



## 103RD GENERAL ASSEMBLY

### State of Illinois

2023 and 2024

HB5380

Introduced 2/9/2024, by Rep. Jennifer Gong-Gershowitz

#### SYNOPSIS AS INTRODUCED:

New Act  
815 ILCS 505/2EEEE new

Creates the Let Parents Choose Protection Act. Provides that the Act may be referred to as Sammy's Law. Provides that, before August 1, 2025, or within 30 days after a service becomes a large social media platform after August 1, 2025, a large social media platform provider shall create, maintain, and make available to any third-party safety software provider a set of third-party-accessible real time application programming interfaces, including any information necessary to use the interfaces, by which a child, if the child is 13 years of age or older, or a parent or legal guardian of a child, may delegate permission to the third-party safety software provider to: (1) manage the child's online interactions, content, and account settings on the large social media platform on the same terms as the child; and (2) initiate secure transfers of user data from the large social media platform in a commonly used and machine-readable format to the third-party safety software provider. Sets forth disclosure requirements to the child and the parents or guardians of a child; requirements of third-party safety software providers; and liability of third-party safety software providers. Provides that a violation of any of the provisions of the Act is an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Amends the Consumer Fraud and Deceptive Business Practices Act to make a conforming change. Effective June 1, 2025.

LRB103 38832 SPS 68969 b

1 AN ACT concerning business.

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

4 Section 1. Short title; references to Act.

5 (a) Short title. This Act may be cited as the Parental  
6 Digital Choice Act.

7 (b) References to Act. This Act may be referred to as  
8 Sammy's Law.

9 Section 5. Findings and intent.

10 (a) The General Assembly finds and declares the following:

11 (1) Parents and legal guardians should be empowered to  
12 use the services of third-party safety software providers  
13 to protect their children from certain harms on large  
14 social media platforms.

15 (2) Dangers like cyberbullying, human trafficking,  
16 illegal drug distribution, sexual harassment, and violence  
17 perpetrated, facilitated, or exacerbated through the use  
18 of certain large social media platforms have harmed  
19 children on those platforms.

20 (b) It is the intent of the General Assembly to require  
21 large social media platforms to create, maintain, and make  
22 available to third-party safety software providers a set of  
23 real-time application programming interfaces, through which a

1 child or a parent or legal guardian of a child may delegate  
2 permission to a third-party safety software provider to manage  
3 the child's online interactions, content, and account settings  
4 on the large social media platform on the same terms as the  
5 child, and for other purposes.

6 Section 10. Definitions. As used in this Act:

7 "Child" means any individual under 18 years of age who has  
8 registered an account with a large social media platform.

9 "Large social media platform" means a service that:

10 (1) is provided through an Internet website, a mobile  
11 application, or both;

12 (2) does not prohibit the use of the service by a  
13 child;

14 (3) includes features that enable a child to share  
15 images, text, or video through the Internet with other  
16 users of the service whom the child has met, identified,  
17 or become aware of solely through the use of the service;  
18 and

19 (4) has more than 100,000,000 monthly global active  
20 users or generates more than \$1,000,000,000 in gross  
21 revenue per year, adjusted yearly for inflation, or both.

22 "Large social media platform" does not include a service  
23 that:

24 (1) primarily serves to facilitate the sale or  
25 provision of professional services or the sale of

1 commercial products;

2 (2) primarily serves to provide news or information  
3 and the service does not offer the ability for content to  
4 be sent by a user directly to a child; or

5 (3) has features that enable a user who communicates  
6 directly with a child through a message, including a text,  
7 audio, or video message, not otherwise available to other  
8 users of the service, to add other users to that message  
9 that the child may not have otherwise met, identified, or  
10 become aware of solely through the use of the service and  
11 does not have any features that enable a child to share  
12 images, text, or video through the Internet with other  
13 users of the service whom the child has met, identified,  
14 or become aware of solely through the use of the service.

15 "Large social media platform provider" means any person  
16 who, for a commercial purpose provides, manages, operates, or  
17 controls a large social media platform.

18 "Third-party safety software provider" means any person  
19 who, for a commercial purpose, is authorized by a child, if the  
20 child is 13 years of age or older, or a parent or legal  
21 guardian of a child, to interact with a large social media  
22 platform to manage the child's online interactions, content,  
23 or account settings for the sole purpose of protecting the  
24 child from harm, including physical or emotional harm.

25 "User data" means any information needed to have a profile  
26 on a large social media platform or content on a large social

1 media platform, including images, video, audio, or text, that  
2 is created by or sent to a child on or through the child's  
3 account with the platform, and the information or content is  
4 created by or sent to the child while a delegation described in  
5 Section 15 is in effect with respect to the account. For the  
6 purposes of this definition, information shall only be  
7 considered "user data" for 90 days after the date the  
8 information or content is created by or sent to the child.

9 Section 15. Delegation of permission to third-party  
10 software provider.

11 (a) Before August 1, 2025, or within 30 days after a  
12 service becomes a large social media platform after August 1,  
13 2025, a large social media platform provider shall create,  
14 maintain, and make available to any third-party safety  
15 software provider that satisfies the requirements described in  
16 Section 20 a set of third-party-accessible real time  
17 application programming interfaces, including any information  
18 necessary to use the interfaces, by which a child, if the child  
19 is 13 years of age or older, or a parent or legal guardian of a  
20 child, may delegate permission to the third-party safety  
21 software provider to:

22 (1) manage the child's online interactions, content,  
23 and account settings on the large social media platform on  
24 the same terms as the child; and

25 (2) initiate secure transfers of user data from the

1 large social media platform in a commonly used and  
2 machine-readable format to the third-party safety software  
3 provider, and the frequency of the transfers may not be  
4 limited by the large social media platform provider to  
5 less than once per hour.

6 (b) Once a child or a parent or legal guardian of a child  
7 makes a delegation under subsection (a), the large social  
8 media platform provider shall make the application programming  
9 interfaces and information available to the third-party safety  
10 software provider on an ongoing basis until one of the  
11 following applies:

12 (1) the delegation is revoked by the child or the  
13 child's parent or legal guardian;

14 (2) the child's account is disabled with the large  
15 social media platform;

16 (3) the third-party safety software provider rejects  
17 the delegation; or

18 (4) one or more of the affirmations made by the  
19 third-party safety software provider under Section 20 is  
20 no longer true.

21 (c) A large social media platform provider shall establish  
22 and implement reasonable policies, practices, and procedures  
23 concerning the secure transfer of user data under a delegation  
24 as described in subsection (a) from the large social media  
25 platform to a third-party safety software provider in order to  
26 mitigate any risks related to user data.

1 (d) If a delegation is made by a child or a parent or legal  
2 guardian of a child as described in subsection (a) with  
3 respect to the account of the child with a large social media  
4 platform. The large social media platform provider shall:

5 (1) disclose to the child and, if the parent or legal  
6 guardian made the delegation, the parent or legal guardian  
7 the fact that the delegation has been made;

8 (2) provide to the child and, if the parent or legal  
9 guardian made the delegation, the parent or legal guardian  
10 a summary of what user data is being transferred to the  
11 third-party safety software provider; and

12 (3) provide any update to the summary as described in  
13 paragraph (2) as necessary to reflect any change to what  
14 user data is being transferred to the third-party safety  
15 software provider.

16 (e) A third-party safety software provider shall not  
17 disclose any user data obtained under this Section to any  
18 person except:

19 (1) in compliance with a lawful request from a  
20 governmental body, including for law enforcement purposes  
21 or for judicial or administrative proceedings by means of  
22 a court order or a court ordered warrant, a subpoena or  
23 summons issued by a judicial officer, or a grand jury  
24 subpoena;

25 (2) to the extent that the disclosure is required by  
26 law and the disclosure complies with and is limited to the

1 requirements of the law;

2 (3) to a reasonable parent or caregiver of a child, if  
3 the third-party safety software provider believes in good  
4 faith that the child is at foreseeable risk or currently  
5 experiencing any of the following harms:

6 (A) suicide;

7 (B) anxiety;

8 (C) depression;

9 (D) eating disorders;

10 (E) violence, including being the victim of or  
11 planning to commit or facilitate battery under Section  
12 12-3 of the Criminal Code of 2012 and assault under  
13 Section 12-1 of the Criminal Code of 2012;

14 (F) substance abuse;

15 (G) fraud;

16 (H) trafficking in persons under Section 10-9 of  
17 the Criminal Code of 2012;

18 (I) sexual abuse;

19 (J) physical injury;

20 (K) harassment, including hate-based harassment,  
21 sexual harassment, and stalking under Section 12-7.3  
22 of the Criminal Code of 2012;

23 (L) exposure to harmful material under Section  
24 11-21 of the Criminal Code of 2012;

25 (M) communicating with a terrorist organization as  
26 defined under Section 219 of the federal Immigration



1 and Nationality Act, 8 U.S.C. 1189;

2 (N) academic dishonesty, including cheating,  
3 plagiarism, or other forms of academic dishonesty that  
4 are intended to gain an unfair academic advantage; or

5 (O) sharing personal information limited to:

6 (i) home address;

7 (ii) telephone number;

8 (iii) social security number;

9 (iv) username;

10 (v) password; and

11 (vi) personal banking information.

12 (4) to a person reasonably able to prevent or lessen  
13 an imminent threat to the health or safety of an  
14 individual, if there is a reasonably foreseeable serious  
15 and imminent threat to the health or safety of an  
16 individual;

17 (5) to a public health authority or other appropriate  
18 governmental authority authorized by law to receive  
19 reports of child abuse or neglect.

20 (f) A third-party safety software provider that makes a  
21 disclosure under paragraphs (1), (2), (4), or (5) of subsection  
22 (e) shall promptly inform the child with respect to whose  
23 account with a large social media platform the delegation was  
24 made and, if a parent or legal guardian of the child made the  
25 delegation, the parent or legal guardian that the disclosure  
26 has been or will be made, except if:

1           (1) the third-party safety software provider, in the  
2           exercise of professional judgment, believes informing such  
3           child or parent or legal guardian would place such child  
4           at risk of serious harm; or

5           (2) the third-party safety software provider is  
6           prohibited by law, including a valid order by a court or  
7           administrative body, from informing such child or parent  
8           or legal guardian.

9           Section 20. Requirements of third-party safety software  
10          providers.

11          (a) A third-party safety software provider is qualified to  
12          access an application programming interface and any  
13          information or user data as described in Section 15 if the  
14          third-party safety software provider:

15               (1) is solely engaged in the business of Internet  
16               safety;

17               (2) use any user data it obtains as described in  
18               Section 15 solely for the purpose of protecting a child  
19               from any harm;

20               (3) only discloses user data it obtains as described  
21               in Section 15 as permitted by Section 15; and

22               (4) will disclose, in an easy-to-understand,  
23               human-readable format, to each child with respect to whose  
24               account with a large social media platform the service of  
25               the third-party safety software provider is operating and

1 if a parent or legal guardian of the child made the  
2 delegation as described in Section 15 with respect to the  
3 account, to the parent or legal guardian, sufficient  
4 information detailing the operation of the service and  
5 what information the third-party safety software provider  
6 is collecting to enable such child and such parent or  
7 legal guardian, if applicable, to make informed decisions  
8 regarding the use of the service.

9 Section 25. Liability of third-party safety software  
10 providers. In any civil action, other than an action brought  
11 by the Attorney General, a large social media platform  
12 provider shall not be held liable for damages arising out of  
13 the transfer of user data to a third-party safety software  
14 provider in accordance with this Act, if the large social  
15 media platform provider has in good faith complied with the  
16 requirements of this Act.

17 Section 30. Enforcement by Attorney General. A violation  
18 of any of the provisions of this Act is an unlawful practice  
19 under the Consumer Fraud and Deceptive Business Practices Act.  
20 All remedies, penalties, and authority granted to the Attorney  
21 General by that Act shall be available to him or her for the  
22 enforcement of this Act.

23 Section 90. The Consumer Fraud and Deceptive Business

1 Practices Act is amended by adding Section 2EEEE as follows:

2 (815 ILCS 505/2EEEE new)

3 Sec. 2EEEE. Violations of the Parental Digital Choice Act.

4 A person who violates the Parental Digital Choice Act commits

5 an unlawful practice within the meaning of this Act.

6 Section 99. Effective date. This Act takes effect June 1,

7 2025.