A bill to be entitled

An act relating to personal privacy; providing a short title; providing that digital data is protected from unreasonable search and seizure; creating s. 933.41, F.S.; prohibiting the use of certain radar technology by law enforcement agencies unless specified criteria are met; providing that evidence unlawfully collected is not admissible in criminal, civil, or administrative actions; creating s. 934.60, F.S.; prohibiting certain Internet protocol addresses from being disclosed unless certain conditions are met; providing a private right of action; providing limitations; providing applicability; creating s. 934.70, F.S.; providing definitions; providing restrictions on government searches of portable electronic devices; requiring a warrant for a search of such devices; providing exceptions; providing that evidence unlawfully collected is not admissible in criminal, civil, or administrative actions; prohibiting government entities from entering into nondisclosure agreements with vendors of specified equipment; declaring existing nondisclosure agreements void; providing that such agreements are subject to public records law; authorizing a private right of action for violations; requiring common carriers and electronic communication services to prepare certain

reports to be delivered to the Florida Department of Law Enforcement; providing requirements for such reports; requiring the department to prepare reports to be delivered to certain legislative and executive entities; providing requirements for such reports; requiring the department, in consultation with the Office of the State Courts Administrator and state attorneys, to develop certain recommendations; requiring that the report be delivered to certain legislative and executive entities; amending s. 1002.222, F.S.; prohibiting school districts from entering into certain agreements without specified provisions; defining the term "student data"; specifying that contracts or agreements without certain required provisions are void; requiring that data collected under such contracts be returned or destroyed; specifying activities which are exempt from such requirements for contracts and agreements; prohibiting the Department of Highway Safety and Motor Vehicles from incorporating a radio frequency identification device or other electronic tracking device upon or within a driver license or identification card; prohibiting the Department of Highway Safety and Motor Vehicles from obtaining fingerprints or biometric DNA material of citizens for specified purposes; providing severability; providing

an appropriation and authorizing a position; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. This act may be cited as the "Florida Privacy Protection Act."

Section 2. The Legislature declares that digital data is property that is constitutionally protected from unreasonable search and seizure.

Section 3. Section 933.41, Florida Statutes, is created to read:

933.41 Prohibition against search using wall-penetrating radar device.—

(1) A law enforcement officer or law enforcement agency in the state may not use a wall-penetrating radar device, except pursuant to a warrant signed by a judge and based upon probable cause or pursuant to a lawful exception to the search warrant requirement, including an exception established by the United States Supreme Court or the Florida Supreme Court.

(2) Evidence obtained in violation of this section is not admissible in a criminal, civil, administrative, or other proceeding except as proof of a violation of this section.

Section 4. Section 934.60, Florida Statutes, is created to read:

934.60 Internet protocol address privacy.—

(1) A provider of an electronic communication service provided to the public shall not provide third parties with information that allows an Internet protocol address to be linked to a specific subscriber or customer without the express permission of the subscriber or customer. The request for permission must be clear and conspicuous and must require the subscriber or customer to take an affirmative action to acknowledge such permission. This subsection does not prohibit the provider of an electronic communication service from complying with a lawful subpoena, court order, or warrant.

(2) A person may bring a civil action in a court of competent jurisdiction to seek injunctive relief to enforce compliance with this section or to recover damages and penalties from a provider that violates this section. A person is entitled to recover a $10,000 penalty for each violation of this section.

(3) An action under this section must commence within 2 years after the date that the information is disclosed.

(4) Consenting to a provider's terms and conditions or a provider's privacy statement describing such provider's data sharing practices constitutes express permission for purposes of subsection (1).

Section 5. Section 934.70, Florida Statutes, is created to read:

934.70 Portable electronic device privacy.—

(1) DEFINITIONS.-As used in this section, the term:

(a) "Department" means the Department of Law Enforcement.

(b) "Government entity" means a federal, state, or local government agency, including, but not limited to, a law enforcement agency or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for, or on behalf of, a federal, state, or local government agency. The term does not include a federal agency to the extent that federal law preempts this section.

(c) "Information" includes any information concerning the substance or meaning or purported substance or meaning of a communication, including, but not limited to, the name and address of the sender and receiver and the time, date, location, and duration of the communication.

(d) "Portable electronic device" means any portable device that is capable of creating, receiving, accessing, or storing electronic data or communications, including, but not limited to, cellular telephones.

(2) Information contained in a portable electronic device is not subject to search by a government entity, including a search incident to a lawful arrest, except pursuant to a warrant signed by a judge and based upon probable cause or pursuant to a lawful exception to the search warrant requirement, including an exception established by the United States Supreme Court or the Florida Supreme Court.

(3) Evidence obtained in violation of subsection (2) is not admissible in a criminal, civil, administrative, or other

proceeding except as proof of a violation of this section.

(4) A government entity may not enter into a nondisclosure agreement with a vendor who sells equipment to monitor electronic devices. Any existing nondisclosure agreements are declared void for public policy. Records otherwise protected by such agreements are declared subject to the public records law, and a government entity may not refuse to disclose such agreements or related records upon request by citing such an agreement.

(5) A person injured by a government entity as a result of a violation of subsection (4) may bring a civil action against the government entity.

(6)(a) By January 15 of each year, a communication common carrier or electronic communication service doing business in the state shall report to the department the following information for the preceding calendar year, disaggregated by each law enforcement agency making the applicable requests:

1. The number of requests made for pen register or trap and trace information.

2. The number of requests made for electronic serial number reader information.

3. The number of requests made for location information.

4. The number of individuals whose location information was disclosed.

5. The amount that each law enforcement agency was billed by the communication common carrier or electronic communication

service for each request made under subsections (1)-(3).

(b) Reports submitted to the department under this section are expressly declared subject to disclosure under the public records laws and are not confidential or exempt.

(c) By March 1 of each year, the department shall submit a report to the Governor, the President of the Senate, the Speaker of the House of Representatives, and the chairs of the standing committees of the Senate and the House of Representatives with primary jurisdiction over criminal justice, on the information provided pursuant to paragraph (a).

(d) The Office of the State Courts Administrator and state attorneys must cooperate with the department to develop a methodology for gathering data regarding requests for a warrant pursuant to subsection (2) and related information. By October 1, 2015, the department shall submit a report containing the recommendations of the Office of the State Courts Administrator and state attorneys to the Governor, the President of the Senate, the Speaker of the House of Representatives, and the chairs of the standing committees of the Senate and the House of Representatives with primary jurisdiction over criminal justice. The report must include a plan for implementation and justification of all associated costs.

Section 6. Paragraph (c) is added to subsection (1) of section 1002.222, Florida Statutes, and subsections (3) and (4) are added to that section, to read:

1002.222 Limitations on collection of information and

disclosure of confidential and exempt student records.—

(1) An agency or institution as defined in s. 1002.22(1) may not:

(c) Enter into any agreement that does not expressly:

1. Prohibit the sale or distribution of student data and access to student data except as instructed by the agency or institution to comply with local, state, or federal reporting requirements.

2. Prohibit the mining of student data for commercial purposes, including the targeting of advertising based upon such data.

3. Require that all student data remain the property of the agency or institution and that such data be returned upon request or be destroyed using a method designed to ensure confidentiality and permanently deleted from any computer hardware, media, or other equipment.

For purposes of this paragraph, "student data" means information that is collected and maintained at the individual student level.

(3) Any contract or agreement entered into after July 1, 2015, that violates this section is void, and any data obtained in violation of this section must be returned to the agency or institution or destroyed using a method designed to ensure confidentiality and permanently deleted from any computer hardware, media, or other equipment.

(4) This section does not:

(a) Prohibit a person from using de-identified student data to improve educational products within a website, service, or application or to demonstrate the effectiveness of the products or services, including marketing.

(b) Prohibit a person from sharing aggregated, de-identified student data for the development or improvement of educational websites, services, or applications.

(c) Prohibit a person from marketing educational products directly to parents if the marketing is not based upon student data obtained through the provision of services under this section.

(d) Limit the authority of a law enforcement agency to obtain information from a person as authorized by law or pursuant to an order of a court of competent jurisdiction.

(e) Limit the ability of a person to use student data for adaptive learning or customized student learning purposes.

(f) Limit Internet service providers from providing Internet connectivity to schools, students, or parents.

(g) Apply to a website, online service, online application, or mobile application intended for use by the general public, even if login credentials created for the contractor's website, service, or application are used to access the public website, service, or application.

(h) Impede the ability of a student to download, export, or otherwise save or maintain his or her own data or documents.

(i) Impose a duty upon:

1. A provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this section.

2. A provider of an interactive computer service, as defined in 47 U.S.C. s. 230, to review or enforce compliance with this section by third-party content providers.

Section 7. The Department of Highway Safety and Motor Vehicles shall not incorporate any radio frequency identification device, or "RFID," or any similar electronic tracking device upon or within any driver license or identification card issued by the department. The department may not obtain fingerprints or biometric DNA material from a United States citizen for purposes of any issuance, renewal, reinstatement, or modification of a driver license or identification card issued by the department.

Section 8. If any provision of this act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this act which can be given effect without the invalid provision or application, and to this end the provisions of this act are severable.

Section 9. For the 2015-2016 fiscal year, the sums of $75,133 in recurring funds and $308,765 in nonrecurring funds are appropriated from the General Revenue Fund to the Department

of Law Enforcement, and one full-time equivalent position with associated salary rate is authorized, to analyze data collected and to comply with the reporting requirements of this act.

Section 10. This act shall take effect July 1, 2015.