HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 669 Offenses Involving Computers
SPONSOR(S): Criminal Justice Subcommittee, Grieco
TIED BILLS: **IDEN./SIM. BILLS:** SB 916

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	14 Y, 0 N, As CS	Bruno	Hall
2) Justice Appropriations Subcommittee	9 Y, 0 N	Jones	Gusky
3) Judiciary Committee			

SUMMARY ANALYSIS

Digital platforms, computer software, phone applications (apps), smart home systems, and home security systems access the most intimate details of a user's life. These technologies can monitor a person's location; log personal, health, and financial data; send, receive, and log communications; and capture and store video and photographs. While providing everyday convenience to the user, these technologies are also susceptible to unauthorized access and abusive surveillance.

Florida law criminalizes certain acts involving a computer, computer system, computer network, or electronic device, such as accessing it or disrupting data, when done knowingly, willfully, and without authorization. In 2018, Miami-Dade County prosecutors dismissed charges against a man accused of repeatedly logging into his ex-girlfriend's home security system to secretly watch her in her home, citing an inability to prove that he did so "without authorization," as statutorily required. In that case, the victim previously authorized the defendant to access the security system during their relationship; although prosecutors believed the defendant exceeded the scope of his authorized access, they were unable to pursue charges against him.

Cyberstalking is a course of conduct that: communicates words, images, or language by or through the use of electronic mail or electronic communication; is directed at a specific person; causes that person substantial emotional distress; and serves no legitimate purpose. A person who willfully, maliciously, and repeatedly cyberstalks another person commits first degree misdemeanor stalking, punishable by up to one year in county jail and a $1,000 fine. Aggravating factors enhance stalking behavior to a third degree felony.

CS/HB 669 includes acts "exceeding authorization" as offenses against users of computers, computer systems, computer networks, or electronic devices. The bill criminalizes unauthorized acts committed by means of authorized access, such as when an offender misuses knowledge of a password.

The bill also expands the definition of cyberstalking to include accessing, or attempting to access, the online accounts or Internet-connected home electronic systems of another person without permission. A person who willfully, maliciously, and repeatedly accesses another person's account without his or her permission commits stalking.

On February 27, 2019, the Criminal Justice Impact Conference reviewed this bill and estimated it would have a "positive indeterminate" impact on prison beds (an unquantifiable increase in prison beds). The bill is also likely to have a positive indeterminate impact on jail beds.

The bill provides that it is effective upon becoming a law.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Digital platforms, computer software, phone applications (apps), smart home systems,[1] and home security systems access the most intimate details of a user's life. These technologies can monitor a person's location; log personal, health, and financial data; send, receive, and log communications; and capture and store video and photographs. While providing everyday convenience to the user, these technologies are also susceptible to unauthorized access and abusive surveillance.

A growing spyware market caters to people seeking to catch cheating partners and spy on exes.[2] A recent academic study found over 200 apps and services capable of spying through location tracking, intercepting text messages, and secretly recording video.[3] Some apps exist for legitimate functions, such as monitoring children or meeting up with friends, but are prone to misuse; others, not available on traditional app store marketplaces, explicitly promote illicit spying activity.[4] Several online communities and forums provide how-to advice for finding and using spyware apps.[5]

Abusers harass victims using spyware and other technologies in a number of ways. For example, an abuser can weaponize private data obtained through spyware apps to embarrass or exploit a victim, or access a smart home system to unnerve and assert control over a victim by changing thermostat settings, unlocking doors, turning on lights, or playing music.[6] A security expert recently demonstrated how an Amazon Echo's microphone might be hacked, permitting an abuser to eavesdrop on a victim.[7]

Use of these technologies can also escalate into physical violence. In a 2013 Florida case, a Deltona man installed an app called "SMS Tracker" onto his wife's phone, allowing him to see text messages and photographs she was exchanging with others.[8] Upon discovering she was having an affair, he murdered her and her 8- and 9-year-old children.

Several Florida laws impose criminal liability for cyberharassment and hacking activities, including:

- Offenses against users of computers, computer systems, computer networks, and electronic devices.[9]
- Cyberstalking.[10]

---

[1] Smart home devices are connected to the internet and offer services such as voice-controlled lights, thermostats, and locks. Examples of smart home devices include the Amazon Echo, Google Home, and platforms such as Samsung SmartThings and Apple Homekit. Eric Zeng, Shrirang Mare, and Franziska Roesner, *End User Security & Privacy Concerns with Smart Homes*, University of Washington (July 2017), https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf (last visited Mar. 19, 2019).
[2] Rahul Chatterjee, *et al*, *The Spyware Used in Intimate Partner Violence*, 2018 IEEE Symposium on Security and Privacy (May 20, 2018), https://www.ipvtechresearch.org/pubs/spyware.pdf (last visited Mar. 19, 2019).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Amanda Kippert, *Smart Home Technology Is Being Used Against Survivors* (Jan. 14, 2019), https://www.domesticshelters.org/articles/technology/smart-home-technology-is-being-used-against-survivors (last visited Mar. 19, 2019).
[7] Jay McGregor, *Listening-in on a Hacked Amazon Echo is Terrifying*, Forbes (Sept. 7, 2017), https://www.forbes.com/sites/jaymcgregor/2017/09/07/listening-in-on-a-hacked-amazon-echo-is-terrifying/#32744f415c7f (last visited Mar. 19, 2019).
[8] Frank Fernandez, *Luis Toledo gets 3 consecutive life sentences for murders of wife, her 2 children*, Daytona-Beach News Journal Online (Jan. 19, 2018), https://www.news-journalonline.com/news/20180119/luis-toledo-gets-3-consecutive-life-sentences-for-murders-of-wife-her-2-children (last visited Mar. 19, 2019); Jennifer Valentino-DiVries, *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, New York Times (May 19, 2018), https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html (last visited Mar. 19, 2019).
[9] S. 815.06, F.S.
[10] S. 784.048, F.S.

- Wiretapping.[11]
- Sexual cyberharassment.[12]

Offenses against Users of Computers

Florida law criminalizes the following acts involving a computer,[13] computer system,[14] computer network,[15] or electronic device[16] when done knowingly, willfully, and without authorization:

- Accessing it with knowledge that such access is unauthorized.
  - Accessing means approaching, instructing, communicating with, storing data in, retrieving data from, or otherwise making use of any resources of a computer, computer system, or computer network.[17]
- Disrupting or denying its ability to transmit data to or from an authorized user under certain circumstances.
- Destroying, taking, injuring, or damaging it, its equipment, or supplies.
- Introducing a computer contaminant.
- Engaging in audio or video surveillance of an individual by accessing one of its inherent features or components, including accessing the data or information stored by a third party.[18]

In general, proscribed conduct against a computer user is a third degree felony,[19] punishable by up to five years in prison and a $5,000 fine.[20] However, the crime is a second degree felony, punishable by up to 15 years in prison and a $10,000 fine,[21] if a person:

- Causes at least $5,000 in damage;
- Acts to defraud or obtain property;
- Interrupts or impairs a government operation or public service;
- Intentionally interrupts public or private transit data transmission; or
- Accesses a computer, computer system, computer network, or electronic device belonging to a mode of public or private transit without authorization.[22]

The crime is enhanced to a first degree felony, punishable by up to 30 years in prison and a $10,000 fine,[23] if the conduct:

- Endangers human life; or
- Disrupts the direct administration of medical care or treatment to a person.[24]

[11] S. 943.03, F.S.
[12] S. 784.049, F.S.
[13] "Computer" means an internally programmed, automatic device that performs data processing. S. 815.03(2), F.S.
[14] "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files. S. 815.03(7), F.S.
[15] "Computer network" means a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or other electronic equipment that is connected to the computer systems or electronic devices by physical or wireless telecommunication facilities. S. 815.03(4), F.S.
[16] "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose. S. 815.03(9), F.S.
[17] S. 815.03(9), F.S.
[18] S. 815.06(2), F.S.
[19] S. 815.06(3)(a), F.S.
[20] Ss. 775.082 and 775.083, F.S.
[21] *Id.*
[22] S. 815.06(3)(b), F.S.
[23] Ss. 775.082 and 775.083, F.S.
[24] S. 815.06(3)(c), F.S.

"Without Authorization"

In 2018, Miami-Dade County prosecutors dismissed charges against a man accused of repeatedly logging into his ex-girlfriend's home security system to secretly watch her in her home, citing an inability to prove that he did so "without authorization" as statutorily required.[25] In that case, the victim previously authorized the defendant to access the security system occasionally during their relationship, leading prosecutors to conclude:

> [E]ven though [the victim] did not intend or allow [the defendant] to repeatedly, on various days, and after their relationship ended, access her home security cameras, this conduct could not be prosecuted because while dating, she may have authorized remote access [to the system] on an isolated occasion or for limited purposes.[26]

Florida case law supports this conclusion. In *Rodriguez v. State*,[27] the Fourth District Court of Appeal (Fourth DCA) held that an employee who used a computer that he was authorized to use to perform a function he was not authorized to perform had not committed an offense against a computer user under Florida law. The Fourth DCA specifically noted that the federal statutes proscribing similar conduct include the phrase "or exceeding authorized access" to address such a situation.[28] "Exceeding authorized access" in federal statute means accessing a computer with authorization and using such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.[29]

In *Umhoefer v. State*,[30] the Second District Court of Appeal (Second DCA) upheld the conviction of a man who accessed his girlfriend's social media account after she changed her password. Because the man had to use a password bypassing app to access the account, the Second DCA held that such access was "unauthorized," as statutorily required. Whether a person is criminally liable under this statute thus may turn on whether a victim has the sophistication and foresight to change all of his or her passwords, regardless of whether the surrounding facts suggest the manner of use was unauthorized.

Stalking and Cyberstalking

Cyberstalking is a course of conduct[31] that:

- Communicates words, images, or language by or through the use of electronic mail or electronic communication;
- Is directed at a specific person;
- Causes that person substantial emotional distress; and
- Serves no legitimate purpose.[32]

A person who willfully, maliciously, and repeatedly cyberstalks another person commits first degree misdemeanor stalking,[33] punishable by up to one year in county jail and a $1,000 fine.[34] A person faces a felony charge for cyberstalking when he or she:

- Makes a credible threat against the victim;
- Is subject to a court-ordered prohibition of contact with the victim, such as an injunction;

[25] Jose Arrojo, Chief Assistant State Attorney, Office of the State Attorney: Eleventh Judicial Circuit, *Colin Knight, F17-23267, Re: Case Disposition – Chief's Summary & Proposed Further Action* (Aug. 9, 2018).
[26] *Id.*
[27] 956 So.2d 1226 (Fla. 4th DCA 2007).
[28] *Id.* at 1230; 18 U.S.C. § 1030.
[29] 18 U.S.C. § 1030(e)(6).
[30] 235 So.3d 989 (Fla. 2d DCA 2017).
[31] "Course of conduct" means a series of acts over a period of time, however short, evidencing continuity of purpose. S. 746.048(1)(b), F.S.
[32] S. 746.048(1)(d), F.S.
[33] S. 784.0048(2), F.S.
[34] Ss. 775.082 and 775.083, F.S.

- Cyberstalks a victim younger than 16; or
- Has a prior conviction for certain sexual offenses and cyberstalks the victim of that offense in violation of a no contact order.[35]

A person may also be charged with stalking for willfully, maliciously, and repeatedly harassing another. Harassment is a course of conduct that:
- Is directed at a specific person;
- Causes that person substantial emotional distress; and
- Serves no legitimate purpose.[36]

Conduct involving digital technologies that does not qualify specifically as cyberstalking may nonetheless qualify as harassment and also give rise to criminal liability for stalking.

Other Relevant Crimes

Florida law prohibits wiretapping.[37] Subject to exceptions, it is a third degree felony[38] for a person to intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept a wire, oral, or electronic communication.[39] Some spyware uses may qualify as wiretapping.

In 2015, the Legislature addressed the growing problem of "revenge porn," which is the publication of sexually explicit photographs taken consensually but expected to remain private, by criminalizing sexual cyberharassment.[40] A person commits sexual cyberharassment by publishing a sexually explicit image that contains or conveys the personal identification information of the depicted person to the Internet:
- Without the depicted person's consent;
- For no legitimate purpose; and
- With the intent of causing the depicted person substantial emotional distress.[41]

A first sexual cyberharassment offense is a first degree misdemeanor; a second or subsequent offense is a third degree felony.[42] A sexual cyberharassment victim may also civilly sue an offender for injunctive relief, damages, and reasonable attorney fees and costs.[43]

Effect of Proposed Changes

CS/HB 669 includes acts "exceeding authorization" as offenses against users of computers, computer systems, computer networks, or electronic devices. The bill criminalizes unauthorized acts committed by means of authorized access, such as when an offender misuses knowledge of a password. An offense against a computer user that exceeds authorization is generally a third degree felony, unless an aggravating circumstance enhances the conduct to a second or first degree felony.

The bill amends the definition of "access" for purposes of computer-related crimes to include approaching, instructing, communicating with, storing data from, or otherwise making use of any resources of an electronic device.

The bill also expands the definition of cyberstalking to include accessing, or attempting to access, the online accounts or Internet-connected home electronic systems of another person without permission.

[35] Ss. 784.048(3), (4), (5), and (7), F.S.
[36] S. 784.048(1)(a), F.S.
[37] S. 934.03, F.S.
[38] A third degree felony is punishable by up to five years in prison and a $5,000 fine. Ss. 775.082 and 775.083, F.S.
[39] S. 934.03(1), F.S.
[40] Ch. 2015-24, § 1, Laws of Fla.
[41] S. 784.049(1)(c), F.S.
[42] S. 784.049(3), F.S.
[43] S. 784.049(5), F.S.

A person who willfully, maliciously, and repeatedly accesses another person's account without his or her permission commits stalking, a first degree misdemeanor or, with an aggravating factor, third degree felony.

B. SECTION DIRECTORY:

Section 1: Amends s. 748.048, F.S., relating to stalking; definitions; penalties.
Section 2: Amends s. 815.03, F.S., relating to definitions.
Section 3: Amends s. 815.06, F.S., relating to offenses against users of computers, computer systems, computer networks, and electronic devices.
Section 4: Reenacts s. 1006.147, F.S., relating to bullying and harassment prohibited.
Section 5: Provides an effective date upon becoming a law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

On February 27, 2019, the Criminal Justice Impact Conference reviewed this bill and determined it would have a "positive indeterminate" impact on prison beds (an unquantifiable increase in prison beds).

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

The bill may have a positive indeterminate impact on jail beds by expanding the scope of criminal offenses.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill appears to be exempt from the requirements of Article VII, Section 18, of the Florida Constitution because it is a criminal law.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

Not applicable.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On March 12, 2019, the Criminal Justice Subcommittee adopted an amendment and reported the bill favorably as a committee substitute. The amendment included electronic devices in the definition of the term “access” for computer-related crimes and clarified that accessing a computer, computer system, computer network, or electronic device with knowledge that the manner of use exceeds authorization is a criminal offense.

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