GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2025

H **D**

HOUSE BILL DRH40244-LR-32B

Short Title: Personal Data Privacy/Social Media Safety. (Public)

Sponsors: Representative T. Brown.

Referred to:

A BILL TO BE ENTITLED

AN ACT TO PROTECT NORTH CAROLINIANS BY ENACTING THE PERSONAL DATA PRIVACY ACT AND SOCIAL MEDIA SAFETY ACT.

The General Assembly of North Carolina enacts:

PART I. ENACT PERSONAL DATA PRIVACY ACT

SECTION 1.1. This act shall be known and may be cited as the "North Carolina Personal Data Privacy Act."

SECTION 1.2. Effective January 1, 2026, the General Statutes are amended by adding a new Chapter to read:

"**Chapter 75F.**

"**Data Privacy Act.**

"**§ 75F-101. Short title.**

This Chapter shall be known and may be cited as the "North Carolina Data Privacy Act."

"**§ 75F-102. Definitions.**

The following definitions apply in this Chapter:

(1) Affiliate. – A legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity. For the purposes of this subdivision, "control" or "controlled" means any of the following:

a. Ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of a legal entity.

b. Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

c. The power to exercise controlling influence over the management of a legal entity.

(2) Authenticate. – To use reasonable means to determine that a request to exercise any of the rights afforded under G.S. 75F-104(a)(1) to (4), inclusive, is being made by, or on behalf of, the consumer who is entitled to exercise the consumer rights with respect to the personal data at issue.

(3) Biometric data. – Personal information and data generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that can be used to identify or authenticate a specific individual. "Biometric data" does not include any of the following:

a. A digital or physical photograph.

b. An audio or video recording.

c. Any data generated from a digital or physical photograph, or an audio or video recording, unless the data is generated to identify a specific individual.

(4) Business associate. – As defined in HIPAA.

(5) Child. – As defined in COPPA.

(6) Child abuse. – With respect to an individual under 18 years of age, as defined in Chapter 14 of the General Statutes or any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

(7) Consent. – A clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include any of the following:

a. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

b. Hovering over, muting, pausing, or closing a given piece of content.

c. Agreement obtained through the use of dark patterns.

(8) Consumer. – An individual who is a resident of this State. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit organization, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization, or government agency.

(9) Controller. – A person that, alone or jointly with others, determines the purpose and means of processing personal data.

(10) COPPA. – The Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, et seq., as amended, and the regulations, rules, guidance, and exemptions adopted pursuant to the act, and such regulations, rules, guidance, and exemptions as may be amended.

(11) Covered entity. – As defined in HIPAA.

(12) Dark pattern. – Any of the following:

a. A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

b. Any other practice the Federal Trade Commission refers to as a dark pattern.

(13) Decisions that produce legal or similarly significant effects concerning the consumer. – Decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.

(14) De-identified data. – Data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to the individual, if the controller that possesses the data does all of the following:

a. Takes reasonable measures to ensure that the data cannot be associated with an individual.

b. Publicly commits to process the data only in a de-identified fashion and not attempt to re-identify the data.

c. Contractually obligates any recipients of the data to comply with all of the provisions of this Chapter applicable to the controller with respect to the data.

(15) Domestic violence. - As defined in Chapter 14 of the General Statutes or any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

(16) Genetic data. – Any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. For purposes of this subdivision, "genetic material" includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(17) HIPAA. – The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d, et seq., as amended.

(18) Human trafficking. – The offense defined in Chapter 14 of the General Statutes or any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

(19) Identified or identifiable individual. – An individual who can be readily identified, directly or indirectly.

(20) Nonprofit organization. – Any organization that is exempt from taxation under section 501(c)(3), 501(c)(4), 501(c)(6), or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended.

(21) Personal data. – Any information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or publicly available information.

(22) Precise geolocation data. – Information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(23) Process or processing. – Any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) Processor. – A person that processes personal data on behalf of a controller.

(25) Profiling. – Any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements.

(26) Protected health information. – As defined in HIPAA.

(27) Pseudonymous data. – Personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(28) Publicly available information. – Information that is lawfully made readily available to the general public through federal, State, or local government records or widely distributed media and a controller has a reasonable basis to believe a consumer has lawfully made readily available to the general public.

(29) Sale of personal data. – The exchange or transfer of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include any of the following:

a. The disclosure of personal data to a processor that processes the personal data on behalf of the controller where limited to the purpose of the processing.

b. The disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer.

c. The disclosure or transfer of personal data to an affiliate of the controller.

d. The disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

e. The disclosure of personal data that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience.

f. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other similar transaction in which the third party assumes control of all or part of the controller's assets, or a proposed merger, acquisition, bankruptcy, or other similar transaction in which the third party assumes control of all or part of the controller's assets.

(30) Sensitive data. – Personal data that includes any of the following:

a. Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis (including pregnancy), sex life, sexual orientation, status as transgender or nonbinary, national origin, citizenship status, or immigration status.

b. Genetic or biometric data.

c. Personal data of a known child.

d. Precise geolocation data.

(31) Sexual assault. – Any of the offenses defined in Chapter 14 of the General Statutes or any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

(32) Stalking. – The offense defined in Chapter 14 of the General Statutes or any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

(33) Targeted advertising. – Displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet websites or

online applications to predict the consumer's preferences or interests. "Targeted advertising" does not include any of the following:

a. Advertisements based on activities within a controller's own internet websites or online applications.

b. Advertisements based on the context of a consumer's current search query, visit to an internet website, or online application.

c. Advertisements directed to a consumer in direct response to the consumer's request for information or feedback.

d. Processing personal data solely to measure or report advertising frequency, performance, or reach.

(34) Third party. – With respect to personal data controlled by a controller, any person other than the relevant consumer, the controller of the personal data, or a processor or an affiliate of the processor or the controller.

(35) Trade secret. – As defined in Chapter 66, 95, or 113 of the General Statutes.

(36) Violent felony. – As defined in section 4201 of Title 11 and includes any equivalent provision in the laws of any other state; the United States; any territory, district, or subdivision of the United States; or any foreign jurisdiction.

"**§ 75F-103. Applicability of Chapter.**

(a) This Chapter applies to persons that conduct business in the State or persons that produce products or services that are targeted to residents of the State and that during the preceding calendar year did any of the following:

(1) Controlled or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.

(2) Controlled or processed the personal data of not less than 10,000 consumers and derived more than twenty percent (20%) of their gross revenue from the sale of personal data.

(b) This Chapter does not apply to any of the following entities:

(1) Any regulatory, administrative, advisory, executive, appointive, legislative, or judicial body of the State or a political subdivision of the State, including any board, bureau, commission, or agency of the State or a political subdivision of the State, but excluding any institution of higher education.

(2) Any financial institution or affiliate of a financial institution, all as defined in 15 U.S.C. § 6809, to the extent that the financial institution or affiliate is subject to Title V of the Gramm Leach Bliley Act (15 U.S.C. § 6801, et seq., as amended) and the rules and implementing regulations promulgated thereunder.

(c) This Chapter does not apply to the following information and data:

(1) Protected health information under HIPAA.

(2) Patient-identifying information for purposes of 42 U.S.C. § 290dd-2.

(3) Identifiable private information, as defined in 45 C.F.R. § 46.102, to the extent that it is used for purposes of the federal policy for the protection of human subjects pursuant to 45 C.F.R. § 46.

(4) Identifiable private information to the extent it is collected and used as part of human subjects research pursuant to the ICH E6 Good Clinical Practice Guideline issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 C.F.R. §§ 50 and 56.

(5) Patient safety work product, as defined in 42 C.F.R. § 3.20, that is created and used for purposes of patient safety improvement pursuant to 42 C.F.R. § 3, established pursuant to 42 U.S.C. §§ 299b–21 to 299b–26.

(6) Information to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a Covered Entity or when provided by or to a Business Associate pursuant to a Business Associate Agreement with a Covered Entity.

(7) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681, et seq., as amended).

(8) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721, et seq., as amended.

(9) Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, et seq., as amended.

(10) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act, 12 U.S.C. § 2001, et seq., as amended.

(11) Data processed or maintained in any of the following ways:

a. In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

b. As the emergency contact information of an individual, used for emergency contact purposes.

c. Necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under sub-subdivision a. of this subdivision and used for the purposes of administering the benefits.

(12) Personal data collected, processed, sold, or disclosed in relation to price, route, or service, as the terms are used in the Airline Deregulation Act, 49 U.S.C. § 40101, et seq., as amended, by an air carrier subject to said act, to the extent any part of this Chapter is preempted by the Airline Deregulation Act, 49 U.S.C. § 41713, as amended.

(13) Personal data of a victim of or witness to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that is collected, processed, or maintained by a nonprofit organization that provides services to victims of or witnesses to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.

(d) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent set forth in this Chapter with respect to a consumer who is a child.

"**§ 75F-104. Consumer personal data rights.**

(a) A consumer has the right to do all of the following:

(1) Confirm whether a controller is processing the consumer's personal data and access the personal data, unless the confirmation or access would require the controller to reveal a trade secret.

(2) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(3) Have personal data provided by, or obtained about, the consumer deleted.

(4) Obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided the controller shall not be required to reveal any trade secret.

(5) Obtain a list of the specific third parties to which the controller has disclosed the consumer's personal data. If the controller does not maintain this information in a format specific to the consumer, a list of specific third parties to whom the controller has disclosed any consumers' personal data may be provided instead.

(6) Opt out of the processing of the personal data for purposes of any of the following:

a. Targeted advertising.

b. The sale of personal data, except as provided in G.S. 75F-106(b).

c. Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with G.S. 75F-105 to exercise the rights of the consumer to opt out of the processing of the consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise the consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise the rights on the consumer's behalf.

(c) Except as otherwise provided in this Chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay but not later than 45 days after receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay but not later than 45 days after receipt of the request of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) through (5), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be

required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good-faith, reasonable, and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller believes the request is fraudulent, why the controller believes the request is fraudulent, and that the controller shall not comply with the request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete the data pursuant to subdivision (3) of subsection (a) of this section if the controller retains a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and does not use the retained data for any other purpose.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Department of Justice to submit a complaint.

"**§ 75F-105. Designation of agent to exercise rights of consumer, including through universal opt-out mechanisms.**

(a) A consumer may designate an authorized agent to act on the consumer's behalf to opt out of the processing of the consumer's personal data for one or more of the purposes specified in G.S. 75F-104(a)(5). The consumer may designate the authorized agent by way of, among other things, a platform, technology, or mechanism, including an internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of the processing. For the purposes of the designation, the platform, technology, or mechanism may function as the agent for purposes of conveying the consumer's decision to opt out.

(b) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. The Department of Justice may publish or reference on its website a list of agents who presumptively shall have the authority unless the controller has established a reasonable basis to conclude that the agent lacks such authority.

"**§ 75F-106. Duties of controllers.**

(a) A controller shall do all of the following:

(1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.

(2) Except as otherwise permitted by this Chapter, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the

disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(4) Not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

(5) Not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination.

(6) Provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of the consent, cease to process the data as soon as practicable but not later than 15 days after the receipt of the request.

(7) Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge or willfully disregards that the consumer is at least 13 years of age but younger than 18 years of age.

(8) Not discriminate against a consumer for exercising any of the consumer rights contained in this Chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

(1) The categories of personal data processed by the controller.

(2) The purpose for processing personal data.

(3) How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request.

(4) The categories of personal data that the controller shares with third parties, if any.

(5) The categories of third parties with which the controller shares personal data, if any.

(6) An active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing.

(e) A controller shall establish and shall describe in the privacy notice required by subsection (c) of this section one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this Chapter. The means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of the requests, and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights but may require a consumer to use an existing account. Any such means shall include all of the following:

(1) Providing a clear and conspicuous link on the controller's internet website to an internet webpage that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or the sale of the consumer's personal data.

(2) Allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the personal data, through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of any such processing or sale. The platform, technology, or mechanism shall do all of the following:

a. Not unfairly disadvantage another controller.

b. Not make use of a default setting but, rather, require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of any processing of the consumer's personal data pursuant to this Chapter.

c. Be consumer-friendly and easy to use by the average consumer.

d. Be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or State law or regulation.

e. Enable the controller to reasonably determine whether the consumer is a resident of the State and whether the consumer has made a legitimate request to opt out of any sale of the consumer's personal data or targeted advertising.

If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the personal data, through an opt-out preference signal sent in accordance with the provisions of subdivision (1) of this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide to the consumer the choice to confirm the controller-specific privacy setting or participation in the program.

If a controller responds to consumer opt-out requests received pursuant to subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subdivision (2) of this subsection for the retention, use, sale, or sharing of the consumer's personal data.

"**§ 75F-107. Duties of processors.**

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this Chapter. The assistance must include all of the following:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests.

(2) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the

notification of a breach of security of the system of the processor, in order to meet the controller's obligations.

(3) Providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract must also require that the processor do all of the following:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this Chapter.

(4) After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(5) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or 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 Chapter, using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller upon request.

(c) Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship, as described in this Chapter.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under this Chapter.

"**§ 75F-108. Data protection assessments.**

(a) A controller that controls or processes the data of not less than 100,000 consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction, shall conduct and document, on a regular basis, a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes any of the following:

(1) The processing of personal data for the purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for the purposes of profiling, where the profiling presents a reasonably foreseeable risk of any of the following:

a. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

b. Financial, physical, or reputational injury to consumers.

c. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person.

d. Other substantial injury to consumers.

(4) The processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this Chapter. Data protection assessments must be treated as confidential and are not public records within the meaning of Chapter 132 of the General Statutes. Notwithstanding the foregoing, a controller's data protection assessment may be used in an action to enforce this Chapter. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes and conspicuously identifies information subject to attorney-client privilege or work product protection, the disclosure by itself does not constitute a waiver of the privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated on or after July 1, 2026, and are not retroactive.

"**§ 75F-109. De-identified data.**

(a) Nothing in this Chapter shall be construed to require a controller or processor to re-identify de-identified data or pseudonymous data, or to maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(b) Nothing in this Chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if all of the following apply:

(1) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

(2) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer.

(3) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(c) The rights afforded under G.S. 75F-104(a)(1) to (4), inclusive, do not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(d) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments. The determination of the reasonableness of the oversight and the appropriateness of contractual enforcement must take into account whether the disclosed data includes data that would be sensitive data if it were re-identified.

"**§ 75F-110. Exclusions.**

(a) Nothing in this Chapter shall be construed to restrict a controller's or processor's ability to do any of the following:

(1) Comply with federal, State, or local laws, rules, or regulations.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, State, local, or other governmental authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, State, or local laws, rules, or regulations.

(4) Investigate, establish, exercise, prepare for, or defend legal claims.

(5) Provide a product or service specifically requested by a consumer.

(6) Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty.

(7) Take steps at the request of a consumer prior to entering into a contract.

(8) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and where the processing cannot be manifestly based on another legal basis.

(9) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such activity.

(10) Engage in public or peer-reviewed scientific research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, the expected benefits of the research outweigh the privacy risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

(11) Assist another controller, processor, or third party with any of the activities under this subsection.

(b) The obligations imposed on controllers or processors under this Chapter, other than those imposed by G.S. 75F-109, do not restrict a controller's or processor's ability to collect data directly from consumers, or use or retain the data, for internal use only, to do any of the following:

(1) Conduct internal research to develop, improve, or repair products, services, or technology.

(2) Effectuate a product recall.

(3) Identify and repair technical errors that impair existing or intended functionality.

(4) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under this Chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this State. Nothing in this Chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this State as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in compliance with this Chapter shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes the personal data violates said sections, provided that (i) at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller had violated or would violate said sections and (ii) the disclosing controller or processor was, and remained, in compliance with its obligations as the discloser of the data hereunder. A third-party controller or processor receiving personal data from a controller or processor in compliance with this Chapter is likewise not in violation of said sections for the independent misconduct of the controller or processor from which the third-party controller or processor receives the personal data.

(e) Nothing in this Chapter may be construed to do any of the following:

(1) Impose any obligation on a controller or processor that adversely affects the rights of any person to freedom of speech or freedom of the press guaranteed by the First Amendment to the United States Constitution or Article I, Section 14 of the North Carolina Constitution.

(2) Apply to any person's processing of personal data in the course of the person's purely personal or household activities.

(f) Personal data processed pursuant to this section may be processed to the extent that the processing is reasonably necessary and proportionate to the purposes listed in this section and is adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention. The data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements of subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to the processing.

"**§ 75F-111. Enforcement.**

(a) The Department of Justice shall investigate and enforce alleged violations of this Chapter.

(b) The Department of Justice may, prior to initiating any action for a violation of any provision of this Chapter, issue a notice of violation to the controller or processor if the

Department of Justice determines that a cure is possible. If the Department of Justice issues a notice of violation, the controller shall have at least 60 days to cure the violation after receipt of the notice. If the controller fails to cure the violation within the time period, the Department of Justice may bring an enforcement proceeding pursuant to subsection (a) of this section. In determining whether to grant a controller or processor an opportunity to cure an alleged violation, the Department of Justice may consider all of the following:

(1) The number of violations.

(2) The size and complexity of the controller or processor.

(3) The nature and extent of the controller's or processor's processing activities.

(4) The substantial likelihood of injury to the public.

(5) The safety of persons or property.

(6) Whether the alleged violation was likely caused by human or technical error.

(7) The extent to which the controller or processor has violated this or similar laws in the past.

(c) Nothing in this Chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(d) A violation of this Chapter shall be deemed an unfair practice under G.S. 75-1.1."

SECTION 1.3. Beginning at least six months prior to the effective date of this act, the Department of Justice shall engage in public outreach to educate consumers and the business community about this act.

PART II. ENACT SOCIAL MEDIA SAFETY ACT

SECTION 2.1. Effective January 1, 2026, the General Statutes are amended by adding a new Chapter to read:

"**Chapter 75G.**

"**Social Media Verification.**

"**§ 75G-101. Definitions.**

The following definitions apply in this Chapter:

(1) Account holder. – An individual who creates an account or a profile to use a social media platform.

(2) Commercial entity. – A corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized entity. The term includes a third-party vendor.

(3) Digitized identification card. – A data file available on a mobile device that has connectivity to the internet through a State-approved application that allows the mobile device to download the data file from the Division of Motor Vehicles that contains all of the data elements visible on the face and back of a drivers license or identification card and displays the current status of the drivers license or identification card, including valid, expired, cancelled, suspended, revoked, active, or inactive.

(4) Minor. – An individual under 18 years of age.

(5) North Carolina user. – An individual who is a resident of the State of North Carolina and who accesses or attempts to access a social media platform while present in this State by accessing the social media platform while using a North Carolina Internet Protocol address or otherwise known or believed to be in this State while using the social media platform.

(6) Reasonable age verification. – To confirm that a person seeking to access a social media platform is at least 18 years old.

(7) Social media company. – An online forum that a company makes available for an account holder to:

a. Create a public profile, establish an account, or register as a user for the primary purpose of interacting socially with other profiles and accounts;

b. Upload or create posts or content;

c. View posts or content of other account holders; and

d. Interact with other account holders or users, including, without limitation, establishing mutual connections through request and acceptance.

(7a) Social media company. – Does not include any of the following:

a. A company that exclusively offers subscription content in which users follow or subscribe unilaterally and whose platforms' primary purpose is not social interaction.

b. A social media company that allows a user to generate short video clips of dancing, voice overs, or other acts of entertainment in which the primary purpose is not educational or informative does not meet the exclusion under sub-subdivision a. of this subdivision.

c. A media company that exclusively offers interactive gaming, virtual gaming, or an online service; that allows the creation and uploading of content for the purpose of interactive gaming, entertainment, or associated entertainment; and the communication related to that content.

d. A company that offers cloud storage services, enterprise cybersecurity services, educational devices, or enterprise collaboration tools for kindergarten through grade 12 (K-12) schools and derives less than twenty-five percent (25%) of the company's revenue from operating a social media platform, including games and advertising.

e. A company that provides career development opportunities, including professional networking, job skills, learning certifications, and job posting and application services.

(8) Social media platform. – A public or semipublic internet-based service or application that has users in North Carolina and on which a substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application; however, a service or application that provides email or direct messaging shall not be considered to be a social media platform on the basis of that function alone.

(8a) Social media platform. – Does not include an online service, a website, or an application if the predominant or exclusive function is:

a. Electronic mail.

b. Direct messaging consisting of messages, photos, or videos that are sent between devices by electronic means if messages are:

1. Shared between the sender and the recipient or recipients;

2. Only visible to the sender and the recipient or recipients; and

3. Are not posted publicly.

c. A streaming service that (i) provides only licensed media in a continuous flow from the service, website, or application to the end user and (ii) does not obtain a license to the media from a user or account holder by agreement of the streaming service's terms of service.

d. News, sports, entertainment, or other content that is preselected by the provider and not user generated, including, without limitation, if any chat, comment, or interactive functionality that is provided is incidental to, directly related to, or dependent upon provision of the content.

e. Online shopping or e-commerce, if the interaction with other users or account holders is generally limited to:

1. The ability to post and comment on reviews;

2. The ability to display lists or collections of goods for sale or wish lists; and

3. Other functions that are focused on online shopping or e-commerce rather than interaction between users or account holders.

f. Business-to-business software that is not accessible to the general public.

g. Cloud storage.

h. Shared document collaboration.

i. Providing access to or interacting with data visualization platforms, libraries, or hubs.

j. To permit comments on a digital news website, if the news content is posted only by the provider of the digital news website.

k. For the purpose of providing or obtaining technical support for the social media company's social media platform, products, or services.

l. Academic or scholarly research.

m. Other research if (i) the majority of the content is posted or created by the provider of the online service, website, or application and (ii) the ability to chat, comment, or interact with other users is directly related to the provider's content; then, the following criteria must also apply:

1. The service is a classified advertising service that only permits the sale of goods and prohibits the solicitation of personal services or that is used by and under the direction of an educational entity, including, without limitation, a learning management system, student engagement program, and subject-specific or skill-specific program.

(8b) Social media platform. – Does not include a social media platform that is controlled by a business entity that has generated less than one hundred million dollars ($100,000,000) in annual gross revenue.

(9) User. – A person who has access to view all or some of the posts and content on a social media platform but is not an account holder.

"**§ 75G-102. Social media platforms; reasonable age verification methods; parental consent required.**

(a) A social media company shall not permit a North Carolina user who is a minor to be an account holder on the social media company's social media platform unless the minor has the express consent of a parent or legal guardian. A social media company shall verify the age of an account holder. If an account holder is a minor, the social media company shall confirm that a minor has consent under this subsection to become a new account holder at the time a North Carolina user opens the account.

(b) A social media company shall use a third-party vendor to perform reasonable age verification before allowing access to the social media company's social media platform.

(c) Reasonable age verification methods under this section include providing one of the following:

(1) A digitized identification card, including a digital copy of a drivers license issued by the Division of Motor Vehicles.

(2) Government-issued identification.

(3) Any commercially reasonable age verification method.

"**§ 75G-103. Liability for social media companies.**

(a) A social media company that knowingly violates this Chapter is liable if the social media company fails to perform a reasonable age verification.

(b) If a social media company performs a reasonable age verification, the social media company shall not retain any identifying information of the individual after access to the social media platform has been granted.

(c1) Violation of G.S. 75G-102 is a Class 1 misdemeanor. As authorized under this section, the district attorney for the county where the North Carolina user resides may initiate a criminal proceeding against a social media company that allegedly violates G.S. 75G-102.

(c2) As authorized under G.S. 75G-104, the Attorney General may initiate a civil enforcement action against a social media company that allegedly commits a violation of G.S. 75G-102.

(c3) A social media company that violates this Chapter is liable to an individual for:

(1) A penalty of two thousand five hundred dollars ($2,500) per violation, court costs, and reasonable attorneys' fees as ordered by the court; or

(2) Damages resulting from a minor accessing a social media platform without his or her parent's or custodian's consent, including court costs and reasonable attorneys' fees as ordered by the court.

(d) This section does not:

(1) Apply to a news or public interest broadcast, website video, report, or event;

(2) Affect the rights of a news-gathering organization; or

(3) Apply to cloud service providers.

(e) An internet service provider, or any of its affiliates or subsidiaries, or search engines shall not violate this Chapter solely by providing access, connection to or from a website, or other information or content on the internet, or a facility, system, or network that is not under that internet service provider's control, including transmission, downloading, intermediate storage, access software, or other service that provides access or connectivity, to the extent the internet service provider is not responsible for the creation of the content or the communication on a social media platform.

"**§ 75G-104. Liability for commercial entity or third-party vendor.**

(a) A commercial entity or third-party vendor shall not retain any identifying information of an individual after access to the social media platform has been granted.

(b) A commercial entity that is found to have knowingly retained identifying information of an individual after access to the material is granted is liable to the individual for damages resulting from the retention of the identifying information, including court costs and reasonable attorneys' fees as ordered by the court."

PART III. SEVERABILITY

SECTION 3.1. If any provision of this act or the application thereof to any person or circumstance is held invalid, the invalidity does not affect any other provision or application of the act which can be given effect without the invalid provision or application and, to that end, the provisions of this act are declared to be severable.

PART IV. EFFECTIVE DATE

SECTION 4.1. Except as otherwise provided, this act is effective when it becomes law.