HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 571 Personal Privacy
SPONSOR(S): Criminal Justice Subcommittee; Rodrigues
TIED BILLS: None **IDEN./SIM. BILLS:** SB 1530

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	9 Y, 3 N, As CS	Cunningham	Cunningham
2) Government Operations Subcommittee			
3) Appropriations Committee			
4) Judiciary Committee			

SUMMARY ANALYSIS

The evolution of the Internet, the widespread use of electronic devices, and the advancement of data gathering technologies has made it exceptionally easy to gather digital data about people. The bill contains a variety of provisions relating to the privacy of digital information. Specifically, the bill:

- Prohibits providers of electronic communications services to the public from providing 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;
- Declares that digital data is constitutionally protected from unreasonable search and seizure;
- Prohibits law enforcement, with exceptions, from using a wall-penetrating radar device without a warrant, except pursuant to a lawful exception to the search warrant requirement;
- Specifies that information contained in a portable electronic device (PED) is not subject to a search by a government entity, including a search incident to arrest, except pursuant to a valid warrant or pursuant to a lawful exception to the search warrant requirement;
- Prohibits a government entity from entering into a nondisclosure agreement with a vendor who sells equipment to monitor electronic devices;
- Imposes a multitude of reporting requirements on the courts, state attorneys, and the Florida Department of Law Enforcement (FDLE) relating to cases in which a PED search warrant was applied for;
- Prohibits data collected on students from being provided to the federal government or to commercial companies without the written consent of the student (or parent if the student is under 18);
- Requires all contracts between school districts and companies that process or receive student data to explicitly prohibit such 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;
- Requires all personally identifiable student data, with few exceptions, to be deleted or destroyed upon the student's graduation, withdrawal, or expulsion, except as otherwise required by law;
- Authorizes a variety of civil actions for violations of the above-described prohibitions; and
- Prohibits the Department of Highway Safety and Motor Vehicles from:
  - Incorporating a radio frequency identification device upon or within any driver license; and
  - Obtaining fingerprints or biometric DNA material for purposes of issuing, etc., a driver license.

The bill may have a fiscal impact state government and private entities. See fiscal section.

The bill is effective July 1, 2015.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Internet Privacy

The widespread use of the Internet has made it much easier to gather data about users.[1] For example, websites such as Facebook and Twitter accumulate substantial amounts of information, such as the age, friends, and interests of people who sign up for accounts and spend time on their sites.[2] Some of it is collected without users being aware of it.

The advertising industry obtains its data in two main ways. "First-party" data are collected by firms with which the user has a direct relationship.[3] Advertisers and publishers can compile them by requiring users to register online. This enables the companies to recognize consumers across multiple devices and see what they read and buy on their site.[4]

"Third-party" data are gathered by thousands of specialist firms across the web. To gather information about users and help serve appropriate ads, sites often host a multitude of third parties that observe who comes to the site and build up digital dossiers about them.[5] BlueKai, for example, compiles around one billion profiles of potential customers around the world.[6]

To identify users as they move from site to site, third parties use technologies such as cookies, web beacons, e-tags and a variety of other tools.[7] Cookies, widely used on desktop computers, are small pieces of code that are dropped on a user's browser. According to TRUSTe, the 100 most widely used websites are monitored by more than 1,300 firms.[8] Some of these firms share data with other outsiders, an arrangement known as "piggybacking."

All this allows firms to glean what sites users have visited, what they have shopped for, what postcode they live in, and so on. From this the firms can infer other personal details, such as a person's income, the size of their home, and whether it is rented or owned.[9]

The system of data-gathering raises several consumer privacy questions. Other concerns relate to the security of the information and how to prevent data leakage.[10]

Effect of the Bill

The bill creates s. 934.60, F.S., which prohibits providers of electronic communications services to the public from providing 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 bill requires the request for permission:

- To be clear and conspicuous; and
- To require the subscriber or customer to take an affirmative action to acknowledge such permission.[11]

---

[1] *Getting to know you*, The Economist, September 14, 2013, http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party (last visited on March 10, 2015).
[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] *Id*.
[11] The bill specifies that consenting to a provider's terms and conditions or a provider's privacy statement describing such provider's data sharing practices shall constitute express permission.

The bill specifies that these provisions do not prohibit a provider of electronic communications services from complying with a lawful subpoena or warrant.

The bill authorizes a person to institute a civil action to seek injunctive relief to enforce compliance with the above-described provisions, or to recover damages and penalties from a provider that violates such provisions. A person is entitled to recover a $10,000 penalty for each violation. Additionally, civil actions must commence within 2 years after the date that the information is disclosed.

The bill also provides that the Legislature declares that digital data is property that is constitutionally protected from unreasonable search and seizure.

Search and Seizure

Generally

The Fourth Amendment to the United States Constitution (Fourth Amendment) protects individuals from unreasonable search and seizure.[12] The text of the Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[13]

A "search" generally occurs when a state actor infringes on an expectation of privacy that society considers to be reasonable.[14] In most instances, the Fourth Amendment requires that a warrant be issued before a search can be conducted.[15]

Article I, Section 12 of the Florida Constitution provides protection against unreasonable search and seizure in a manner similar to the United States Constitution. However, Section 12 provides additional protection for private communications as follows:

> The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated.[16]

Section 12 goes on to require that "[a]rticles or information obtained in violation of this right shall not be admissible in evidence if such articles or information would be inadmissible under decisions of the United States Supreme Court construing the 4th Amendment to the United States Constitution." Florida courts consistently hold that Section 12 of the Florida Constitution binds courts to render decisions in accordance with United States Supreme Court precedent on the Fourth Amendment.[17]

Exceptions to the Warrant Requirement

As noted above, the Fourth Amendment usually requires that a warrant be issued before a search can be conducted. However, a number of exceptions to the warrant requirement exist.[18] These exceptions are usually hallmarked by circumstances which make a warrant impractical, impossible, or unreasonable to obtain prior to conducting a search or seizure.

A common exception to the warrant requirement is the exigent circumstances exception, which allows a warrantless search under circumstances where the safety or property of officers or the public is

[12] *Arizona v. Hicks*, 480 U.S. 321 (1987); *U.S. v. Jacobsen*, 466 U.S. 109 (1983).
[13] U.S. CONST. amend. IV.
[14] *U.S. v. Jacobsen*, 466 U.S. 109 (1983); *U.S. v. Maple*, 348 F.3d 260 (D.C. Cir. 2003); *Fraternal Order of Police Montgomery County Lodge 35, Inc. v. Manger*, 929 A.2d 958 (Ct. Spec. App. M.D. 2007).
[15] *See e.g., Minnesota v. Dickerson*, 508 U.S. 366 (1993); *Arizona v. Hicks*, 480 U.S. 321 (1987); and *Ornelas v. U.S.*, 517 U.S. 690 (1996).
[16] FLA. CONST. art. I, § 12.
[17] *State v. Lavazzoli*, 434 So.2d 321 (Fla.1983); *Smallwood v. State*, 61 So.3d 448 (Fla. 2011).
[18] *Donovan v. Dewey*, 452 U.S. 594 (1981).

threatened.[19] "An entry may be justified by hot pursuit of a fleeing felon, the imminent destruction of evidence, the need to prevent a suspect's escape, or the risk of danger to the police or others."[20]

The "search incident to arrest" is an exception to the warrant requirement that arises out of the same safety-oriented logic that forms the basis for the exigent circumstances exception.[21] The United States Supreme Court has long recognized the exception to the warrant requirement for searches incident to arrest.[22] However, the Court has broadened this exception over time from the narrowly-tailored exception described in *Trupiano v. United States*,[23] to the broader exception described in *Chimel v. California*.[24] The Court in *Chimel* held that regardless of whether any additional exigency exists, "[w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons… [and] to search for and seize any evidence."[25] The Court continued to say a search incident to arrest may include searching the arrestee's person as well as any nearby area where the arrestee could have grabbed a weapon or evidence.[26]

Wall-Penetrating Radar

In recent years, researchers have developed new radar technologies that can "see" through walls and other objects.[27] Wall penetrating radar devices have been used mainly for military purposes (e.g., to provide a situational understanding of enemies inside a building while the army is operating a counter-terrorism action plan).[28] However, recent news reports suggest that at least 50 law enforcement agencies in the United States, including the FBI and the U.S. Marshals Office, have equipped their officers with such devices.[29]

The device these agencies are using looks like a stud-finder. Its display shows whether it has detected movement on the other side of a wall and, if so, how far away it is — it does not show a picture of what's happening inside.[30] Other radar devices have far more advanced capabilities, including three-dimensional displays of where people are located inside a building, according to marketing materials from their manufacturers. One is capable of being mounted on a drone.[31]

Officials say the information gleaned from using wall-penetrating radar devices is critical for keeping law enforcement officers safe if they need to storm buildings or rescue hostages. But privacy advocates have expressed concern about the circumstances in which law enforcement agencies may be using the radars.[32]

To date, courts have not specifically ruled whether the use of wall-penetrating radar constitutes a search for Fourth Amendment purposes. However, in *Kyllo v. U.S.*,[33] the United States Supreme Court reviewed a case in which a thermal imaging device was used to determine whether the defendant was in his home. The Court held that when the government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical

---

[19] *Minnesota v. Olson*, 495 U.S. 91 (1990).
[20] *Id.* at 91.
[21] *Arizona v. Gant*, 556 U.S. 332 (2009).
[22] *Trupiano v. United States*, 334 U.S. 699 (1948).
[23] The Court described the exception as "a strictly limited right" of law enforcement officers, and further explained that the exception does not exist simply on the basis that an arrest has been affected. *Trupiano*, 344 U.S. at 708.
[24] *Chimel v. California*, 395 U.S. 752, 763 (1969).
[25] *Id.*
[26] *Id.*
[27] *Seeing through walls: New radar technology provides real-time video of what's going on behind solid walls*, October 18, 2011, http://www.sciencedaily.com/releases/2011/10/111018102703.htm (last visited March 5, 2015).
[28] *Super-resolution imaging with wall penetrating radar*, July 8, 2014, http://www.dgist.ac.kr/site/dgist_eng/menu/508.do?siteId=dgist_eng&snapshotId=3&pageId=429&cmd=read&contentNo=27398 (last visited March 5, 2015).
[29] *New police radars can 'see' inside homes*, Brad Heath, USA Today, January 20, 2015, http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/ (last visited March 5, 2015).
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] 553 U.S. 27 (2001).

intrusion, the surveillance is a Fourth Amendment search and is presumptively unreasonable without a warrant.[34]

Effect of the Bill

The bill creates s. 933.41, F.S., which prohibits law enforcement officers and agencies from using a wall-penetrating radar device, except pursuant to a valid warrant or pursuant to a lawful exception to the search warrant requirement.

The bill specifies that evidence obtained in violation of the prohibition is not admissible in a criminal, civil, administrative, or other proceeding except as proof of a violation.

Portable Electronic Devices

Search and Seizure

In 2013, the Florida Supreme Court reviewed a case in which a law enforcement officer searched an arrestee's cell phone after placing the arrestee in the officer's patrol car.[35] After extensively reviewing relevant state and federal case law, the Court held that the search incident to arrest exception to the search warrant requirement does not allow a police officer to search an arrestee's cell phone.[36] The Court reasoned that because there was no possibility that the suspect could use the device as a weapon or destroy evidence that existed on the phone, the rationales for the exception did not apply.[37]

Florida Security of Communications

Currently, ch. 934, F.S., governs the security of electronic and telephonic communications. The law covers a number of different investigative and monitoring procedures, including wiretapping, obtaining service provider records, and mobile tracking devices, among others.

Law enforcement officers are currently authorized to acquire service providers' records for portable electronic devices on the provider's network after securing a court order issued under s. 934.23(5), F.S.[38] In order to obtain this court order, the law enforcement officer is required to offer "specific and articulable facts showing that there are reasonable grounds to believe the contents of a wire or electronic communication or the records of other information sought are relevant and material to an ongoing criminal investigation."[39] The showing of "specific and articulable facts" required in s. 934.23(5), F.S., is a lower standard than the probable cause standard[40] required for obtaining a lawful warrant.

Effect of the Bill

Search and Seizure

The bill defines the term "portable electronic device" (PED) as any portable device that is capable of creating, receiving, accessing, or storing electronic data or communications, including, but not limited to, cellular telephones.

The bill creates s. 934.70, F.S., which specifies that information[41] contained in a PED is not subject to a search by a government entity,[42] including a search incident to arrest, except pursuant to a valid warrant or pursuant to a lawful exception to the search warrant requirement. Evidence obtained in

---

[34] *Id*.
[35] *Smallwood v. State*, 113 So. 3d 724 (Fla. 2013).
[36] *Id*.
[37] *Id*.
[38] *Mitchell v. State*, 25 So.3d 632 (Fla. 4th DCA 2009).
[39] Section 934.23(5), F.S.
[40] *Tracey v. State*, 69 So.3d 992, 998 (Fla. 4th DCA 2011).
[41] The bill defines "information" to include 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.
[42] The bill defines "government entity" as 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.

violation of this provision is not admissible in a criminal, civil, administrative, or other proceeding except as proof of a violation.

Nondisclosure Agreements
The bill prohibits a government entity from entering into a nondisclosure agreement with a vendor who sells equipment to monitor electronic devices. All existing nondisclosure agreements are declared void as being against the public policy of the state. The bill also specifies that records otherwise protected by such agreements are declared subject to the public records laws, and requires an agency to disclose such agreements or related records upon request.

The bill specifies that a person injured by a government entity as a result of a violation of the above-described provision may bring a civil action against the government entity.

Reporting Requirements
The bill requires communication common carriers and electronic communications services doing business in this state to annually[43] report the following information for the preceding calendar year to the Florida Department of Law Enforcement (FDLE):[44]

- The number of requests made for pen register or trap and trace information;
- The number of requests made for electronic serial number reader information;
- The number of requests made for location information;
- The number of individuals whose location information was disclosed; and
- The amount that each law enforcement agency was billed by the communication common carrier or electronic communications service for such requests.

The bill also imposes a multitude of reporting requirements on the courts and state attorneys relating to the application for PED search warrants. Specifically, the bill requires the court to submit the following information to FDLE:

- The receipt of an application for a warrant;
- The type of warrant for which the application was made;
- Whether any application for an order of extension was granted, granted as modified by the court, or denied;
- The period of monitoring authorized by the warrant and the number and duration of any extensions of the warrant;
- The offense under investigation, as specified in the application for the warrant or an extension of the warrant; and
- The name of the law enforcement agency or prosecutor that submitted an application for the warrant or an extension of the warrant.

This information must be reported:

- By the 30th day after expiration of a PED search warrant or an order extending the period of a PED search warrant; or
- By the 30th day after the court denies an application for a PED search warrant.

The bill requires each prosecutor that submits an application for a PED search warrant or an extension of a PED search warrant to submit the following information for the preceding calendar year to FDLE:

- The information required to be submitted by a court (described above) with respect to each application submitted by the prosecutor for the warrant or an extension of the warrant;
- A general description of information collected under each warrant 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 those individuals;
- The number of arrests made as a result of information obtained under a PED search warrant;
- The number of criminal trials commenced as a result of information obtained under a PED search warrant; and

[43] By January 15th of each year.
[44] Disaggregated by each law enforcement agency in this state making the applicable requests.

- The number of convictions obtained as a result of information obtained under a PED search warrant.[45]

The bill specifies that all of the above-described reports that are submitted to FDLE are subject to disclosure under the public records laws and are not confidential or exempt.

By March 1 of each year, FDLE must submit a report to the Governor and the Legislature that contains the following information for the preceding calendar year:

- 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;
- A comparison of the ratio of the number of applications for PED warrants to the number of arrests and convictions resulting from information obtained under a PED warrant;
- Identification of the types of offenses investigated under a PED warrant; and
- With respect to both state and local jurisdictions, an estimate of the total cost of conducting investigations under a PED warrant.

Student Data

Florida law contains a variety of provisions relating to the privacy of student data. For example, s. 1002.22, F.S., requires the rights of students and their parents with respect to education records created, maintained, or used by public educational institutions and agencies to be protected in accordance with the Family Educational Rights and Privacy Act (FERPA)[46] and the implementing regulations issued pursuant thereto. In order for public educational institutions and agencies to remain eligible to receive federal funds and participate in federal programs, the State Board of Education must comply with the FERPA after the board has evaluated and determined that the FERPA is consistent with the following principles:

- Students and their parents shall have the right to access their education records, including the right to inspect and review those records.
- Students and their parents shall have the right to waive their access to their education records in certain circumstances.
- Students and their parents shall have the right to challenge the content of education records in order to ensure that the records are not inaccurate, misleading, or otherwise a violation of privacy or other rights.
- Students and their parents shall have the right of privacy with respect to such records and reports.
- Students and their parents shall receive annual notice of their rights with respect to education records.[47]

The statute specifies that if any official or employee of an institution refuses to comply, the aggrieved parent or student has an immediate right to bring an action in circuit court to enforce his or her rights by injunction.[48]

Similarly, s. 1002.221, F.S., specifies that education records, as defined in FERPA, are confidential and exempt from public record. The statute prohibits an agency or institution[49] from releasing a student's education records without the written consent of the student or parent to any individual, agency, or organization, except in accordance with and as permitted by the FERPA.[50]

---

[45] This information must be submitted by January 15 of each year.
[46] 20 U.S.C. § 1232g.
[47] Section 1002.22, F.S.
[48] *Id*. Any aggrieved parent or student who receives injunctive relief may be awarded attorney fees and court costs
[49] Section 1002.22, F.S., defines "agency" as any board, agency, or other entity that provides administrative control or direction of or performs services for public elementary or secondary schools, centers, or other institutions as defined in this chapter. "Institution" is defined as any public school, center, institution, or other entity that is part of Florida's education system under s. 1000.04(1), (3), and (4).
[50] Section 1002.221, F.S.

Section 1002.221, F.S., also allows an agency or institution, in accordance with FERPA, to release a student's education records without written consent of the student or parent to parties to an interagency agreement among the Department of Juvenile Justice, the school, law enforcement authorities, and other signatory agencies.[51] The statute specifies that information provided in furtherance of an interagency agreement is intended solely for use in determining the appropriate programs and services for each juvenile or the juvenile's family, or for coordinating the delivery of the programs and services, and as such is inadmissible in any court proceeding before a dispositional hearing unless written consent is provided by a parent or other responsible adult on behalf of the juvenile.[52]

In addition, s. 1002.222, F.S., prohibits an agency or institution from:

- Collecting, obtaining, or retaining information on the political affiliation, voting history, religious affiliation, or biometric information[53] of a student or a parent or sibling of the student.
- Sharing education records made confidential and exempt by s. 1002.221, F.S., or federal law to:
    - A person, except when authorized by s. 1002.221, F.S., or in response to a lawfully issued subpoena or court order;
    - A public body, body politic, or political subdivision except when authorized by s. 1002.221, F.S., or in response to a lawfully issued subpoena or court order; or
    - An agency of the federal government except when authorized by s. 1002.221, F.S., required by federal law, or in response to a lawfully issued subpoena or court order.

According to the State University System Board of Governors (BOG), each university has regulations and policies related to student data privacy.[54] The BOG also notes that most identifying student information is protected under federal law (FERPA) and state law (ss. 1002.222 and 1002.225, F.S.).[55] According to the BOG, FERPA prohibits schools from disclosing student education records or non-directory information (e.g., student identification numbers, financial records, etc.) without consent.[56]

Effect of the Bill

The bill creates a new section of statute, s. 1002.227, F.S., that prohibits data collected on a student who is 18 years of age or older from being provided to the federal government or to commercial companies without the written consent of the adult student. Similarly, the bill prohibits data collected on a student who is younger than 18 years of age from being provided to the federal government or to commercial companies without the written consent of the parent or the guardian of the student.

The bill requires all contracts between school districts and companies that process or receive student data (company) to explicitly prohibit such 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.

The bill specifies that any data collected from students through online learning is the property of the school district, not the company.

The bill prohibits technical companies that contract with public schools from mining student data for commercial purposes.

---

[51] *Id*.
[52] *Id*.
[53] "Biometric information" means information collected from the electronic measurement or evaluation of any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty. Examples of biometric information include, but are not limited to, a fingerprint or hand scan, a retina or iris scan, a voice print, or a facial geometry scan. Notwithstanding the provisions of this paragraph, a school district that used a palm scanner system for identifying students for breakfast and lunch programs on March 1, 2014, may continue to use the palm scanner system through the 2014-2015 school year. s. 1002.222, F.S.
[54] State University System Board of Governors 2015 Legislative Bill Analysis of HB 571, March 3, 2015 (on file with the Criminal Justice Subcommittee).
[55] *Id*.
[56] *Id*.

The bill also provides that 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:

- Stored in a student information system must be deleted.
- In the possession or under the control of a school employee or third party must be deleted or destroyed.

The bill specifies that a violation of the above-described provisions shall result in a civil fine of up to $10,000 against the elected school board members under whose jurisdiction the violation occurred. 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 violated these above-described provisions.

Driver Licenses - RFID Technology

RFID Technology

Radio Frequency Identification (RFID) technology uses radio waves to identify people or objects. RFID devices read information contained in a wireless device or "tag" from a distance without making any physical contact or requiring a line of sight.[57] RFID technology has been commercially available in some form since the 1970s.[58] It is now part of our daily lives, and can be found in car keys, employee identification, medical history/billing, highway toll tags and security access cards.[59]

The United States government uses two types of RFID technology for border management:

- Vicinity RFID-enabled documents can be securely and accurately read by authorized readers from up to 20 to 30 feet away.
- Proximity RFID-enabled documents must be scanned in close proximity to an authorized reader and can only be read from a few inches away.[60]

According to the U.S. Department of Homeland Security (USDHS), no personal information is stored on RFID cards – only a number, which points to the information housed in secure databases.[61]

Driver Licenses

In recent years, the USDHS has been working with states to enhance their driver licenses and identification documents to comply with travel rules under the Western Hemisphere Travel Initiative.[62] State-issued enhanced drivers licenses (EDLs) provide proof of identity and U.S. citizenship, are issued in a secure process, and include technology that makes travel easier.[63]

The USDHS reports that the top 39 land ports of entry, which process more than 95 percent of land border crossings, are equipped with RFID technology that helps facilitate travel by individual presenting EDLs or one of the other RFID-enabled documents.[64] As such enhanced drivers licenses make it easier for U.S. citizens to cross the border into the United States because they include:

- A vicinity Radio Frequency Identification (RFID) chip that will signal a secure system to pull up your biographic and biometric data for the border patrol officer as you approach the border inspection booth; and

---

[57] *Radio Frequency Identification (RFID): What is it?*, U.S. Department of Homeland Security, August 9, 2012, http://www.dhs.gov/radio-frequency-identification-rfid-what-it (last visited on March 11, 2015).
[58] *Id*.
[59] *Id*.
[60] *Id*.
[61] *Id*
[62] *Enhanced Drivers Licenses: What Are They?* U.S. Department of Homeland Security, November 6, 2014, http://www.dhs.gov/enhanced-drivers-licenses-what-are-they (last visited on March 11, 2015).
[63] *Id*.
[64] *Id*.

- A Machine Readable Zone (MRZ) or barcode that the border patrol officer can read electronically if RFID isn't available.[65]

Florida Legislation
In recent years, legislation has been filed in Florida that prohibited the Florida Department of Highway Safety and Motor Vehicles (DHSMV) from incorporating RFID technology into driver licenses and identification cards.[66] None of this legislation has become law.

Effect of the Bill
The bill prohibits the Department of Highway Safety and Motor Vehicles (DHSMV) from:
- Incorporating any radio frequency identification device, or "RFID," or any similar electronic tracking device upon or within any driver license or identification card; and
- Obtaining 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.

B. SECTION DIRECTORY:

Section 1. Cites the act as the "Florida Privacy Protection Act."

Section 2. Provides a legislative declaration that digital data is property that is constitutionally protected from unreasonable search and seizure.

Section 3. Creates s. 933.41, F.S., relating to prohibition against search using wall-penetrating radar device.

Section 4. Creates s. 934.60, F.S., relating to Internet protocol address privacy.

Section 5. Creates s. 934.70, F.S., relating to portable electronic device privacy.

Section 6. Creates s. 1002.227, F.S., relating to contract requirements relating to student data.

Section 7. Prohibits the Department of Highway Safety and Motor Vehicles from incorporating any radio frequency identification device upon or within a driver license or identification card and from obtaining fingerprints or biometric DNA material from a US citizen fur purposes of issuing, renewing, reinstating, or modifying a driver license or identification card.

Section 8. Provides a severability clause.

Section 9. Provides an effective date of July 1, 2015.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill specifies that violations of the student data privacy provisions shall result in a civil fine of up to $10,000 against the elected school board members under whose jurisdiction the violation occurred. Such fines would be deposited into the fine and forfeiture fund pursuant to s. 142.01, F.S. This may have a positive fiscal impact on state government.

2. Expenditures:

[65] *Id*.
[66] *See, e.g.,* SB1346 (2014), HB 109 (2012), SB 220 (2012), and CS/CS/SB 1150 (2011).

The bill imposes a multitude of reporting requirements on the courts, state attorneys, and the Florida Department of Law Enforcement (FDLE) relating to cases in which a PED search warrant was applied for. These requirements may have a negative fiscal impact on these entities.

The bill authorizes a person to bring a civil action against a government entity that enters into a nondisclosure agreement when a vendor who sells equipment to monitor electronic devices. This could have a negative fiscal impact on government entities.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill does not appear to have an impact on local government revenues.

2. Expenditures:

The bill does not appear to have an impact on local government expenditures.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill prohibits providers of electronic communications services to the public from providing 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 bill authorizes a civil action against providers who violate this prohibition. These provisions could have a substantial negative fiscal impact on providers.

The bill specifies that violations of the student data privacy provisions shall result in a civil fine of up to $10,000 against the elected school board members under whose jurisdiction the violation occurred. This may have a negative fiscal impact on such school board members.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

This bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

The bill does not appear to create a need for rulemaking or rulemaking authority.

C. DRAFTING ISSUES OR OTHER COMMENTS:

Portable Electronic Devices
The bill imposes a variety of reporting requirements relating to PED warrants on the courts (e.g., whether the warrant was granted, the offense under investigation, and the name of the law enforcement agency or prosecutor submitting the warrant). No such reporting requirements exist for search warrants for any other type of object.

The bill also imposes a variety of reporting requirements relating to PED warrants on state attorneys (e.g., a general description of information collected under each warrant, he number of arrests made as a result of information obtained under a warrant, the number of criminal trials commenced as a result of information obtained under warrant; and the number of convictions obtained as a result of information obtained under warrant). No such reporting requirements exist for search warrants for any other type of object. Additionally, it is likely not possible to accurately report whether a trial commenced or a convicted was obtained solely because of the issuance of a PED warrant.

The bill also requires FDLE to submit a report to the Governor and the Legislature that contains the following information for the preceding calendar year:

- 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;
- A comparison of the ratio of the number of applications for PED warrants to the number of arrests and convictions resulting from information obtained under a PED warrant;
- Identification of the types of offenses investigated under a PED warrant; and
- With respect to both state and local jurisdictions, an estimate of the total cost of conducting investigations under a PED warrant.

It is likely not possible to determine whether an arrest or conviction resulted from the issuance of a PED warrant. Nor is it likely feasible for FDLE to estimate the total cost of conducting investigations under a PED warrant.

Internet Privacy

The bill prohibits providers of electronic communications services to the public from providing 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. It is unknown how often providers of electronic communications services currently engage in this behavior. It is also unknown the reasons providers share such information. However, to the extent providers are sharing such information for legitimate and appropriate reasons, they will no longer be able to do so.

Student Data

The bill prohibits data collected on students from being provided to the federal government or to commercial companies without the written consent of the student (or their parent if the student is under 18). The BOG reports that if universities are required to obtain written consent of the student or the student's parent or guardian prior to releasing information to the federal government or commercial companies, this will impede the university and the company acting on its behalf from complying with exceptions to FERPA and Florida Public Records laws.[67]

The bill requires all contracts between school districts and companies that process or receive student data (company) to explicitly prohibit such 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. The BOG reports that it is unclear whether the bill's contract requirements apply to school districts only or any institution with student data.[68]

The bill also requires all personally identifiable student data, with few exceptions, to be deleted or destroyed upon the student's graduation, withdrawal, or expulsion except as otherwise required by law. The BOG reports that while record retention schedules promulgated by the Division of Library and Information Services may allow these records to be retained for a period of time, once that period has expired the document must be destroyed despite best practices or the best interest of the university.[69]

The BOG reports that it is unclear whether the newly-created s. 1002.227, F.S., applies to school districts only, or whether universities are included. If the section applies to universities, then subsection

[67] State University System Board of Governors 2015 Legislative Bill Analysis of HB 571, March 3, 2015 (on file with the Criminal Justice Subcommittee).
[68] *Id*.
[69] *Id*.

(3) (prohibiting data collected on students from being provided to the federal government or to commercial companies without the written consent of the student) would seem to conflict with many critical data processes currently in place across the State University System both for federal and state reporting.[70]

In order to receive federal student financial aid, the universities and the BOG need access to longitudinal student records for financial aid auditing and reporting requirements.[71] The universities and the Board of Governors aggregate this longitudinal data in order to supply aggregate reports to the federal government to meet their requirements. Without these records universities would not be able to comply with federal audit and reporting requirements which would jeopardize their ability to receive federal student financial aid.[72]

These data are also used to establish metrics for use with Florida's standard and performance-based university budgeting process.[73] Deletion of student information upon graduation, withdrawal, or expulsion would prohibit the universities and the Board from accurately creating and validating the annual budget. Florida's longitudinal student data is also used by all of Florida's educational sectors in program evaluation, program improvement, articulation, student transfer, credentialing, and by state auditors. The inability of institutions to hold this data would adversely affect their ability to perform standard operations.[74] Deletion of student educational information upon withdrawal or expulsion deprives universities of the ability to readmit students previously withdrawn, transfer educational information at the request of withdrawn students transferring to another institution, and prevent readmission of expelled students. Deletion of educational information after graduation also prevents students from obtaining transcripts for internships, employment, and continuing education.[75]

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On March 12, 2015, the Criminal Justice Subcommittee adopted a strike-all amendment, and one amendment to the strike-all amendment, and reported the bill favorably as a committee substitute. The amendments, collectively:

- Removed provisions prohibiting government entities from selling personal identifying information for secondary commercial purposes;
- Removed provisions relating to license plate readers;
- Removed the misdemeanor penalty applicable to government entities entering into a nondisclosure agreement with a vendor who sells equipment to monitor electronic devices;
- Prohibited law enforcement officers and agencies from using a wall-penetrating radar device, except pursuant to a valid warrant or pursuant to a lawful exception to the search warrant requirement; and
- Renumbered sections of statute that the bill created.

This analysis is drafted to the committee substitute as passed by the Criminal Justice Subcommittee.

[70] *Id*.
[71] *Id*.
[72] *Id*.
[73] *Id*.
[74] *Id*.
[75] *Id*.