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, electronic communication services, courts, and

prosecutors 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; creating s. 1002.227, F.S.; requiring school district contracts involving student data contain a provision barring contractors from selling, distributing, or accessing such data; providing exceptions; declaring student data to be the property of the school district; providing that student data shall not be provided to the Federal Government or commercial interests without written permission of a parent or guardian or the student; prohibiting companies from mining student data for commercial purposes; requiring a school or third party to delete or destroy certain student data under specified circumstances; providing penalties; restricting the use of public funds in defense of or for the reimbursement of a person who knowingly or willfully violates this act; 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 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) By the 30th day after expiration of a warrant or order issued under subsection (2) or an order extending the period of a warrant or order issued under subsection (2), or by the 30th day after the court denies an application for a warrant or order under subsection (2), the court shall submit to the department the following information, as applicable:

1. The receipt of an application for a warrant or order.

2. The type of warrant or order for which application was made.

3. Whether any application for an order of extension was granted, granted as modified by the court, or denied.

4. The period of monitoring authorized by the warrant or order and the number and duration of any extensions of the warrant.

5. The offense under investigation, as specified in the application for the warrant or order or an extension of the warrant or order.

6. The name of the law enforcement agency or prosecutor that submitted an application for the warrant or order or an extension of the warrant or order.

(c) By January 15 of each year, each prosecutor that submits an application for a warrant or order or an extension of a warrant or order under this section shall submit to the department the following information for the preceding calendar

year:

1. The information required to be submitted by a court under paragraph (b) with respect to each application submitted by the prosecutor for the warrant or order or an extension of the warrant or order.

2. A general description of information collected under each warrant or order that was issued by the court, including the approximate number of individuals for whom location information was intercepted and the approximate duration of the monitoring of the location information of the individuals.

3. The number of arrests made as a result of information obtained under a warrant or order issued pursuant to subsection (2).

4. The number of criminal trials commenced as a result of information obtained under a warrant or order issued pursuant to subsection (2).

5. The number of convictions obtained as a result of information obtained under a warrant or order issued pursuant to subsection (2).

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

(e) 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. The report shall contain the following information for the preceding calendar year:

1. An assessment of the extent of tracking or monitoring by law enforcement agencies of pen registers, trap and trace devices, electronic serial number readers, and location information.

2. A comparison of the ratio of the number of applications for warrants or orders made pursuant to subsection (2) to the number of arrests and convictions resulting from information obtained under a warrant or order issued pursuant to subsection (2).

3. Identification of the types of offenses investigated under a warrant or order issued pursuant to subsection (2).

4. With respect to both state and local jurisdictions, an estimate of the total cost of conducting investigations under a warrant or order issued pursuant to subsection (2).

Section 6. Section 1002.227, Florida Statutes, is created to read:

1002.227 Contract requirements relating to student data.—

(1) All contracts between school districts and companies that process or receive student data shall explicitly prohibit the companies from selling, distributing, or accessing any student data, except as instructed by the school district in order to comply with local, state, or federal reporting requirements.

(2) Any data collected from students through online learning is the property of the school district, not the company.

(3)(a) Data collected on a student who is younger than 18 years of age may not be provided to the Federal Government or to commercial companies without the written consent of the parent or the guardian of the student.

(b) Data collected on a student who is 18 years of age or older may not be provided to the Federal Government or to commercial companies without the written consent of the adult student.

(c) This subsection does not prohibit any party from complying with a lawful subpoena or warrant.

(4) Education technical companies that contract with public schools shall be prohibited from mining student data for commercial purposes.

(5) Except as otherwise required by law, or where such information is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding, upon a student's graduation, withdrawal, or expulsion from an educational institution, all personally identifiable student data related to that student:

(a) Stored in a student information system shall be deleted.

(b) In the possession or under the control of a school employee or third party shall be deleted or destroyed.

(6)(a) A violation of this section shall result in a civil fine of up to $10,000 against the elected school board members under whose jurisdiction the violation occurred.

(b) Except as required by applicable law, public funds may not be used to defend or reimburse the unlawful conduct of any person found to knowingly and willfully violate this section.

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. This act shall take effect July 1, 2015.