

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 123 Session of 2009

INTRODUCED BY GORDNER, WOZNIAK, ERICKSON, LEACH, ALLOWAY, BOSCOLA, CORMAN, COSTA, EARLL, FERLO, KASUNIC, KITCHEN, LOGAN, O'PAKE, ORIE, RAFFERTY, SMUCKER, STOUT, TARTAGLIONE, VANCE, WAUGH, D. WHITE, WILLIAMS, STACK, WONDERLING, BRUBAKER AND WASHINGTON, JANUARY 30, 2009

AS AMENDED ON SECOND CONSIDERATION, APRIL 20, 2009

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.

TABLE OF CONTENTS

- 4 Section 1. Short title.
5 Section 2. Definitions.
6 Section 3. Computer spyware prohibitions.
7 Section 4. Control or modification.
8 Section 5. Misrepresentation and deception.
9 Section 6. Nonapplicability.
10 Section 7. Criminal enforcement.
11 Section 8. Penalty.
12 Section 9. Civil relief.
13 Section 19. Construction.
14 Section 20. Effective date.

16 The General Assembly of the Commonwealth of Pennsylvania
17 hereby enacts as follows:

1 Section 1. Short title.

2 This act shall be known and may be cited as the Consumer
3 Protection Against Computer Spyware Act.

4 Section 2. Definitions.

5 The following words and phrases when used in this act shall
6 have the meanings given to them in this section unless the
7 context clearly indicates otherwise:

8 "Authorized user." With respect to a computer, a person who
9 owns or is authorized by the owner or lessee to use the
10 computer.

11 "Cause to be copied." To distribute, transfer or procure the
12 copying of computer software or any component thereof. The term
13 shall not include the following:

14 (1) Transmission, routing, provision of intermediate
15 temporary storage or caching of software.

16 (2) A storage or hosting medium, such as a compact disc,
17 Internet website or computer server, through which the
18 software was distributed by a third party.

19 (3) An information location tool, such as a directory,
20 index, reference, pointer or hypertext link, through which
21 the user of the computer located the software.

22 "Communications provider." Entity providing communications
23 networks or services that enable consumers to access the
24 Internet or destinations on the public switched telephone
25 network via a computer modem. This term shall include cable
26 service providers that also provide telephone services and
27 providers of Voice over Internet Protocol services.

28 "Computer software." A sequence of instructions written in
29 any programming language that is executed on a computer. The
30 term shall not include a text or data file, an Internet website

1 or a data component of an Internet website that is not
2 executable independently of the Internet website.

3 "Computer virus." A computer program or other set of
4 instructions that is designed to degrade the performance of or
5 disable a computer, computer network or computer software and is
6 designed to have the ability to replicate itself on other
7 computers or computer networks without the authorization of the
8 owners of those computers or computer networks.

9 "Damage." Any material impairment to the integrity,
10 functionality or availability of data, software, a computer, a
11 system or information.

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

13 (1) An intentionally and materially false or fraudulent
14 statement.

15 (2) A statement or description that intentionally omits
16 or misrepresents material information in order to deceive the
17 authorized user.

18 (3) An intentional and material failure to provide any
19 notice to an authorized user regarding the download or
20 installation of software in order to deceive the authorized
21 user.

22 "Execute." With respect to computer software, the
23 performance of the functions or the carrying out of the
24 instructions of the computer software.

25 "Internet." The global information system that is logically
26 linked together by a globally unique address space based on the
27 Internet Protocol (IP), or its subsequent extensions, and that
28 is able to support communications using the Transmission Control
29 Protocol/Internet Protocol (TCP/IP) suite, or its subsequent
30 extensions, or other IP-compatible protocols, and that provides,

1 uses or makes accessible, either publicly or privately, high-
2 level services layered on the communications and related
3 infrastructure described in this act.

4 "Message." A graphical or text communication presented to an
5 authorized user of a computer other than communications
6 originated and sent by the computer's operating system or
7 communications presented for any of the purposes described in
8 section 6.

9 "Person." Any individual, partnership, corporation, limited
10 liability company or other organization, or any combination
11 thereof.

12 "Personally identifiable information." The term shall
13 include any of the following:

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

16 (2) Credit or debit card numbers or other financial
17 account numbers.

18 (3) A password or personal identification number
19 required to access an identified financial account other than
20 a password, personal identification number or other
21 identification number transmitted by an authorized user to
22 the issuer of the account or its agent.

23 (4) Social Security number.

24 (5) Any of the following information in a form that
25 personally identifies an authorized user:

26 (i) Account balances.

27 (ii) Overdraft history.

28 (iii) Payment history.

29 (iv) A history of Internet websites visited.

30 (v) Home address.

1 (vi) Work address.

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

3 "Procure the copying." To pay, provide other consideration
4 to or induce another person to cause software to be copied onto
5 a computer.

6 Section 3. Computer spyware prohibitions.

7 A person or entity that is not an authorized user shall not,
8 with actual knowledge with conscious avoidance of actual
9 knowledge or willfully, cause computer software to be copied or
10 procure the copying onto the computer of an authorized user in
11 this Commonwealth and use the software to do any of the
12 following acts or any other acts deemed to be deceptive:

13 (1) Modify through deceptive means any of the following
14 settings related to the computer's access to or use of the
15 Internet:

16 (i) The page that appears when an authorized user
17 launches an Internet browser or similar software program
18 used to access and navigate the Internet.

19 (ii) The default provider or Internet website proxy
20 the authorized user uses to access or search the
21 Internet.

22 (iii) The authorized user's list of bookmarks used
23 to access Internet website pages.

24 (2) Collect through deceptive means personally
25 identifiable information that meets any of the following
26 criteria:

27 (i) It is collected through the use of a keystroke-
28 logging function that records all keystrokes made by an
29 authorized user who uses the computer and transfers that
30 information from the computer to another person.

1 (ii) It includes all or substantially all of the
2 Internet websites visited by an authorized user, other
3 than Internet websites of the provider of the software,
4 if the computer software was installed in a manner
5 designed to conceal from all authorized users of the
6 computer the fact that the software is being installed.

7 (iii) It is a data element described in paragraph
8 (2), (3), (4) or (5)(i) or (ii) of the definition of
9 "personally identifiable information" that is extracted
10 from the authorized user's computer hard drive for a
11 purpose wholly unrelated to any of the purposes of the
12 software or service described to an authorized user.

13 (3) Prevent, without the authorization of an authorized
14 user, through deceptive means an authorized user's reasonable
15 efforts to block the installation of or to disable software
16 by causing software that the authorized user has properly
17 removed or disabled to automatically reinstall or reactivate
18 on the computer without the authorization of an authorized
19 user.

20 (4) Misrepresent that software will be uninstalled or
21 disabled by an authorized user's action with knowledge that
22 the software will not be so uninstalled or disabled.

23 (5) Through deceptive means, remove, disable or render
24 inoperative security, antispyware or antivirus software
25 installed on the computer.

26 Section 4. Control or modification.

27 A person or entity that is not an authorized user shall not,
28 with actual knowledge, with conscious avoidance of actual
29 knowledge or willfully, cause computer software to be copied or
30 procure the copying onto the computer of an authorized user in

1 this Commonwealth and use the software to do any of the
2 following acts or any other acts deemed to be deceptive:

3 (1) Take control of the authorized user's computer by
4 doing any of the following:

5 (i) Transmitting or relaying commercial electronic
6 mail or a computer virus from the authorized user's
7 computer, where the transmission or relaying is initiated
8 by a person other than the authorized user and without
9 the authorization of an authorized user.

10 (ii) Accessing or using the authorized user's modem
11 or Internet service for the purpose of causing damage to
12 the authorized user's computer or of causing an
13 authorized user to incur financial charges for a service
14 that is not authorized by an authorized user.

15 (iii) Using the authorized user's computer as part
16 of an activity performed by a group of computers for the
17 purpose of causing damage to another computer, including,
18 but not limited to, launching a denial of service attack.

19 (iv) Opening a series of stand-alone messages in the
20 authorized user's computer without the authorization of
21 an authorized user and with knowledge that a reasonable
22 computer user cannot close the advertisements without
23 turning off the computer or closing the Internet
24 application.

25 (2) Modify any of the following settings related to the
26 computer's access to or use of the Internet:

27 (i) An authorized user's security or other settings
28 that protect information about the authorized user for
29 the purpose of stealing personal information of an
30 authorized user.

1 (ii) The security settings of the computer for the
2 purpose of causing damage to one or more computers.

3 (3) Prevent, without the authorization of an authorized
4 user, an authorized user's reasonable efforts to block the
5 installation of or to disable software by doing any of the
6 following:

7 (i) Presenting the authorized user with an option to
8 decline installation of software with knowledge that,
9 when the option is selected by the authorized user, the
10 installation nevertheless proceeds.

11 (ii) Falsely representing that software has been
12 disabled.

13 (iii) Requiring, in a deceptive manner, the user to
14 access the Internet to remove the software with knowledge
15 or reckless disregard of the fact that the software
16 frequently operates in a manner that prevents the user
17 from accessing the Internet.

18 (iv) Changing the name, location or other
19 designation information of the software for the purpose
20 of preventing an authorized user from locating the
21 software to remove it.

22 (v) Using randomized or deceptive file names,
23 directory folders, formats or registry entries for the
24 purpose of avoiding detection and removal of the software
25 by an authorized user.

26 (vi) Causing the installation of software in a
27 particular computer directory or computer memory for the
28 purpose of evading authorized users' attempts to remove
29 the software from the computer.

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

1 of the computer, that an authorized user obtain a special
2 code or download software from a third party to uninstall
3 the software.

4 Section 5. Misrepresentation and deception.

5 A person or entity who is not an authorized user shall not do
6 any of the following or any other misrepresenting and deceptive
7 acts with regard to the computer of an authorized user in this
8 Commonwealth:

9 (1) Induce an authorized user to install a software
10 component onto the computer by misrepresenting that
11 installing software is necessary for security or privacy
12 reasons or in order to open, view or play a particular type
13 of content.

14 (2) Causing the copying and execution on the computer of
15 a computer software component with the intent of causing an
16 authorized user to use the component in a way that violates
17 any other provision of this section.

18 Section 6. Nonapplicability.

19 (1) Nothing in section 4 or 5 shall apply to any
20 monitoring of or interaction with a user's Internet or other
21 network connection or service, or a protected computer, by a
22 cable operator, computer hardware or software provider or
23 provider of information service or interactive computer
24 service for network or computer security purposes,
25 diagnostics, technical support, repair, authorized updates of
26 software or system firmware, network management or
27 maintenance, authorized remote system management or detection
28 or prevention of the unauthorized use of or fraudulent or
29 other illegal activities in connection with a network,
30 service or computer software, including scanning for and

1 removing software proscribed under this act.

2 (2) Nothing in this act shall limit the rights of
3 providers of wire and electronic communications under 18
4 U.S.C. § 2511 (relating to interception and disclosure of
5 wire, oral, or electronic communications prohibited).

6 Section 7. Criminal enforcement.

7 (a) District attorneys.--The district attorneys of the
8 several counties shall have authority to investigate and to
9 institute criminal proceedings for any violations of this act.

10 (b) Attorney General.--In addition to the authority
11 conferred upon the Attorney General under the act of October 15,
12 1980 (P.L.950, No.164), known as the Commonwealth Attorneys Act,
13 the Attorney General shall have the authority to investigate and
14 institute criminal proceedings for any violation of this act. A
15 person charged with a violation of this act by the Attorney
16 General shall not have standing to challenge the authority of
17 the Attorney General to investigate or prosecute the case and,
18 if any such challenge is made, the challenge shall be dismissed
19 and no relief shall be available in the courts of this
20 Commonwealth to the person making the challenge.

21 (c) Proceedings against persons outside Commonwealth.--In
22 addition to powers conferred upon district attorneys and the
23 Attorney General in subsections (a) and (b), district attorneys
24 and the Attorney General shall have the authority to investigate
25 and initiate criminal proceedings against persons for violations
26 of this act in accordance with 18 Pa.C.S. § 102 (relating to
27 territorial applicability).

28 Section 8. Penalty.

29 Any person that violates the provisions of sections 3(2) and
30 4(1)(i), (ii) and (iii) and (2) commits a felony of the second

1 degree and shall, upon conviction, be sentenced to imprisonment
2 for not ~~less than one nor~~ more than ten years or to pay a fine,
3 notwithstanding 18 Pa.C.S. § 1101 (relating to fines), of not
4 more than \$25,000, or both.



5 Section 9. Civil relief.

6 (a) General rule.--The following persons may bring a civil
7 action against a person who violates this act:

8 (1) A provider of computer software who is adversely
9 affected by the violation.

10 (2) An Internet Service Provider who is adversely
11 affected by the violation.

12 (3) A trademark owner whose trademark is used without
13 the authorization of the owner to deceive users in the course
14 of any of the deceptive practices prohibited by this section.

15 (b) Additional remedies.--In addition to any other remedy
16 provided by law, a permitted person bringing an action under
17 this section may:

18 (1) Seek injunctive relief to restrain the violator from
19 continuing the violation.

20 (2) Recover damages in an amount equal to the greater
21 of:

22 (i) Actual damages arising from the violation.

23 (ii) Up to \$100,000 for each violation, as the court
24 considers just.

25 (3) Seek both injunctive relief and recovery of damages
26 as provided by this subsection.

27 (c) Increase by court.--The court may increase an award of
28 actual damages in an action brought under this section to an
29 amount not to exceed three times the actual damages sustained if
30 the court finds that the violations have occurred with a

1 frequency with respect to a group of victims as to constitute a
2 pattern or practice.

3 (d) Fees and costs.--A plaintiff who prevails in an action
4 filed under this section is entitled to recover reasonable
5 attorney fees and court costs.

6 (e) Communications provider relief.--In the case of a
7 violation of section 4(1)(ii) that causes a communications
8 provider to incur costs for the origination, transport or
9 termination of a call triggered using the modem of a customer of
10 the communications provider as a result of a violation, the
11 communications provider may bring a civil action against the
12 violator to recover any or all of the following:

13 (1) The charges the carrier is obligated to pay to
14 another carrier or to an information service provider as a
15 result of the violation, including, but not limited to,
16 charges for the origination, transport or termination of the
17 call.

18 (2) Costs of handling customer inquiries or complaints
19 with respect to amounts billed for calls.

20 (3) Costs and a reasonable attorney fee.

21 (4) An order to enjoin the violation.

22 (f) Multiple violations.--For purposes of a civil action
23 under this section, any single action or conduct that violates
24 more than one paragraph of this act shall be considered multiple
25 violations based on the number of such paragraphs violated.

26 Section 19. Construction.

27 The provisions of this act shall not limit the jurisdiction
28 and authority of the Office of Attorney General, including, but
29 not limited to, the jurisdiction and authority granted pursuant
30 to the act of October 15, 1980 (P.L.950, No.164), known as the

1 Commonwealth Attorneys Act, and the act of December 17, 1968
2 (P.L.1224, No.387), known as the Unfair Trade Practices and
3 Consumer Protection Law.

4 Section 20. Effective date.

5 This act shall take effect in 60 days.