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 Commerce Committee

BILL:	CS/SB 164
INTRODUCER:	Commerce Committee and Senator Ring
SUBJECT:	Offenses against computer users
DATE:	February 20, 2009 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	O'Callaghan	Cooper	CM	**Fav/CS**
2.			JU	
3.			JA	
4.				
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 Florida Computer Crimes Act, enacted in 1978, provides computer users protection from computer contaminants by making illegal certain unauthorized uses of computers.[1]

This committee substitute (CS) expands computer users' protections under the act by prohibiting certain unauthorized acts. The CS provides that a person may not deceptively, 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 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;

[1] See s. 815.08, F.S.

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

This CS also makes any of the above-listed actions an offense against computer users, thus making a person, who commits any of the above-listed actions, subject to any penalties existing in current law.

This CS provides exceptions 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.

This CS provides specific authority for the Department of Legal Affairs or a state attorney to seek civil remedies and penalties on behalf of people of the state and clarifies that private litigants may file civil actions for damages arising under the CS.

This CS creates sections 815.051, 815.053, and 815.055, and substantially amends sections 815.03 and 815.06 of the Florida Statutes.

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.[2] This widespread corruption in 2007 cost victims a total of $239.09 million, with a median dollar loss of $680.00 per complaint.[3]

Technology used by criminals often outpaces technology used to prevent or protect against Internet criminal activity.[4] The technology used, often referred to as malware (malicious software) or computer contaminants, includes viruses, Trojan horses, worms, spyware, and adware.[5] Malware is used to monitor other 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 and can also be used to redirect Web browser activity, install additional software on a computer, or change computer settings, resulting in slow connection speeds, slow processing speeds, or altered computer programs.[6]

---

[2] See the 2007 Internet Crime Report prepared by the National White Collar Crime Center, Bureau of Justice Assistance, and Federal Bureau of Investigation, found at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf .
[3] *Id*.
[4] Information available at http://www.infoworld.com/article/08/04/08/Web-users-in-malware-crosshairs_1.html.
[5] Information available at http://en.wikipedia.org/wiki/Malware.
[6] See http://www.onguardonline.gov/topics/spyware.aspx, http://www.onguardonline.gov/topics/malware.aspx, and http://www.microsoft.com/technet/security/alerts/info/malware.mspx.

There are several federal laws designed to prevent or impede computer users from committing crimes.[7] The Computer Fraud and Abuse Act (CFAA) is the most frequently used federal law for prosecuting various computer crimes.[8] 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.[9] 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.[10] 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.[11]

Florida was the first state to respond to computer crime by enacting legislation in 1978, called the Florida Computer Crimes Act, which criminalized certain uses of computers.[12] Since 1978, every state except Vermont has enacted legislation relating to unauthorized access or unauthorized alteration of computers.[13] Under Florida's Computer Crimes 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
- introduces any computer contaminant into any computer, computer system, or computer network.

"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."

Under the act, if a person commits one of the above-listed crimes and causes damage of $5,000 or greater; 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 under s. 815.06, F.S.

---

[7] 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.
[8] See 18 U.S.C. §1030 and http://www.sans.org/reading_room/whitepapers/legal/federal_computer_crime_laws_1446?show=1446.php&cat=legal.
[9] "Protected computer" under 18 U.S.C. §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.
[10] See 18 U.S.C. §1030.
[11] See 18 U.S.C. §1030 and http://www.sans.org/reading_room/whitepapers/legal/federal_computer_crime_laws_1446?show=1446.php&cat=legal.
[12] Information available at http://phrack.org/issues.html?issue=22&id=7&mode=txt.
[13] Information available at http://www.ncsl.org/programs/lis/CIP/compcrime-subs.htm.

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA), ch. 501, part II, F.S., 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. The act 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 the FUDTPA subjects the violator to a civil penalty of not more than $10,000 for each violation.

The use of malware may also be a violation of Florida's Wiretap Act, under ch. 934, F.S. For example, Florida's Fifth District Court of Appeals 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 Florida's wiretap act.[14] The court held in *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. 5th DCA 2005), that a wife's use of spyware to monitor her husband's intimate communications with another woman was illegal under s. 934.03(1), F.S. Florida's wiretap 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.

III. Effect of Proposed Changes:

Section 1 amends s. 815.03, F.S., to define several terms 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 deceptively, 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 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 or operator's efforts to block or disable computer software by making certain misrepresentations and using specific strategies.

[14] *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. 5th DCA 2005).

Section 3 creates s. 815.053, F.S., to prohibit a person who is not an owner or operator of a computer from committing other certain acts. Prohibited acts include 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 or use 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 chapter.

Section 4 creates 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 or operator's computer to provide security, technical support, maintenance, repair or other specified services. This section also specifies that no liability 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 and specifies that parents or guardians are not prohibited from using software to monitor their children's computer usage.

Subsection (2) clarifies that the section does not provide a defense to any liability arising under the common law, any state law, or any federal law, and does not grant authority to engage in any action listed in the section.

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, subjecting that person to any penalties provided for under this section.

Subsection (4) is created to provide specific authority for the Department of Legal Affairs 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. This subsection also provides for civil remedies including the award of court costs and reasonable attorney's fees to the prevailing party. Damages awarded by a court may not exceed $10,000 per violation or $1 million per defendant.

Subsection (9) is created to clarify that a private litigant is not prohibited from filing a civil action for any damages arising under this section.

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 have 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 CS may restrict such practices.

Should individuals or entities be found in violation of this law, they may be subject to financial 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. At this time, there has been no official estimate of the impact this law will have on the prison population.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Current law does not address whether an authorized user of a computer, who goes beyond their authorization to commit one of the acts under s. 815.06, F.S., should be penalized under the act. Federal law under 18 U.S.C.A. §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*, 618 So. 2d 757 (Fla. 4th DCA 1993), 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.

This CS prohibits certain uses of computer software without authorization. It is unclear as to whether the CS will protect consumers from certain software that seeks authorization by burying waiver or consent clauses in lengthy user or license agreements, a common practice.[15]

VIII. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

This CS 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 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.

[15] See http://www.ftc.gov/opa/2008/06/spyware.shtm, http://www.watchguard.com/infocenter/editorial/19743.asp, and http://www.informationweek.com/news/windows/microsoft_news/showArticle.jhtml?articleID=190303180.