, connected device, or portion thereof, is primarily directed to minors; or

(b) when the personal data concerns a covered user.

§ 899-gg. Processors. 1. Except as provided for in section eight hundred ninety-nine-jj of this article, no operator or processor shall disclose the personal data of a covered user to a third party, or allow the processing of the personal data of a covered user by a third party, without a written, binding agreement governing such disclosure or processing. Such agreement shall clearly set forth instructions for the nature and purpose of the processor's processing of the personal data, instructions for using or further disclosing the personal data, and the rights and obligations of both parties.

2. Processors shall process the personal data of covered users only when permitted by the terms of the agreement pursuant to subdivision one of this section, unless otherwise required by federal, state, or local laws, rules, or regulations.

3. A processor shall, at the direction of the operator, dispose of, destroy, or delete personal data, and notify any other processor to which it disclosed the personal data of the operator's direction, unless retention of the personal data is required by federal, state, or local laws, rules, or regulations. The processor shall provide evidence of such deletion to the operator within thirty days of the deletion request.

4. A processor shall delete or return to the operator all personal data of covered users at the end of its provision of services, unless retention of the personal data is required by federal, state, or local laws, rules, or regulations. The processor shall provide evidence of such deletion to the operator within thirty days of the deletion request.

5. An agreement pursuant to subdivision one of this section shall require that the processor:

(a) process the personal data of covered users only pursuant to the instructions of the operator, unless otherwise required by federal, state, or local laws, rules, or regulations;

(b) assist the operator in meeting the operator's obligations under this article. The processor shall, taking into account the nature of processing and the information available to them, assist the operator by taking appropriate technical and organizational measures, to the extent practicable, for the fulfillment of the operator's obligation to delete personal data pursuant to section eight hundred ninety-nine-ff of this article;

(c) upon reasonable request of the operator, make available to the operator all information in its possession necessary to demonstrate the processor's compliance with the obligations in this section;

(d) allow, and cooperate with, reasonable assessments by the operator or the operator's designated assessor for purposes of evaluating compliance with the obligations of this article. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this article using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the operator upon request; and

(e) notify the operator a reasonable time in advance before disclosing or transferring the personal data of covered users to any further processors, which may be in the form of a regularly updated list of further processors that may access personal data of covered users.

§ 899-hh. Ongoing coverage. 1. Upon learning that a user is no longer a covered user, an operator:

(a) shall not process the personal data of the covered user that would otherwise be subject to the provisions of this article until it receives informed consent pursuant to subdivision three of section eight hundred ninety-nine-ff of this article, and

(b) shall provide notice to such user that they may no longer be entitled to all of the protections and rights provided under this article.

2. Upon learning that a user is no longer a covered user, an operator shall provide notice to such user that such user is no longer covered by the protections and rights provided under this article.

§ 899-ii. Respecting user-provided age flags. 1. For the purposes of this article, an operator shall treat a user as a covered user if the user's device communicates or signals that the user is or shall be treated as a minor, including through a browser plug-in or privacy setting, device setting, or other mechanism that complies with regulations promulgated by the attorney general.

2. For the purposes of subdivision three of section eight hundred ninety-nine-ff of this article, an operator shall adhere to any clear and unambiguous communications or signals from a covered user's device, including through a browser plug-in or privacy setting, device setting, or other mechanism, concerning processing that the covered user consents to or declines to consent to. An operator shall not adhere to unclear or ambiguous communications or signals from a covered user's device, and shall instead request informed consent pursuant to the provisions of paragraph a of subdivision three of section eight hundred ninety-nine-ff of this article.

§ 899-jj. Protections for third-party operators. Sections eight hundred ninety-nine-ff and eight hundred ninety-nine-gg of this article shall not apply where a third-party operator is processing the personal data of a covered user of another website, online service, online application, mobile application, or connected device, or portion thereof, provided that the third-party operator received reasonable written representations that the covered user provided informed consent for such processing, or:

1. the operator does not have actual knowledge that the covered user is a minor; and

2. the operator does not have actual knowledge that the other website, online service, online application, mobile application, or connected device, or portion thereof, is primarily directed to minors.

§ 899-kk. Rulemaking authority. The attorney general may promulgate such rules and regulations as are necessary to effectuate and enforce the provisions of this article.

§ 899-ll. Scope. 1. This article shall apply to conduct that occurs in whole or in part in the state of New York. For purposes of this article, commercial conduct takes place wholly outside of the state of New York if the business collected such information while the covered user was outside of the state of New York, no part of the use of the covered user's personal data occurred in the state of New York, and no personal data collected while the covered user was in the state of New York is used.

2. Nothing in this article shall be construed to prohibit an operator from storing a covered user's personal data that was collected pursuant to section eight hundred ninety-nine-ff of this article when such covered user is in the state.

3. Nothing in this article shall be construed to impose liability for commercial activities or actions by operators subject to 15 U.S.C. 6501 that is inconsistent with the treatment of such activities or actions under 15 U.S.C. 6502.

§ 899-mm. Remedies. Whenever it appears to the attorney general, either upon complaint or otherwise, that any person, within or outside the state, has engaged in or is about to engage in any of the acts or practices stated to be unlawful in this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits or gains obtained directly or indirectly by any such violation, including but not limited to the destruction of unlawfully obtained data, to obtain damages caused directly or indirectly by any such violation, to obtain civil penalties of up to five thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

§ 2. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. It is hereby declared to be the intent of the legislature that this act would have been enacted even if such invalid provisions had not been included herein.

§ 3. This act shall take effect one year after it shall have become a law. Effective immediately, the addition, amendment and/or repeal of any rule or regulation necessary for the implementation of this act on its effective date are authorized to be made and completed on or before such effective date.