THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 711　　Session of 2007

INTRODUCED BY GORDNER, WONDERLING, ARMSTRONG, BOSCOLA, BRUBAKER,
CORMAN, COSTA, ERICKSON, FERLO, FOLMER, FONTANA, KASUNIC,
LAVALLE, LOGAN, O'PAKE, ORIE, PIPPY, RAFFERTY, STACK,
TARTAGLIONE, VANCE, WASHINGTON, WAUGH, C. WILLIAMS, WOZNIAK,
GREENLEAF, D. WHITE AND EARLL, APRIL 30, 2007

SENATOR ARMSTRONG, APPROPRIATIONS, RE-REPORTED AS AMENDED,
DECEMBER 3, 2007

AN ACT

1　Providing for the protection of consumers from having spyware
2　　deceptively installed on their computers and for criminal and
3　　civil enforcement.

16　　　The General Assembly of the Commonwealth of Pennsylvania

1 hereby enacts as follows:

2 Section 1. Short title.

3   This act shall be known and may be cited as the Consumer

4 Protection Against Computer Spyware Act.

5 Section 2. Definitions.

6   The following words and phrases when used in this act shall

7 have the meanings given to them in this section unless the

8 context clearly indicates otherwise:

9   "Authorized user." With respect to a computer, a person who

10 owns or is authorized by the owner or lessee to use the

11 computer.

12   "Cause to be copied." To distribute, transfer or procure the

13 copying of computer software or any component thereof. The term

14 shall not include the following:

15   (1) Transmission, routing, provision of intermediate

16   temporary storage or caching of software.

17   (2) A storage or hosting medium, such as a compact disc,

18   Internet website or computer server, through which the

19   software was distributed by a third party.

20   (3) An information location tool, such as a directory,

21   index, reference, pointer or hypertext link, through which

22   the user of the computer located the software.

23   "Communications provider." Entity providing communications

24 networks or services that enable consumers to access the

25 Internet or destinations on the public switched telephone

26 network via a computer modem. This term shall include cable

27 service providers that also provide telephone services and

28 providers of Voice over Internet Protocol services.

29   "Computer software." A sequence of instructions written in

30 any programming language that is executed on a computer. The

1 term shall not include a text or data file, an Internet website

2 or a data component of an Internet website that is not

3 executable independently of the Internet website.

4   "Computer virus." A computer program or other set of

5 instructions that is designed to degrade the performance of or

6 disable a computer, computer network or computer software and is

7 designed to have the ability to replicate itself on other

8 computers or computer networks without the authorization of the

9 owners of those computers or computer networks.

10   "Damage." Any material impairment to the integrity,

11 functionality or availability of data, software, a computer, a

12 system or information.

13   "Deceptive" or "deception." Includes, but is not limited to:

14   (1) An intentionally and materially false or fraudulent

15   statement.

16   (2) A statement or description that intentionally omits

17   or misrepresents material information in order to deceive the

18   authorized user.

19   (3) An intentional and material failure to provide any

20   notice to an authorized user regarding the download or

21   installation of software in order to deceive the authorized

22   user.

23   "Execute." With respect to computer software, the

24 performance of the functions or the carrying out of the

25 instructions of the computer software.

26   "Internet." The global information system that is logically

27 linked together by a globally unique address space based on the

28 Internet Protocol (IP), or its subsequent extensions, and that

29 is able to support communications using the Transmission Control

30 Protocol/Internet Protocol (TCP/IP) suite, or its subsequent

1 extensions, or other IP-compatible protocols, and that provides,

2 uses or makes accessible, either publicly or privately, high-

3 level services layered on the communications and related

4 infrastructure described in this act.

5   "Message." A graphical or text communication presented to an

6 authorized user of a computer other than communications

7 originated and sent by the computer's operating system or

8 communications presented for any of the purposes described in

9 section 6.

10   "Person." Any individual, partnership, corporation, limited

11 liability company or other organization, or any combination

12 thereof.

13   "Personally identifiable information." The term shall

14 include any of the following:

15   (1) First name or first initial in combination with last

16   name.

17   (2) Credit or debit card numbers or other financial

18   account numbers.

19   (3) A password or personal identification number

20   required to access an identified financial account other than

21   a password, personal identification number or other

22   identification number transmitted by an authorized user to

23   the issuer of the account or its agent.

24   (4) Social Security number.

25   (5) Any of the following information in a form that

26   personally identifies an authorized user:

27   (i) Account balances.

28   (ii) Overdraft history.

29   (iii) Payment history.

30   (iv) A history of Internet websites visited.

1   (v) Home address.

2   (vi) Work address.

3   (vii) A record of a purchase or purchases.

4   "Procure the copying." To pay or provide other consideration

5 to, or induce another person to cause software to be copied onto

6 a computer.

7 Section 3. Computer spyware prohibitions.

8   A person or entity that is not an authorized user shall not,

9 with actual knowledge, with conscious avoidance of actual

10 knowledge, or willfully, cause computer software to be copied or

11 procure the copying onto the computer of an authorized user in

12 this Commonwealth and use the software to do any of the

13 following acts or any other acts deemed to be deceptive:

14   (1) Modify through deceptive means any of the following

15   settings related to the computer's access to or use of the

16   Internet:

17   (i) The page that appears when an authorized user

18   launches an Internet browser or similar software program

19   used to access and navigate the Internet.

20   (ii) The default provider or Internet website proxy

21   the authorized user uses to access or search the

22   Internet.

23   (iii) The authorized user's list of bookmarks used

24   to access Internet website pages.

25   (2) Collect through deceptive means personally

26   identifiable information that meets any of the following

27   criteria:

28   (i) It is collected through the use of a keystroke-

29   logging function that records all keystrokes made by an

30   authorized user who uses the computer and transfers that

1   information from the computer to another person.

2   (ii) It includes all or substantially all of the

3   Internet websites visited by an authorized user, other

4   than Internet websites of the provider of the software,

5   if the computer software was installed in a manner

6   designed to conceal from all authorized users of the

7   computer the fact that the software is being installed.

8   (iii) It is a data element described in paragraph

9   (2), (3), (4) or (5)(i) or (ii) of the definition of

10   "personally identifiable information" that is extracted

11   from the authorized user's computer hard drive for a

12   purpose wholly unrelated to any of the purposes of the

13   software or service described to an authorized user.

14   (3) Prevent, without the authorization of an authorized

15   user, through deceptive means an authorized user's reasonable

16   efforts to block the installation of or to disable software

17   by causing software that the authorized user has properly

18   removed or disabled to automatically reinstall or reactivate

19   on the computer without the authorization of an authorized

20   user.

21   (4) Misrepresent that software will be uninstalled or

22   disabled by an authorized user's action with knowledge that

23   the software will not be so uninstalled or disabled.

24   (5) Through deceptive means, remove, disable or render

25   inoperative security, antispyware or antivirus software

26   installed on the computer.

27 Section 4. Control or modification.

28   A person or entity that is not an authorized user shall not,

29 with actual knowledge, with conscious avoidance of actual

30 knowledge, or willfully, cause computer software to be copied or

1 procure the copying onto the computer of an authorized user in

2 this Commonwealth and use the software to do any of the

3 following acts or any other acts deemed to be deceptive:

4   (1) Take control of the authorized user's computer by

5   doing any of the following:

6   (i) Transmitting or relaying commercial electronic

7   mail or a computer virus from the authorized user's

8   computer, where the transmission or relaying is initiated

9   by a person other than the authorized user and without

10   the authorization of an authorized user.

11   (ii) Accessing or using the authorized user's modem

12   or Internet service for the purpose of causing damage to

13   the authorized user's computer or of causing an

14   authorized user to incur financial charges for a service

15   that is not authorized by an authorized user.

16   (iii) Using the authorized user's computer as part

17   of an activity performed by a group of computers for the

18   purpose of causing damage to another computer, including,

19   but not limited to, launching a denial of service attack.

20   (iv) Opening a series of stand-alone messages in the

21   authorized user's computer without the authorization of

22   an authorized user and with knowledge that a reasonable

23   computer user cannot close the advertisements without

24   turning off the computer or closing the Internet

25   application.

26   (2) Modify any of the following settings related to the

27   computer's access to or use of the Internet:

28   (i) An authorized user's security or other settings

29   that protect information about the authorized user for

30   the purpose of stealing personal information of an

1   authorized user.

2   (ii) The security settings of the computer for the

3   purpose of causing damage to one or more computers.

4   (3) Prevent, without the authorization of an authorized

5   user, an authorized user's reasonable efforts to block the

6   installation of or to disable software by doing any of the

7   following:

8   (i) Presenting the authorized user with an option to

9   decline installation of software with knowledge that,

10   when the option is selected by the authorized user, the

11   installation nevertheless proceeds.

12   (ii) Falsely representing that software has been

13   disabled.

14   (iii) Requiring in a deceptive manner the user to

15   access the Internet to remove the software with knowledge

16   or reckless disregard of the fact that the software

17   frequently operates in a manner that prevents the user

18   from accessing the Internet.

19   (iv) Changing the name, location or other

20   designation information of the software for the purpose

21   of preventing an authorized user from locating the

22   software to remove it.

23   (v) Using randomized or deceptive file names,

24   directory folders, formats or registry entries for the

25   purpose of avoiding detection and removal of the software

26   by an authorized user.

27   (vi) Causing the installation of software in a

28   particular computer directory or computer memory for the

29   purpose of evading authorized users' attempts to remove

30   the software from the computer.

1   (vii) Requiring, without the authority of the owner

2   of the computer, that an authorized user obtain a special

3   code or download software from a third party to uninstall

4   the software.

5   Section 5. Misrepresentation and deception.

6   A person or entity who is not an authorized user shall not do

7   any of the following or any other misrepresenting and deceptive

8   acts with regard to the computer of an authorized user in this

9   Commonwealth:

10   (1) Induce an authorized user to install a software

11   component onto the computer by misrepresenting that

12   installing software is necessary for security or privacy

13   reasons or in order to open, view or play a particular type

14   of content.

15   (2) Causing the copying and execution on the computer of

16   a computer software component with the intent of causing an

17   authorized user to use the component in a way that violates

18   any other provision of this section.

19   Section 6. Nonapplicability.

20   (1) Nothing in section 4 or 5 shall apply to any

21   monitoring of or interaction with a user's Internet or other

22   network connection or service, or a protected computer, by a

23   cable operator, computer hardware or software provider or

24   provider of information service or interactive computer

25   service for network or computer security purposes,

26   diagnostics, technical support, repair, authorized updates of

27   software or system firmware, network management or

28   maintenance, authorized remote system management or detection

29   or prevention of the unauthorized use of or fraudulent or

30   other illegal activities in connection with a network,

1   service or computer software, including scanning for and

2   removing software proscribed under this act.

3   (2)   Nothing in this act shall limit the rights of

4   providers of wire and electronic communications under 18

5   U.S.C. § 2511 (relating to interception and disclosure of

6   wire, oral, or electronic communications prohibited).

7 Section 7. Criminal enforcement.

8   (a) District attorneys.--The district attorneys of the

9 several counties shall have authority to investigate and to

10 institute criminal proceedings for any violations of this act.

11   (b) Attorney General.--In addition to the authority

12 conferred upon the Attorney General under the act of October 15,

13 1980 (P.L.950, No.164), known as the Commonwealth Attorneys Act,

14 the Attorney General shall have the authority to investigate and

15 institute criminal proceedings for any violation of this act. A

16 person charged with a violation of this act by the Attorney

17 General shall not have standing to challenge the authority of

18 the Attorney General to investigate or prosecute the case, and,

19 if any such challenge is made, the challenge shall be dismissed

20 and no relief shall be available in the courts of this

21 Commonwealth to the person making the challenge.

22   (c) Proceedings against persons outside Commonwealth.--In

23 addition to powers conferred upon district attorneys and the

24 Attorney General in subsections (a) and (b), district attorneys

25 and the Attorney General shall have the authority to investigate

26 and initiate criminal proceedings against persons for violations

27 of this act in accordance with 18 Pa.C.S. § 102 (relating to

28 territorial applicability).

29 Section 8. Penalty.

30   Any person that violates the provisions of sections 3(2) and

1 4(1)(i), (ii) and (iii) and (2) commits a felony of the second

2 degree and shall, upon conviction, be sentenced to imprisonment

3 for not less than one nor more than ten years or to pay a fine,

4 notwithstanding 18 Pa.C.S. § 1101 (relating to fines), of not

5 more than $25,000, or both.

6 Section 9. Civil relief.

7   (a) General rule.--~~Subject to the limitation set forth in~~   <—

8 ~~subsection (g), the~~ THE following persons may bring a civil   <—

9 action against a person who violates this act:

10   (1) A provider of computer software who is adversely

11   affected by the violation.

12   (2) An Internet Service Provider who is adversely

13   affected by the violation.

14   (3) A trademark owner whose trademark is used without

15   the authorization of the owner to deceive users in the course

16   of any of the deceptive practices prohibited by this section.

17   ~~(4) The Attorney General.~~   <—

18   (b) Additional remedies.--In addition to any other remedy

19 provided by law, a permitted person bringing an action under

20 this section may:

21   (1) Seek injunctive relief to restrain the violator from

22   continuing the violation.

23   (2) Recover damages in an amount equal to the greater

24   of:

25   (i) Actual damages arising from the violation.

26   (ii) Up to $100,000 for each violation, as the court

27   considers just.

28   (3) Seek both injunctive relief and recovery of damages

29   as provided by this subsection.

30   (c) Increase by court.--The court may increase an award of

1 actual damages in an action brought under this section to an

2 amount not to exceed three times the actual damages sustained if

3 the court finds that the violations have occurred with a

4 frequency with respect to a group of victims as to constitute a

5 pattern or practice.

6   (d) Fees and costs.--A plaintiff who prevails in an action

7 filed under this section is entitled to recover reasonable

8 attorney fees and court costs.

9   (e) Communications provider relief.--In the case of a

10 violation of section 4(1)(ii) that causes a communications

11 provider to incur costs for the origination, transport or

12 termination of a call triggered using the modem of a customer of

13 the communications provider as a result of a violation, the

14 communications provider may bring a civil action against the

15 violator to recover any or all of the following:

16   (1) The charges the carrier is obligated to pay to

17   another carrier or to an information service provider as a

18   result of the violation, including, but not limited to,

19   charges for the origination, transport or termination of the

20   call.

21   (2) Costs of handling customer inquiries or complaints

22   with respect to amounts billed for calls.

23   (3) Costs and a reasonable attorney fee.

24   (4) An order to enjoin the violation.

25   (f) Multiple violations.--For purposes of a civil action

26 under this section, any single action or conduct that violates

27 more than one paragraph of this act shall be considered multiple

28 violations based on the number of such paragraphs violated.

29   (g) Unfair trade practice. A violation of this act shall be <--

30 deemed to be an unfair or deceptive act or practice in violation

1 ~~of the act of December 17, 1968 (P.L.1224, No.387), known as the~~

2 ~~Unfair Trade Practices and Consumer Protection Law. The Office~~

3 ~~of Attorney General shall have exclusive authority to bring an~~

4 ~~action under the Unfair Trade Practices and Consumer Protection~~

5 ~~Law for a violation of that act.~~

6 SECTION 19. CONSTRUCTION.   <——

7   THE PROVISIONS OF THIS ACT SHALL NOT LIMIT THE JURISDICTION

8 AND AUTHORITY OF THE OFFICE OF ATTORNEY GENERAL, INCLUDING, BUT

9 NOT LIMITED TO, THE JURISDICTION AND AUTHORITY GRANTED PURSUANT

10 TO THE ACT OF OCTOBER 15, 1980 (P.L.950, NO.164), KNOWN AS THE

11 COMMONWEALTH ATTORNEYS ACT, AND THE ACT OF DECEMBER 17, 1968

12 (P.L.1224, NO.387), KNOWN AS THE UNFAIR TRADE PRACTICES AND

13 CONSUMER PROTECTION LAW.

14 Section ~~10~~ 20. Effective date.   <——

15   This act shall take effect in 60 days.