

## **The Online Industry’s Model Legislation to Pursue and Control Child Predators**

*Section 1 requires Internet access providers to make available to subscribers a product or service that controls a child’s use of the Internet. Section 2 requires teaching online safety in the classroom. Section 3 increases post-conviction controls on convicted sex offenders. Section 4 requires sex offenders to register their usernames used on interactive online forums. Section 5 requires online services to preserve and disclose customer information pursuant to law enforcement requests. Section 6 expands child porn reporting obligations. Section 7 criminalizes Internet sexual exploitation. Section 8 criminalizes the luring of a child. Section 9 criminalizes age misrepresentation with intent to solicit a child.*

### **Definitions**

1. “Child” means a person who is less than 18 years of age.
2. “Computer network” means the computer network commonly known as the Internet and any other local, regional or global computer network that is similar to or is a predecessor or successor of the Internet.
3. “Internet” means the international computer network of both federal and non-federal interoperable packet switched data networks.<sup>1</sup>
4. “Internet Access Provider” means a provider offering directly to residential customers a facility to access the Internet in exchange for consideration such as through a paid subscription or through an agreement to view specific ads or content. Systems operated or services offered by libraries or educational institutions are excluded from this definition.
5. “Interactive Computer Service” means any information service, system, or access software provider that offers users the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via an Internet Access Provider, including a service or system that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.
6. “Order” means a legal process for the release of information, including but not limited to a court order or search warrant.
7. “Username” means a string of characters used on an Interactive Computer Service to uniquely identify individuals participating in interactive online forums or instant messaging for primarily social purposes.

---

<sup>1</sup> [47 USC § 230](#)

## **Section 1 - Parental Controls**

1. If an Internet access provider knows or has reason to know based upon registration data in its possession that a subscriber currently resides within this state, the provider shall make available to the subscriber a product or service that enables the subscriber to control a child's use of the Internet, provided such product or service is reasonably and commercially available for the technology used by the subscriber to access the Internet. Such product or service shall, in a commercially reasonable manner, enable the subscriber to do at least one of the following:

- (a) Block all access to the internet, or
- (b) Block a child's access to web sites by specifying prohibited web sites or by selecting a category of sites to block, or
- (c) Restrict a child's access exclusively to web sites approved by the subscriber or to select a category of approved web sites, or
- (d) Restrict a child's access to web sites designated by the Internet access provider, or
- (e) Monitor a child's use of the Internet by providing a report to the subscriber indicating specific web sites that the child has attempted to visit but could not access because access to the web sites were blocked or restricted by the subscriber, or
- (f) Monitor a child's use of the Internet by providing a report to the subscriber indicating specific web sites that the child has visited.

2. The Internet access provider shall make available to the subscriber, at or near the time of subscription, a product or service described in subsection 1. The Internet access provider may make such product or service available either directly or through a link to a third-party. The Internet access provider or third-party may charge for such product or service.

## **Section 2 - Internet Safety Curricula<sup>2</sup>**

1. The State Department of Education shall propose to the local school districts in the state, model curricula for educating children regarding online safety, taking into consideration the curricula on this subject developed by the other states (as well as any other curricular materials suggested by education experts, child psychologists, or technology companies who work on child online safety issues, or any other currently available curricula).
2. Each local school district shall incorporate into its curriculum a component on Internet safety to be taught at least once annually to students in grade 3 or above.
3. The State Department of Education shall provide to each school district educational materials for parents and caregivers regarding child online safety.

---

<sup>2</sup> Virginia § 22.1-70.2

### **Section 3 - Online Monitoring of Convicted Sex Offenders<sup>3</sup>**

1. A judge imposing sentence on a person who has been convicted of aggravated sexual assault against a child, sexual assault against a child, aggravated criminal sexual contact against a child, kidnapping of a child, endangering the welfare of a child, luring a minor, possession of Child Pornography or convicted of an attempt to commit any of these offenses may include, in addition to any sentence, a special sentence of supervision as set forth in section 2. The supervision shall be conducted by a probation officer, parole officer, law enforcement officer or assigned computer information technology specialist, in a manner and form prescribed by the Attorney General.

2. Persons serving a special sentence of parole supervision shall be subject to one or more of the provisions and conditions set forth in this subsection including, but not be limited to

(a) Continued supervision, either in person or through remote monitoring, of the person's incoming and outgoing e-mail and other Internet-based communication for evidence relevant to any crime described in paragraph 1.

(b) Continued supervision, either in person or through remote monitoring, of the person's history of websites visited and content accessed for evidence relevant to any crime described in paragraph 1.

(c) Periodic unannounced inspections of the contents of the person's computer or any other device with Internet access, including the retrieval and copying of all data from the computer or device and any internal or external storage or portable media, and removal of such information, computer, device or media to conduct a more thorough inspection for evidence relevant to any crime described in paragraph

3. If the Internet was used by the person in the commission of a crime described in paragraph 1, the judge, as part of the sentence, may limit or restrict the person's Internet access in a manner tailored to prevent further use of the Internet by the person to commit any such crime.

4. A person specially sentenced to supervision may petition the Court for release from that supervision. The judge may grant a petition for release only upon proof by clear and convincing evidence that the person has not committed a crime described in paragraph 1 since the last conviction or release from incarceration, whichever is later, and that the person is not likely to pose a threat to the safety of others if released from parole supervision.

5. A person who refuses to submit to any of the provisions and conditions imposed pursuant to subsection 2 or any Internet access restriction imposed pursuant to subsection 3 shall be guilty of a class 5 felony and shall be sentenced to a term of imprisonment of no less than 5 years, unless the court finds that in that particular case, the interests of justice outweigh the need to deter crimes described in paragraph 1 and that a sentence to imprisonment would be a manifest injustice.

---

<sup>3</sup> New Jersey Assembly Bill 3902

#### **Section 4 - Registration of Online Identifiers**

1. In addition to any other information required pursuant to the state's sex offender registry law, any and all Email addresses and Usernames that the sex offender uses or intends to use shall be provided at the time of registration.
2. If a person required to register pursuant to the state's sex offender registry law fails to provide any and all Email addresses and Usernames that the person uses or intends to use as required by subsection 1, the person shall be subject to the same penalties applicable to the failure to register a residence or a change of residence.
3. The state shall make the Email and Username of registered sex offenders available to the public under the same rules and restrictions set forth in the state's sex offender registry law.

**[OR IN STATES THAT PROHIBIT PUBLIC DISCLOSURE OR COMMERCIAL USE OF THE LIST: —**The state shall make the Email and Username and other information collected from the sex offender registry available through a formal mechanism, to any commercial or non-profit entity, including child safety organizations, educational institutions, and Interactive Computer Service providers for the purpose of protecting children from sex offenders.]

4. No provider of an interactive computer service shall be liable under this Act or any other provision of law:
  - (a) for identifying, removing, disabling, blocking or otherwise affecting a user based on a good faith belief that such user's electronic mail address, Username, or other similar Internet identifier appeared in the National Sex Offender Registry or any analogous State registry; or
  - (b) for failing to identify, block or otherwise prevent a person from registering for its service, or for failing to remove, disable or otherwise affect a registered user, whose electronic mail address, instant message address, or other similar Internet identifier appears in the National Sex Offender Registry or any analogous State registry.

#### **Section 5 - Internet Evidence for Law Enforcement Investigations**

5

1.
  - (a) An Interactive Computer Service, upon the request of a law enforcement agency for an investigation of a possible sex offense involving a child under section \_\_\_\_\_, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of an order or other legal process. The Interactive Computer Service shall comply with the request as soon as reasonably practical following receipt.
  - (b) Records referred to in paragraph (a) of this subsection shall be retained for a period of ninety days, which shall be extended for an additional ninety-day period upon a further request of the law enforcement agency within the initial 90 day period.
2.
  - (a) An Interactive Computer Service shall, as soon as reasonably practical, considering other outstanding law enforcement and legal requests, after receiving appropriate legal

process as set forth in 18 U.S.C. § 2703 relating to an investigation of a possible sex offense involving a child under section \_\_\_\_\_, provide the information that is in its possession and is legally justified pursuant to the means of legal process as set forth in 18 U.S.C. § 2703.

(b) In connection with any criminal investigation of a possible sex offense involving a child under section \_\_\_\_\_, that involves immediate danger of death or serious bodily harm, a law enforcement agency in this state may issue a request, without compulsory legal process or court order, to a designated recipient of the Interactive Computer Service to disclose, consistent with 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), the information identified in paragraph (a) of this subsection. The Interactive Computer Service shall communicate with the requesting agency to discuss the nature of the request and to coordinate an appropriate response immediately and without delay.

3. Subsections (1) and (2) of this section shall be interpreted in a manner consistent with the requirements of federal law that apply to providers of an electronic communications service, including but not limited to 18 U.S.C. ch. 121 (§§ 2701-2712) and 42 U.S.C. § 13032.

#### **Section 6 - Reporting Images of Child Pornography and Other Crimes**

1. An Interactive Computer Service doing business in this state that obtains knowledge of facts or circumstances from which a violation of any law in this state prohibiting possession, distribution or creation of images containing child pornography or prohibiting sexual activity involving a child is apparent, shall make a report, as soon as reasonably possible, of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children consistent with the requirements of 42 U.S.C. § 13032.

#### **Section 7 - Internet sexual exploitation of a child.<sup>4</sup>**

1. A person commits internet sexual exploitation of a child if a person, who is at least four years older than a child who is under fifteen years of age, knowingly requests or encourages the child through communication via the Internet or other computer network to:

(a) Expose or touch the child's own or another person's intimate parts while communicating with the person via a computer network or system; or

(b) Observe the person's intimate parts while communicating with the person via a computer network or system.

2. It shall not be an affirmative defense to this section that the child was actually a law enforcement officer posing as a child under fifteen years of age.

3. Internet sexual exploitation of a child is a class 4 felony.

---

<sup>4</sup> Colorado § [362](#)

### **Section 8 - Internet luring of a child.<sup>5</sup>**

1. A person more than four years older than the child commits internet luring of a child if the person knowingly communicates a statement or an image over a computer or computer network to a child under fifteen years of age, describing or depicting sexual conduct, and, in connection with the communication, makes a statement persuading or inviting the child to meet the person for purposes of criminal sexual conduct.
2. It shall not be an affirmative defense to this section that:
  - (a) A meeting did not occur; or
  - (b) The child was actually a law enforcement officer posing as a child under fifteen years of age.
3. Internet luring of a child is a class 5 felony; except that luring of a child is a class 3 felony if committed with the intent to meet the child for the purpose of engaging in sexual exploitation or sexual contact.
4. For purposes of this section, “in connection with” means communications that further, advance, promote, or have a continuity of purpose and may occur before, during, or after the invitation to meet.

### **Section 9 – Age misrepresentation with intent to solicit a minor.**

1. A person is guilty of age misrepresentation with intent to solicit a minor when he or she is more than four years older than the minor and knowingly misrepresents his or her age with the intent to use the Internet to engage in criminal sexual conduct involving a minor.
2. It shall not be an affirmative defense to this section that:
  - (a) A meeting did not occur; or
  - (b) The child was actually a law enforcement office posing as a child under fifteen years of age.
3. Age misrepresentation with intent to solicit a minor is a class 4 felony.

---

<sup>5</sup> Colorado § [362](#)