STATE OF NEW YORK

_____

7695--B

2023-2024 Regular Sessions

IN SENATE

October 13, 2023
_____

Introduced by Sens. GOUNARDES, BAILEY, BORRELLO, BROUK, CHU, CLEARE, COMRIE, FERNANDEZ, GONZALEZ, HARCKHAM, HINCHEY, HOYLMAN-SIGAL, JACKSON, KAVANAGH, KRUEGER, LIU, MANNION, MARTINEZ, MAY, MAYER, MURRAY, MYRIE, PALUMBO, PARKER, RAMOS, RHOADS, RIVERA, RYAN, SALAZAR, SEPULVEDA, SERRANO, SKOUFIS, STAVISKY, TEDISCO, WEBB, WEBER, WEIK -- read twice and ordered printed, and when printed to be committed to the Committee on Rules -- recommitted to the Committee on Internet and Technology in accordance with Senate Rule 6, sec. 8 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- 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:

1   Section 1. The general business law is amended by adding a new article
2 39-FF to read as follows:
3   ARTICLE 39-FF
4   NEW YORK CHILD DATA PROTECTION ACT
5 Section 899-ee. Definitions.
6   899-ff. Privacy protection by default.
7   899-gg. Processors.
8   899-hh. Ongoing coverage.
9   899-ii. Respecting user-provided age flags.
10   899-jj. Protections for third-party operators.
11   899-kk. Rulemaking authority.
12   899-ll. Scope.
13   899-mm. Remedies.
14   § 899-ee. Definitions. For purposes of this article, the following
15 terms shall have the following meanings:

1   1. "Covered user" shall mean a user of a website, online service,
2 online application, mobile application, or connected device, or portion
3 thereof, in the state of New York who is:
4   (a) actually known by the operator of such website, online service,
5 online application, mobile application, or connected device to be a
6 minor; or
7   (b) using a website, online service, online application, mobile appli-
8 cation, or connected device primarily directed to minors.
9   2. "Minor" shall mean a natural person under the age of eighteen.
10   3. "Operator" shall mean any person who operates or provides a website
11 on the internet, online service, online application, mobile application,
12 or connected device, and who, alone or jointly with others, controls the
13 purposes and means of processing personal data. A person that acts as
14 both an operator and processor shall comply with the applicable obli-
15 gations of an operator and the obligations of a processor, depending on
16 its role with respect to each specific processing of personal data.
17   4. "Personal data" shall mean any data that identifies or could
18 reasonably be linked, directly or indirectly, with a specific natural
19 person or device.
20   5. "Process" or "processing" shall mean an operation or set of oper-
21 ations performed on personal data, including but not limited to the
22 collection, use, access, sharing, sale, monetization,   analysis,
23 retention, creation, generation, derivation, recording, organization,
24 structuring, storage, disclosure, transmission, disposal, licensing,
25 destruction, deletion, modification, or deidentification of personal
26 data.
27   6. "Primarily directed to minors" shall mean a website, online
28 service, online application, mobile application, or connected device, or
29 a portion thereof, that is targeted to minors. A website, online
30 service, online application, mobile application, or connected device, or
31 portion thereof, shall not be deemed directed primarily to minors solely
32 because such website, online service, online application, mobile appli-
33 cation, or connected device, or portion thereof refers or links to any
34 other website, online service, online application, mobile application,
35 or connected device directed to minors by using information location
36 tools, including a directory, index, reference, pointer, or hypertext
37 link. A website, online service, online application, mobile application,
38 or connected device, or portion thereof, shall be deemed directed to
39 minors when it has actual knowledge that it is collecting personal data
40 of users directly from users of another website, online service, online
41 application, mobile application, or connected device primarily directed
42 to minors.
43   7. "Sell" shall mean to share personal data for monetary or other
44 valuable consideration. "Selling" shall not include the sharing of
45 personal data for monetary or other valuable consideration to another
46 person as an asset that is part of a merger, acquisition, bankruptcy, or
47 other transaction in which that person assumes control of all or part of
48 the operator's assets or the sharing of personal data with a processor.
49   8. "Processor" shall mean any person who processes data on behalf of
50 the operator. A person that acts as both an operator and processor shall
51 comply with the applicable obligations of an operator and the obli-
52 gations of a processor, depending on its role with respect to each
53 specific processing of personal data.
54   9. "Third-party operator" shall mean an operator who is not the oper-
55 ator:
56   (a) with whom the user intentionally and directly interacts; or

 1   (b) that collects personal data from the direct and current inter-
 2 actions with the user.
 3   § 899-ff. Privacy protection by default. 1. Except as provided for in
 4 subdivision six of this section and section eight hundred ninety-nine-jj
 5 of this article, an operator shall not process, or allow a processor to
 6 process, the personal data of a covered user collected through the use
 7 of a website, online service, online application, mobile application, or
 8 connected device, or allow a third-party operator to collect the
 9 personal data of a covered user collected through the operator's
10 website, online service, online application, mobile application, or
11 connected device unless and to the extent:
12   (a) the covered user is twelve years of age or younger and processing
13 is permitted under 15 U.S.C. § 6502 and its implementing regulations; or
14   (b) the covered user is thirteen years of age or older and processing
15 is strictly necessary for an activity set forth in subdivision two of
16 this section, or informed consent has been obtained as set forth in
17 subdivision three of this section.
18   2. For the purposes of paragraph (b) of subdivision one of this
19 section, the processing of personal data of a covered user is permissi-
20 ble where it is strictly necessary for the following permissible
21 purposes:
22   (a) providing or maintaining a specific product or service requested
23 by the covered user;
24   (b) conducting the operator's internal business operations. For
25 purposes of this paragraph, such internal business operations shall not
26 include any activities related to marketing, advertising, research and
27 development, providing products or services to third parties, or prompt-
28 ing covered users to use the website, online service, online applica-
29 tion, mobile application, or connected device when it is not in use;
30   (c) identifying and repairing technical errors that impair existing or
31 intended functionality;
32   (d) protecting against malicious, fraudulent, or illegal activity;
33   (e) investigating, establishing, exercising, preparing for, or defend-
34 ing legal claims;
35   (f) complying with federal, state, or local laws, rules, or regu-
36 lations;
37   (g) complying with a civil, criminal, or regulatory inquiry, investi-
38 gation, subpoena, or summons by federal, state, local, or other govern-
39 mental authorities;
40   (h) detecting, responding to, or preventing security incidents or
41 threats; or
42   (i) protecting the vital interests of a natural person.
43   3. (a) For the purposes of paragraph (b) of subdivision one of this
44 section, to process personal data of a covered user where such process-
45 ing is not strictly necessary under subdivision two of this section,
46 informed consent must be obtained from the covered user either through a
47 device communication or signal pursuant to the provisions of subdivision
48 two of section eight hundred ninety-nine-ii of this article or through a
49 request. Requests for such informed consent shall:
50   (i) be made separately from any other transaction or part of a trans-
51 action;
52   (ii) be made in the absence of any mechanism that has the purpose or
53 substantial effect of obscuring, subverting, or impairing a covered
54 user's decision-making regarding authorization for the processing;
55   (iii) clearly and conspicuously state that the processing for which
56 the consent is requested is not strictly necessary, and that the covered

1 user may decline without preventing continued use of the website, online
2 service, online application, mobile application, or connected device;
3 and
4   (iv) clearly present an option to refuse to provide consent as the
5 most prominent option.
6   (b) Such informed consent, once given, shall be freely revocable at
7 any time, and shall be at least as easy to revoke as it was to provide.
8   (c) If a covered user declines to provide or revokes informed consent
9 for processing, another request may not be made for such processing for
10 the following calendar year, however an operator may make available a
11 mechanism that a covered user can use unprompted and at the user's
12 discretion to provide informed consent.
13   (d) If a covered user's device communicates or signals that the
14 covered user declines to provide informed consent for processing pursu-
15 ant to the provisions of subdivision two of section eight hundred nine-
16 ty-nine-ii of this article, an operator shall not request informed
17 consent for such processing, however an operator may make available a
18 mechanism that a covered user can use unprompted and at the user's
19 discretion to provide informed consent.
20   4. Except where processing is strictly necessary to provide a product,
21 service, or feature, an operator may not withhold, degrade, lower the
22 quality, or increase the price of any product, service, or feature to a
23 covered user due to the operator not obtaining verifiable parental
24 consent under 15 U.S.C. § 6502 and its implementing regulations or
25 informed consent under subdivision three of this section.
26   5. Except as provided for in section eight hundred ninety-nine-jj of
27 this article, an operator shall not purchase or sell, or allow a proces-
28 sor or third-party operator to purchase or sell, the personal data of a
29 covered user.
30   6. Within thirty days of determining or being informed that a user is
31 a covered user, an operator shall:
32   (a) dispose of, destroy, or delete and direct all of its processors to
33 dispose of, destroy, or delete all personal data of such covered user
34 that it maintains, unless processing such personal data is permitted
35 under 15 U.S.C. § 6502 and its implementing regulations, is strictly
36 necessary for an activity listed in subdivision two of this section, or
37 informed consent is obtained as set forth in subdivision three of this
38 section; and
39   (b) notify any third-party operators to whom it knows it disclosed
40 personal data of that covered user, and any third-party operators it
41 knows it allowed to process the personal data that may include the
42 personal data of that user, that the user is a covered user.
43   7. Except as provided for in section eight hundred ninety-nine-jj of
44 this article, prior to disclosing personal data to a third-party opera-
45 tor, or permitting a third-party operator to collect personal data from
46 the operator's website, online service, online application, mobile
47 application, connected device, or portion thereof, the operator shall
48 disclose to the third-party operator:
49   (a) when their website, online service, online application, mobile
50 application, connected device, or portion thereof, is primarily directed
51 to minors; or
52   (b) when the personal data concerns a covered user.
53   § 899-gg. Processors. 1. Except as provided for in section eight
54 hundred ninety-nine-jj of this article, no operator or processor shall
55 disclose the personal data of a covered user to a third party, or allow
56 the processing of the personal data of a covered user by a third party,

 1 without a written, binding agreement governing such disclosure or proc-
 2 essing. Such agreement shall clearly set forth instructions for the
 3 nature and purpose of the processor's processing of the personal data,
 4 instructions for using or further disclosing the personal data, and the
 5 rights and obligations of both parties.
 6   2. Processors shall process the personal data of covered users only
 7 when permitted by the terms of the agreement pursuant to subdivision one
 8 of this section, unless otherwise required by federal, state, or local
 9 laws, rules, or regulations.
10   3. A processor shall, at the direction of the operator, dispose of,
11 destroy, or delete personal data, and notify any other processor to
12 which it disclosed the personal data of the operator's direction, unless
13 retention of the personal data is required by federal, state, or local
14 laws, rules, or regulations. The processor shall provide evidence of
15 such deletion to the operator within thirty days of the deletion
16 request.
17   4. A processor shall delete or return to the operator all personal
18 data of covered users at the end of its provision of services, unless
19 retention of the personal data is required by federal, state, or local
20 laws, rules, or regulations. The processor shall provide evidence of
21 such deletion to the operator within thirty days of the deletion
22 request.
23   5. An agreement pursuant to subdivision one of this section shall
24 require that the processor:
25   (a) process the personal data of covered users only pursuant to the
26 instructions of the operator, unless otherwise required by federal,
27 state, or local laws, rules, or regulations;
28   (b) assist the operator in meeting the operator's obligations under
29 this article. The processor shall, taking into account the nature of
30 processing and the information available to them, assist the operator by
31 taking appropriate technical and organizational measures, to the extent
32 practicable, for the fulfillment of the operator's obligation to delete
33 personal data pursuant to section eight hundred ninety-nine-ff of this
34 article;
35   (c) upon reasonable request of the operator, make available to the
36 operator all information in its possession necessary to demonstrate the
37 processor's compliance with the obligations in this section;
38   (d) allow, and cooperate with, reasonable assessments by the operator
39 or the operator's designated assessor for purposes of evaluating compli-
40 ance with the obligations of this article. Alternatively, the processor
41 may arrange for a qualified and independent assessor to conduct an
42 assessment of the processor's policies and technical and organizational
43 measures in support of the obligations under this article using an
44 appropriate and accepted control standard or framework and assessment
45 procedure for such assessments. The processor shall provide a report of
46 such assessment to the operator upon request; and
47   (e) notify the operator a reasonable time in advance before disclosing
48 or transferring the personal data of covered users to any further
49 processors, which may be in the form of a regularly updated list of
50 further processors that may access personal data of covered users.
51   § 899-hh. Ongoing coverage. 1. Upon learning that a user is no longer
52 a covered user, an operator:
53   (a) shall not process the personal data of the covered user that would
54 otherwise be subject to the provisions of this article until it receives
55 informed consent pursuant to subdivision three of section eight hundred
56 ninety-nine-ff of this article, and

(b) shall provide notice to such user that they may no longer be enti-
tled 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 regu-
lations 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 appli-
cation, 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

1   practices stated to be unlawful in this article, the attorney general
2   may bring an action or special proceeding in the name and on behalf of
3   the people of the state of New York to enjoin any violation of this
4   article, to obtain restitution of any moneys or property obtained
5   directly or indirectly by any such violation, to obtain disgorgement of
6   any profits or gains obtained directly or indirectly by any such
7   violation, including but not limited to the destruction of unlawfully
8   obtained data, to obtain damages caused directly or indirectly by any
9   such violation, to obtain civil penalties of up to five thousand dollars
10 per violation, and to obtain any such other and further relief as the
11 court may deem proper, including preliminary relief.
12   § 2. Severability. If any clause, sentence, paragraph, subdivision,
13 section or part of this act shall be adjudged by any court of competent
14 jurisdiction to be invalid, such judgment shall not affect, impair, or
15 invalidate the remainder thereof, but shall be confined in its operation
16 to the clause, sentence, paragraph, subdivision, section or part thereof
17 directly involved in the controversy in which such judgment shall have
18 been rendered. It is hereby declared to be the intent of the legislature
19 that this act would have been enacted even if such invalid provisions
20 had not been included herein.
21   § 3. This act shall take effect one year after it shall have become a
22 law. Effective immediately, the addition, amendment and/or repeal of any
23 rule or regulation necessary for the implementation of this act on its
24 effective date are authorized to be made and completed on or before such
25 effective date.