

GOVERNOR'S PRESS RELEASE ON SIGNING:

Yes 10-20-09

FOLLOWING WERE PRINTED:

To check for circulating copies, contact New Jersey State Government
Publications at the State Library (609) 278-2640 ext.103 or <mailto:refdesk@njstatelib.org>

REPORTS:

No

HEARINGS:

No

NEWSPAPER ARTICLES:

No

LAW/RWH

P.L. 2009, CHAPTER 142, *approved October 19, 2009*
Assembly, No. 3761

1 AN ACT concerning interception of computer trespasser
2 communications and supplementing Title 2A of New Jersey
3 Statutes.

4

5 **BE IT ENACTED** by the Senate and General Assembly of the State
6 of New Jersey:

7

8 1. a. It shall not be a violation of any provision of P.L.1968,
9 c.409 (C.2A:156A-1 et seq.) for a person acting under color of law
10 to intercept the wire or electronic communications of a suspected
11 computer trespasser transmitted to, through, or from a computer or
12 any other device with Internet capability, if:

13 (1) the owner or operator of the computer or other device
14 authorizes the interception of the computer trespasser's wire or
15 electronic communications on the computer;

16 (2) the person acting under color of law is lawfully engaged in
17 an investigation;

18 (3) the person acting under color of law has reasonable grounds
19 to believe that the contents of the computer trespasser's wire or
20 electronic communications will be relevant to the investigation; and

21 (4) such interception does not acquire communications other
22 than those transmitted to or from the computer trespasser.

23 b. For purposes of this section, "computer trespasser" means a
24 person who accesses a computer or any other device with Internet
25 capability without authorization and thus has no reasonable
26 expectation of privacy in any communication transmitted to,
27 through, or from the computer or other device. The term "computer
28 trespasser" does not include a person known by the owner or
29 operator of the computer or other device with Internet capability to
30 have an existing contractual relationship with the owner or operator
31 of the computer or other device for access to all or part of the
32 computer or other device.

33 c. Any aggrieved person in any trial, hearing, or proceeding in
34 or before any court or other authority of this State may move to
35 suppress the contents of any wire or electronic communication
36 intercepted in accordance with subsection a. of this section, or
37 evidence derived therefrom, on the grounds that the communication
38 was unlawfully intercepted or the interception was not made in
39 conformity with the provisions of this section. The motion shall be
40 made at least 10 days before the trial, hearing, or proceeding unless
41 there was no opportunity to make the motion or the moving party
42 was not aware of the grounds for the motion. Motions by
43 coincidees are to be heard in a single consolidated hearing. The
44 court, upon the filing of such motion by the aggrieved person, shall

1 make available to the aggrieved person or his counsel for inspection
2 such portions of the intercepted communication, or evidence
3 derived therefrom, as the court determines to be in the interests of
4 justice. If the motion is granted, the entire contents of all
5 intercepted wire or electronic communications obtained during or
6 after any interception which is determined to be in violation of this
7 P.L.1968, c.409 (C.2A:156A-1 et seq.) or evidence derived
8 therefrom, shall not be received in evidence in the trial, hearing or
9 proceeding.

10 In addition to any other right to appeal, the State shall have the
11 right to appeal from an order granting a motion to suppress upon
12 certification to the court that the appeal is not taken for purposes of
13 delay. The appeal shall be taken within the time specified by the
14 Rules of Court and shall be diligently prosecuted.

15
16 2. This act shall take effect immediately.

17
18
19 STATEMENT

20
21 This bill authorizes a person acting under color of law to
22 intercept the wire or electronic communications of a suspected
23 computer trespasser transmitted to, through, or from a computer or
24 any other device with Internet capability under certain
25 circumstances. Under the bill, such interception would be
26 authorized if:

27 (1) the owner or operator of the computer or other device
28 authorizes the interception;

29 (2) the person acting under color of law is lawfully engaged in
30 an investigation;

31 (3) the person acting under color of law has reasonable grounds
32 to believe that the contents of the computer trespasser's wire or
33 electronic communications will be relevant to the investigation; and

34 (4) such interception does not acquire communications other
35 than those transmitted to or from the computer trespasser.

36 The bill defines "computer trespasser" as "a person who accesses
37 a computer or any other device with Internet capability without
38 authorization and thus has no reasonable expectation of privacy in
39 any communication transmitted to, through, or from the computer
40 or other device."

41 The bill sets out procedures for persons to challenge the
42 interception. It provides that any aggrieved person in any trial,
43 hearing, or proceeding in or before any court or other authority of
44 this State may move to suppress the contents of any wire or
45 electronic communication intercepted in accordance with the bill, or
46 evidence derived therefrom, on the grounds that the communication
47 was unlawfully intercepted or the interception was not made in
48 conformity with the bill.

A3761

3

1 This bill is part of the Attorney General's initiative concerning
2 Internet safety.

3

4

5

6

7 Authorizes interception of wire or electronic communications of
8 suspected computer trespasser under certain circumstances.

ASSEMBLY JUDICIARY COMMITTEE

STATEMENT TO

ASSEMBLY, No. 3761

STATE OF NEW JERSEY

DATED: FEBRUARY 26, 2009

The Assembly Judiciary Committee reports favorably Assembly Bill No. 3761.

This bill authorizes a person acting under color of law to intercept the wire or electronic communications of a suspected computer trespasser transmitted to, through, or from a computer or any other device with Internet capability under certain circumstances. Under the bill, such interception would be authorized if:

(1) the owner or operator of the computer or other device authorizes the interception;

(2) the person acting under color of law is lawfully engaged in an investigation;

(3) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's wire or electronic communications will be relevant to the investigation; and

(4) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

The bill defines "computer trespasser" as "a person who accesses a computer or any other device with Internet capability without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the computer or other device."

The bill sets out procedures for persons to challenge the interception. It provides that any aggrieved person in any trial, hearing, or proceeding in or before any court or other authority of this State may move to suppress the contents of any wire or electronic communication intercepted in accordance with the bill, or evidence derived therefrom, on the grounds that the communication was unlawfully intercepted or the interception was not made in conformity with the bill.

This bill is part of the Attorney General's initiative concerning Internet safety.

SENATE JUDICIARY COMMITTEE

STATEMENT TO

ASSEMBLY, No. 3761

STATE OF NEW JERSEY

DATED: JUNE 18, 2009

The Senate Judiciary Committee reports favorably Assembly Bill No. 3761.

This bill authorizes a person acting under color of law to intercept the wire or electronic communications of a suspected computer trespasser transmitted to, through, or from a computer or any other device with Internet capability under certain circumstances. Under the bill, such interception would be authorized if:

(1) the owner or operator of the computer or other device authorizes the interception;

(2) the person acting under color of law is lawfully engaged in an investigation;

(3) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's wire or electronic communications will be relevant to the investigation; and

(4) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

The bill in subsection b. of section 1 defines "computer trespasser" as "a person who accesses a computer or any other device with Internet capability without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the computer or other device."

The bill in subsection c. of section 1 sets out procedures for persons to challenge the interception. It provides that any aggrieved person in any trial, hearing, or proceeding in or before any court or other authority of this State may move to suppress the contents of any wire or electronic communication intercepted in accordance with the bill, or evidence derived therefrom, on the grounds that the communication was unlawfully intercepted or the interception was not made in conformity with the bill.

This bill is part of the Attorney General's initiative concerning Internet safety.

This bill is identical to Senate, No. 2697.

SENATE, No. 2697

STATE OF NEW JERSEY
213th LEGISLATURE

INTRODUCED MARCH 9, 2009

Sponsored by:
Senator JAMES BEACH
District 6 (Camden)

SYNOPSIS

Authorizes interception of wire or electronic communications of suspected computer trespasser under certain circumstances.

CURRENT VERSION OF TEXT

As introduced.



S2697 BEACH

2

1 AN ACT concerning interception of computer trespasser
2 communications and supplementing Title 2A of New Jersey
3 Statutes.

4

5 **BE IT ENACTED** by the Senate and General Assembly of the State
6 of New Jersey:

7

8 1. a. It shall not be a violation of any provision of P.L.1968,
9 c.409 (C.2A:156A-1 et seq.) for a person acting under color of law
10 to intercept the wire or electronic communications of a suspected
11 computer trespasser transmitted to, through, or from a computer or
12 any other device with Internet capability, if:

13 (1) the owner or operator of the computer or other device
14 authorizes the interception of the computer trespasser's wire or
15 electronic communications on the computer;

16 (2) the person acting under color of law is lawfully engaged in
17 an investigation;

18 (3) the person acting under color of law has reasonable grounds
19 to believe that the contents of the computer trespasser's wire or
20 electronic communications will be relevant to the investigation; and

21 (4) such interception does not acquire communications other
22 than those transmitted to or from the computer trespasser.

23 b. For purposes of this section, "computer trespasser" means a
24 person who accesses a computer or any other device with Internet
25 capability without authorization and thus has no reasonable
26 expectation of privacy in any communication transmitted to,
27 through, or from the computer or other device. The term "computer
28 trespasser" does not include a person known by the owner or
29 operator of the computer or other device with Internet capability to
30 have an existing contractual relationship with the owner or operator
31 of the computer or other device for access to all or part of the
32 computer or other device.

33 c. Any aggrieved person in any trial, hearing, or proceeding in
34 or before any court or other authority of this State may move to
35 suppress the contents of any wire or electronic communication
36 intercepted in accordance with subsection a. of this section, or
37 evidence derived therefrom, on the grounds that the communication
38 was unlawfully intercepted or the interception was not made in
39 conformity with the provisions of this section. The motion shall be
40 made at least 10 days before the trial, hearing, or proceeding unless
41 there was no opportunity to make the motion or the moving party
42 was not aware of the grounds for the motion. Motions by
43 coindictees are to be heard in a single consolidated hearing. The
44 court, upon the filing of such motion by the aggrieved person, shall
45 make available to the aggrieved person or his counsel for inspection
46 such portions of the intercepted communication, or evidence
47 derived therefrom, as the court determines to be in the interests of
48 justice. If the motion is granted, the entire contents of all

1 intercepted wire or electronic communications obtained during or
2 after any interception which is determined to be in violation of this
3 P.L.1968, c.409 (C.2A:156A-1 et seq.) or evidence derived
4 therefrom, shall not be received in evidence in the trial, hearing or
5 proceeding.

6 In addition to any other right to appeal, the State shall have the
7 right to appeal from an order granting a motion to suppress upon
8 certification to the court that the appeal is not taken for purposes of
9 delay. The appeal shall be taken within the time specified by the
10 Rules of Court and shall be diligently prosecuted.

11

12 2. This act shall take effect immediately.

13

14

15 STATEMENT

16

17 This bill authorizes a person acting under color of law to
18 intercept the wire or electronic communications of a suspected
19 computer trespasser transmitted to, through, or from a computer or
20 any other device with Internet capability under certain
21 circumstances. Under the bill, such interception would be
22 authorized if:

23 (1) the owner or operator of the computer or other device
24 authorizes the interception;

25 (2) the person acting under color of law is lawfully engaged in
26 an investigation;

27 (3) the person acting under color of law has reasonable grounds
28 to believe that the contents of the computer trespasser's wire or
29 electronic communications will be relevant to the investigation; and

30 (4) such interception does not acquire communications other
31 than those transmitted to or from the computer trespasser.

32 The bill defines "computer trespasser" as "a person who accesses
33 a computer or any other device with Internet capability without
34 authorization and thus has no reasonable expectation of privacy in
35 any communication transmitted to, through, or from the computer
36 or other device."

37 The bill sets out procedures for persons to challenge the
38 interception. It provides that any aggrieved person in any trial,
39 hearing, or proceeding in or before any court or other authority of
40 this State may move to suppress the contents of any wire or
41 electronic communication intercepted in accordance with the bill, or
42 evidence derived therefrom, on the grounds that the communication
43 was unlawfully intercepted or the interception was not made in
44 conformity with the bill.

45 This bill is part of the Attorney General's initiative concerning
46 Internet safety.

SENATE JUDICIARY COMMITTEE

STATEMENT TO

SENATE, No. 2697

STATE OF NEW JERSEY

DATED: JUNE 18, 2009

The Senate Judiciary Committee reports favorably Senate Bill No. 2697.

This bill authorizes a person acting under color of law to intercept the wire or electronic communications of a suspected computer trespasser transmitted to, through, or from a computer or any other device with Internet capability under certain circumstances. Under the bill, such interception would be authorized if:

- (1) the owner or operator of the computer or other device authorizes the interception;
- (2) the person acting under color of law is lawfully engaged in an investigation;
- (3) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's wire or electronic communications will be relevant to the investigation; and
- (4) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

The bill in subsection b. of section 1 defines "computer trespasser" as "a person who accesses a computer or any other device with Internet capability without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the computer or other device."

The bill in subsection c. of section 1 sets out procedures for persons to challenge the interception. It provides that any aggrieved person in any trial, hearing, or proceeding in or before any court or other authority of this State may move to suppress the contents of any wire or electronic communication intercepted in accordance with the bill, or evidence derived therefrom, on the grounds that the communication was unlawfully intercepted or the interception was not made in conformity with the bill.

This bill is part of the Attorney General's initiative concerning Internet safety.

This bill is identical to Assembly, No. 3761.



Newsroom

[Event Photos](#)[Features](#)[Press Releases](#)[Featured Videos](#)[Audio Clips](#)[Newsletters](#)[Speeches](#)[Executive Orders](#)[RSS Feeds](#)[Home](#) > [Newsroom](#) > [Press Releases](#) > [2009](#) > [Oct-20-09 Governor Corzine Signs Internet Safety Measures](#)JON S. CORZINE
Governor**For Immediate Release:**
Date: October 20, 2009**For More Information:**
Robert Corrales**Phone:** 609-777-2600

Governor Corzine Signs Internet Safety Measures

TRENTON - Further enhancing the State's aggressive Internet Safety initiatives, Governor Jon S. Corzine today signed two bills that will increase Internet security and aid Internet crime prevention in New Jersey.

"With all of the benefits that evolving technologies provide us, there remains to be unfortunate opportunities that exist for the exploitation of children and adults through the use of the Internet," Governor Corzine said. "These two measures will help to close that door on these dangerous situations and prevent Internet predators from perpetrating these criminal encounters."

According to the National Center for Missing & Exploited Children, approximately one in seven young people online (10 to 17-years-old) were solicited or approached over the Internet.

"The Internet serves as a hub for communication, learning, and socialization, but use of the Internet is not without risk," Attorney General Anne Milgram said. "Sexual solicitation, harassment, bullying, and exposure to violent and inappropriate online content represent consistent threats to the safety of our children. That is why this legislation is so important and why my office has employed an aggressive, multi-pronged approach ranging from criminal and civil investigations to cooperative efforts with networking sites and service providers to education initiatives aimed at teachers, school administrators, parents and students."

The first bill, A-3761 / S-2697, authorizes wire or electronic communications of a suspected computer trespasser to be intercepted under certain circumstances. Authorized circumstances include direct approval from the owner or operator of the computer; the information's relevance to an investigation and if the seizure does not acquire communications other than those transmitted to or from the computer trespasser.

"Online stalkers who target children cannot be treated lightly," said Assemblyman Fred Scalera (D-Essex/Bergen/Passaic). "We need to be able to go after these individuals swiftly and bring the full force of the law to bear."

"This helps give law enforcement the tools they need to better protect children who use the Internet for education and recreation," said Assemblywoman Linda Greenstein (D-Middlesex/Mercer). "No longer will Web sites be the playgrounds of criminals looking to prey on vulnerable children."

"Every parent worries when their child logs onto a computer and enters that new world that has evolved on the Internet," said Assemblyman Matthew Milam (D-Atlantic/Cape May/Cumberland). "It can be a wonderful tool for education and keeping in touch with friends and loved ones, but it can also be a dangerous place. These bills aim to give authorities what they need to keep pace with the criminals."

The second bill, A-3763/S-2702, creates the Computer Crime Prevention Fund through fines imposed on individuals convicted of certain internet crimes. These penalties range from \$250 for a case of a disorderly persons or petty disorderly persons offense to \$2,000 in the case of crime in the first degree.

"Penalizing the people who force us to investigate these nightmarish crimes is sensible public policy that puts the burden on offenders, not taxpayers," said Assemblyman Peter J. Barnes III (D-Middlesex).

"Times and technology have changed and so must our laws," said Assemblywoman Elise Evans (D-Passaic).

Collected fines will be placed in a Computer Crime Prevention Fund located within the Department of the Treasury. The funds can be used by the Department of Law and Public Safety to investigate and raise public awareness of computer crimes.

"Law enforcement needs the tools to keep pace with today's ever-changing technology and ward off predators who lurk behind a computer screen in hopes of preying on children," said Assemblyman Nelson Albano (D-Atlantic/Cape May/Cumberland) "This is a common-sense step forward to help give parents peace of mind that we're doing all we can to protect their children in this technological age."

"Through these measures, we are furthering our commitment to ensuring the safety and well-being of New Jersey's children," said Senator James Beach, (D-Camden). "We are also sending an unmistakably clear message that anyone who intends to harm our youth will be prosecuted to the fullest extent of the law. As parents and grandparents, and as adults, we must protect the children of our State."

Both bills signed by Governor Corzine augment the Internet Safety initiatives implemented by the Department of Law and Public Safety. Through these initiatives:

- The State Police, the Division of Criminal Justice and county prosecutors have arrested and prosecuted more than 200 people for possession or distribution of child pornography, including trading child pornography on peer to peer file sharing networks. The Attorney General has also asked Internet Service Providers to block access to child pornography websites to help prevent the victimization of children.
- The Attorney General's Office, working with social networking sites, has identified convicted sex offenders with profiles on social networking sites. As a result of information derived from this initiative, supervised sex offenders have been arrested for violating their conditions of parole by accessing social networking sites.
- The Attorney General's Office developed a unique Report Abuse icon, which is in use on MyYearbook.com and is being tested by Facebook, that provides a common, easily accessible and recognizable mechanism on social networking website pages that allows users to report offensive content quickly and effectively in a way that facilitates and ensures follow-up by the websites and, when appropriate, results in alerts to law enforcement.
- A Civil investigation into potential violations of the Consumer Fraud Act by a college gossip website which allowed malicious and anonymous postings was launched. The website eventually shut down on its own, while the Attorney General advised all New Jersey colleges and universities to adopt best practices to make cyber-security a priority on their campuses.
- In collaboration with the Department of Education, the Attorney General's Office and the Division of State Police have trained more than 1,000 school teachers and administrators on how best to teach children about Internet safety.

Governor Corzine signed the legislation as part of National Cyber Safety Awareness Month, which was designed to encourage citizens to protect their computers and the nation's critical cyber infrastructure.

###

Get our press releases via RSS at: <feed://nj.gov/governor/news/news/2009/approved/rss.xml>

Photos from Governor Corzine's public events are available at www.nj.gov/governor/news

Video from the Governor's Office is available at www.nj.gov/governor/news/video and www.youtube.com/user/jonscorzine

[Contact Us](#) | [Privacy Notice](#) | [Legal Statement](#) | [Accessibility Statement](#)



Statewide: [NJ Home](#) | [Services A to Z](#) | [Departments/Agencies](#) | [FAQs](#)
Office of the Governor: [Governor Home](#) | [Meet the Governor](#) | [Executive Staff](#) | [Cabinet](#) | [Newsroom](#) | [Boards, Commissions and Authorities](#) | [Photo Blog](#) | [For Kids](#)

Copyright © State of New Jersey, 1996-2010
Office of the Governor
PO Box 001
Trenton, NJ 08625
609-292-6000