The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Judiciary Committee

BILL:	CS/CS/SB 164
INTRODUCER:	Judiciary Committee, Commerce Committee, and Senator Ring
SUBJECT:	Offenses Against Computer Users
DATE:	March 19, 2009 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	O'Callaghan	Cooper	CM	**Fav/CS**
2.	Treadwell	Maclure	JU	**Fav/CS**
3.			CJ	
4.			JA	
5.				
6.				

Please see Section VIII. for Additional Information:

A. COMMITTEE SUBSTITUTE.....	X	Statement of Substantial Changes
B. AMENDMENTS.....		Technical amendments were recommended
		Amendments were recommended
		Significant amendments were recommended

I. Summary:

The bill expands computer users' protections under the Florida Computer Crimes Act (the act) by prohibiting certain unauthorized acts relating to computer usage. The bill provides that a person may not willfully, knowingly, and without authorization perform any of the following acts:

- Modify computer settings that control web pages, web proxies, or bookmarks;
- Collect personally identifiable information;
- Prevent an owner's or operator's efforts to block or disable computer software by automatically reinstalling the software;
- Misrepresent that computer software will be uninstalled or disabled;
- Remove, disable, or render inoperative security, antispyware, or antivirus computer software;
- Enable the use of a computer to cause damage to that computer, open messages that a computer user cannot close without closing a program or shutting off the computer, or transmit or relay commercial electronic mail or a virus from the computer;
- Modify settings related to accessing or using the Internet; or

- Prevent an owner's or operator's efforts to block or disable computer software by making certain misrepresentations and using specific strategies.

Under the bill, a person who is not an owner or operator of a computer is prohibited from inducing an owner or operator to install software by deceptively misrepresenting that the software is necessary for security or privacy reasons, or in order to open, view, or play a particular type of content. In addition, a person who is not an owner or operator of a computer is prohibited from using deception to execute computer software with the intent of causing the computer to use the software in a manner that violates any of the other prohibited acts provided in the act.

The bill makes all of these actions an offense against computer users, thus making a person who commits any of these actions subject to any civil or criminal penalties existing in current law.

Exceptions from liability are included for certain service providers providing security, technical support, maintenance, repair, or other specified services, and for providers that provide transmission, storage, or caching of electronic communications. There is also an exception for parents or guardians using software to monitor children's computer use.

The Department of Legal Affairs or a state attorney is granted authority to seek civil remedies and penalties on behalf of the people of the state.

The bill substantially amends the following sections of the Florida Statutes: 815.03 and 815.06. The bill also creates the following sections of the Florida Statutes: 815.051, 815.053, and 815.055.

II. Present Situation:

The Internet is commonly abused by criminals who illegally access personal records and steal information for unlawful purposes. According to the Federal Bureau of Investigation's (FBI) 2007 Internet Crime Report, more than 219,553 Internet crime complaints were processed by the bureau's Internet Crime Complaint Center (IC3) in 2007.[1] This widespread corruption in 2007 cost victims a total of $239.09 million, with a median dollar loss of $680.00 per complaint.[2]

Technology used by criminals often outpaces technology used to prevent or protect against Internet criminal activity.[3] The technology used, often referred to as malware (malicious software) or computer contaminants, includes viruses, Trojan horses, worms, spyware, and adware.[4] Malware is used to monitor another computer user's behavior and collect various types of personal information, including Internet surfing habits or passwords and PIN numbers, by capturing keystrokes of the computer user. Malware can also be used to redirect web browser

[1] National White Collar Crime Center, Bureau of Justice Assistance, and Federal Bureau of Investigation, *2007 Internet Crime Report*, 1 (2007), *available at* http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf (last visited Mar. 9, 2009).
[2] *Id*.
[3] Matt Hines, *Web users in malware crosshairs*, http://www.infoworld.com/article/08/04/08/Web-users-in-malware-crosshairs_1.html (Apr. 8, 2008) (last visited May 9, 2009).
[4] Jane M. Coviello, *Internet Safety: Legislative Initiatives for Our Protection*, 255 N.J. LAW 54, 58 (2008).

activity, install additional software on a computer, or change computer settings, resulting in slow connection speeds, slow processing speeds, or altered computer programs.[5]

Federal Protection Against Computer Crimes

There are several federal laws designed to prevent or impede computer users from committing crimes.[6] The Computer Fraud and Abuse Act (CFAA) is the most frequently used federal law for prosecuting various computer crimes.[7] The CFAA is a comprehensive law that makes it illegal to intentionally access a "protected computer" without authorization or in excess of authorization in order to obtain records of a financial institution, or to obtain personal records of consumers from a consumer reporting agency.[8] The act also makes it illegal to obtain information from any federal department or agency or any protected computer involved in interstate or foreign communications.[9] Furthermore, the CFAA makes it a crime to cause or attempt to cause damage to protected computers through malicious software such as viruses or worms.[10]

Florida Computer Crimes Act

Florida was the first state to respond to computer crime by enacting legislation in 1978, called the Florida Computer Crimes Act (the act), which criminalized certain uses of computers.[11] Since 1978, every state except Vermont has enacted legislation relating to unauthorized access or unauthorized alteration of computers.[12] Under the act, a third-degree felony is committed if an individual willfully, knowingly, and without authorization:

- Accesses or causes to be accessed any computer, computer system, or computer network;
- Disrupts or denies or causes the denial of computer system services to an authorized user of a computer;
- Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;
- Destroys, injures, or damages any computer, computer system, or computer network; or

[5] See OnGuard Online, *Spyware*, http://www.onguardonline.gov/topics/spyware.aspx (last visited March 11, 2009); OnGuard Online, *Malware*, http://www.onguardonline.gov/topics/malware.aspx (last visited March 11, 2009); and Robert Moir, Microsoft TechNet, *Defining Malware: FAQ* (Oct. 1, 2003), http://www.microsoft.com/technet/security/alerts/info/malware.mspx (last visited March 11, 2009).

[6] Federal laws used to combat computer crimes include: the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Cyber Security Enhancement Act, the Digital Millennium Copyright Act, the Economic Espionage Act, the National Stolen Property Act, the Federal Trade Commission Act, the Wiretap Act, and the U.S. SAFE WEB Act.

[7] See 18 U.S.C. s. 1030 and SANS Institute, Maxim May, *Federal Computer Crime Laws* (June 1, 2004), http://www.sans.org/reading_room/whitepapers/legal/federal_computer_crime_laws_1446?show=1446.php&cat=legal (last visited March 9, 2009).

[8] "Protected computer" under 18 U.S.C. s. 1030 means either a computer in use by a financial institution or the United States Government or a computer used in interstate or foreign commerce or communication.

[9] See 18 U.S.C. s. 1030.

[10] See 18 U.S.C. s. 1030 and SANS Institute, *supra* note 7.

[11] Richard C. Hollinger, *Computer Hackers Follow A Guttman-Like Progression*, http://phrack.org/issues.html?issue=22&id=7&mode=txt (last visited March 9, 2009).

[12] National Conference of State Legislatures, *Computer Crime Statutes: Index by Crime*, http://www.ncsl.org/programs/lis/CIP/compcrime-subs.htm (last visited March 9, 2009).

- Introduces any computer contaminant into any computer, computer system, or computer network.[13]

"Computer contaminant" is defined as "any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information."[14]

Under the act, if a person commits one of the above-listed crimes and causes damage of $5,000 or more, intends to devise or execute a scheme or artifice to defraud or obtain property, or interrupts or impairs a governmental operation or public communication, transportation, supply of water, gas, or other public service, he or she commits a felony of the second degree. A person committing a computer crime who also endangers human life commits a felony of the first degree. Additionally, an individual may file a civil suit against a person convicted for these computer crimes.[15]

Florida Deceptive and Unfair Trade Practices Act

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA) is a law under which challenges may be made to certain deceptive or unfair practices, which may include deceptive or unfair computer practices, affecting trade or commerce.[16] The FDUTPA prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce. "Trade or commerce," which includes the conduct of any trade or commerce, is defined as the advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated. The act provides for remedies such as cease and desist orders, injunctions, remedies by the enforcing authority, and the award of attorney's fees and costs to the prevailing party in civil litigation. A willful violation of FDUTPA subjects the violator to a civil penalty of not more than $10,000 for each violation.

Florida Security of Communications Act (Wiretap Statutes)

The use of malware may also be a violation of the Florida Security of Communications Act.[17] The act makes it illegal to intentionally intercept, endeavor to intercept, or procure another person to intercept or endeavor to intercept any wire, oral, or electronic communication.[18] Florida's Fifth District Court of Appeal has interpreted that using software to monitor another's communications over the Internet, to the extent that it is used to intercept real-time communication, is illegal under the act.[19] In *O'Brien v. O'Brien*, the court held that a wife's use

[13] Section 815.06, F.S.
[14] Section 815.03(3), F.S.
[15] Section 815.06, F.S.
[16] Chapter 501, part II, F.S.
[17] Chapter 934, F.S. The Florida requirements contained in this chapter governing the security of communications generally are no stricter than those imposed by the federal wiretap laws, but the language of the Florida statute tracks that of the federal statute almost exactly. 14A FLA. JUR 2D *Criminal Law* § 886 (2009).
[18] Section 934.03(1)(a), F.S.
[19] *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. 5th DCA 2005).

of spyware to monitor her husband's intimate communications with another woman was illegal under the act.[20]

III. Effect of Proposed Changes:

The bill expands computer users' protections under the Florida Computer Crimes Act by prohibiting certain unauthorized acts relating to malware and other unauthorized uses of computers. Following is a section-by-section analysis of the bill.

Section 1 amends s. 815.03, F.S., to define several terms used throughout the Florida Computer Crimes Act (the act), including:

- Cause to be copied;
- Computer software;
- Computer virus;
- Damage;
- Deceptive;
- Execute;
- Internet;
- Owner or operator;
- Message;
- Person; and
- Personally identifiable information.

Section 2 creates s. 815.051, F.S., to prohibit specific uses of computer software. This section provides that a person may not willfully or knowingly, and without authorization, perform any of the following acts:

- Modify, through deceptive means, computer settings that control web pages, web proxies, or bookmarks;
- Collect, through deceptive means, personally identifiable information;
- Prevent an owner or operator's efforts to block or disable computer software by automatically reinstalling the software;
- Misrepresent that computer software will be uninstalled or disabled;
- Remove, disable, or render inoperative security, antispyware, or antivirus computer software;
- Enable the use of a computer to cause damage to that computer, open messages that a computer user cannot close without closing a program or shutting off the computer, or transmit or relay commercial electronic mail or a virus from the computer;[21]
- Modify, through deceptive means, settings related to accessing or using the Internet; or
- Prevent an owner's or operator's efforts to block or disable computer software by making certain misrepresentations and using specific strategies.

[20] *Id.*

[21] The bill provides that this provision does not apply to communications originated by the computer's operating system, originated by a software application that the user chooses to activate, originated by a service provider that the user chooses to use, or presented for any of the purposes described in s. 815.06(7), F.S.

Section 3 creates s. 815.053, F.S., to prohibit a person who is not an owner or operator of a computer from inducing an owner or operator to install software by deceptively misrepresenting that the software is necessary for security or privacy reasons, or in order to open, view, or play a particular type of content. In addition, a person who is not an owner or operator of a computer is prohibited from using deception to execute computer software with the intent of causing the computer to use the software in a manner that violates any of the other prohibited acts provided in the Florida Computer Crimes Act.

Section 4 creates s. 815.055, F.S., to provide exceptions to prohibited uses of software. Software may be used by certain service providers (telecommunications carrier, cable operator, computer hardware or software provider, information service provider, or interactive computer service) to monitor or interact with an owner's or operator's computer to provide security, technical support, maintenance, repair, or other specified services. This section also specifies that no liability for violations of the provisions of the bill is imposed on certain service providers (communication service providers, commercial mobile service providers, and information service providers) for the transmission, storage, or caching of electronic communications. A final exemption is created that specifies that parents or guardians are not prohibited from using software to monitor their children's computer usage.

The bill also clarifies that the exceptions provided in this section do not provide a defense to any liability arising under the common law, any state law, or any federal law, and do not grant authority to engage in any action listed in the section. Although a person may not be criminally liable if he or she satisfies one of the enumerated exceptions, these exceptions do not constitute a defense if a person is sued civilly for actions related to computer usage.

Section 5 amends s. 815.06, F.S., to specify that any person using software as prohibited in ss. 815.051 and 815.053, F.S., commits an offense against computer users, which is a third-degree felony.[22] In some instances the violation may be a second-degree felony[23] if the offender violates these sections and:

- Damages a computer and related equipment with more than $5,000 in damages;
- Commits the offense for the purpose of devising or executing any scheme to defraud or obtain property; or
- Interrupts or impairs a governmental operation or public communication, transportation, or supply of utility services.

The bill provides specific authority for the Department of Legal Affairs (department) or a state attorney to file a civil action on behalf of the people of the state for injunctive relief against any person or group committing offenses against computer users. The bill also provides for civil remedies including the award of court costs and reasonable attorney's fees to the prevailing party. A civil penalty may be awarded by a court, but the penalty must not exceed $10,000 per violation or $1 million per defendant.

[22] A third-degree felony is punishable by up to five years imprisonment and a $5,000 fine. Sections 775.082, 775.083, and 775.084, F.S.
[23] A second-degree felony is punishable by up to 15 years imprisonment and a $10,000 fine. Sections 775.082, 775.083, and 775.084, F.S.

Pursuant to the Florida Rules of Civil Procedure, if a party requests a temporary injunction, the court has the discretion to require the posting of a bond.[24] If the department seeks a temporary injunction under the act, the department may be required to post a bond. Additionally, if a bond is not required, and the court grants the temporary injunction, but later denies permanent relief, the department may be liable for any resulting damages to the defendant or respondent in the case.

The risk of an award of attorney's fees in the event the department is unsuccessful in pursuing a civil action for injunctive and other relief may deter the department from initiating these actions. Additionally, because the award of attorney's fees is discretionary, in instances where the court does not award attorney's fees, the department must assume all costs of pursuing the civil action. If it is the intent of the Legislature to encourage pursuit of civil actions to enjoin and deter prohibited computer-related actions, it may consider clarifying that an attorney's fee award in favor of the department is mandatory, if the department is successful in pursuing the claim.

Section 6 provides an effective date of July 1, 2009.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Commercial entities may be required to develop programs to solicit consent from computer users to track or monitor information. The cost to commercial entities to develop such programs is indeterminate.

To the extent that commercial entities use malware to track Web surfing habits to enable them to target certain computer users for advertising, this bill may restrict such practices.

[24] Fla. R. Civ. P. 1.610(b).

Should individuals or entities be found in violation of the new crimes created in this bill, they may be subject to civil or criminal penalties.

C. Government Sector Impact:

To the extent that the Department of Legal Affairs or state attorneys enforce the provisions of this law, there will be attendant costs of this enforcement. In addition, the department may be liable for attorney's fees and costs in unsuccessful suits to enjoin unauthorized computer usage under the Florida Computer Crimes Act.

The Criminal Justice Impact Conference analyzed HB 219, which is similar to this bill, and determined that the bill would have an insignificant prison bed impact.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Current law does not address whether an authorized user of a computer, who goes beyond his or her authorization to commit one of the acts under s. 815.06, F.S., should be penalized under the Florida Computer Crimes Act. Federal law, under 18 U.S.C.A. s. 1030(a)(3), specifically outlaws certain acts by an individual who intentionally accesses a computer without authorization or who "exceeds authorized access." In his dissenting opinion in *Gallagher v. State*, Chief Judge Glickstein opined that using a computer "without authorization" has a different meaning from "exceeding authorized access" and that current law under the Florida Computer Crimes Act does not provide a penalty for exceeding authorized access.[25]

This bill prohibits certain uses of computer software without authorization. It is unclear whether the bill will protect consumers from certain software that seeks authorization by burying waiver or consent clauses in lengthy user or license agreements, a common practice.[26]

VIII. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS/CS by Judiciary on March 18, 2009:
The committee substitute:

[25] *Gallagher v. State*, 618 So. 2d 757 (Fla. 4th DCA 1993).
[26] *See* News Release, Federal Trade Commission, *FTC Testifies on Spyware* (June 11, 2008), http://www.ftc.gov/opa/2008/06/spyware.shtm (last visited March 9, 2009); Corey Nachreiner, *Foundations: How Does Spyware Get onto My Computer?*, http://www.watchguard.com/infocenter/editorial/19743.asp (last visited March 9, 2009); and Larry Greenemeier, *Microsoft's WGA Woes Highlight User Rights* (June 13, 2006), http://www.informationweek.com/news/windows/microsoft_news/showArticle.jhtml?articleID=190303180 (last visited March 9, 2009).

- Substitutes the defined word "personally identifiable information" for specified types of personal information in the provision governing deceptive collection of personal information;
- Reorganizes the exemption section of the bill and clarifies that the denoted exceptions apply to violations of ss. 815.051 and 815.053, F.S.; and
- Removes from the bill the provision specifying that the criminal and civil penalties afforded in s. 815.06, F.S., do not preclude a private cause of action for damages.

CS by Commerce on March 3, 2009:
This committee substitute replaces the prohibition of unauthorized use of "spyware," as defined in the bill, with a detailed prohibition of activity commonly associated with the unauthorized use of malware or other similar software. In addition, it:

- Exempts monitoring of and interaction with certain service providers (telecommunications carrier, cable operator, computer hardware or software provider, information service provider, or interactive computer service) providing maintenance or repair, technical support, network management, computer security, remote system management, and fraud detection services;
- Exempts certain providers (communication service providers, commercial mobile service providers, and information service providers) when they provide transmission, storage, or caching of communications;
- Exempts software used by parents or guardians to monitor Internet activity of their minor children;
- Includes any of the prohibited acts listed in the CS as offenses against computer users, bringing persons who commit those acts within the ambit of penalties provided for those offenses;
- Expressly authorizes the Department of Legal Affairs or a state attorney to file civil actions to enjoin the prohibited acts;
- Provides civil remedies and penalties, including the potential award of court costs and attorney's fees to the prevailing party and up to $10,000 per violation, but not to exceed $1 million in penalties per defendant; and
- Clarifies that a private litigant is not prohibited from filing a civil action for damages incurred as a result of prohibited conduct under the CS.

B. Amendments:

None.