



1330 Connecticut Avenue, N.W. ♦ Washington, D.C. 20036 ♦ 202.862.3816 (v) ♦ 202.261.0604 (f)

June 3, 2005

The U. S. Internet Service Provider Association (US ISPA) respectfully submits these comments on sunset provisions in the USA PATRIOT Act. US ISPA is a national trade association that represents the common policy and legal concerns of the major Internet service providers (ISPs), portal companies and network providers.

We look forward to hearing from you on these positions and welcome feedback and questions from staff.

Respectfully,

Thomas M. Dailey  
Chairman

Christopher G. Bubb  
Vice Chairman

Stewart A. Baker  
General Counsel

## **US ISPA COMMENTS ON THE USA PATRIOT ACT SUNSET PROVISIONS**

The USA PATRIOT Act (“Patriot Act”)<sup>1</sup> and the previously enacted Electronic Communications Privacy Act (“ECPA”)<sup>2</sup> place Internet Service Providers (“ISPs”) and other telecommunications providers in a unique position between their customers and the government as holders of records.

ISPs assist the government in gathering information about serious crimes, from terrorism to child abuse. They know how important electronic evidence can be in investigating and preventing such crimes.

At the same time, ISPs have a strong commitment to the privacy of their customers. Part of this commitment is holding the government to strict compliance with the law by demanding that investigators “turn square corners” in seeking information about individuals.

From their vantage point in the middle of the debate about privacy and government authority, ISPs closely followed the enactment of the Patriot Act in 2001. The U.S. Internet Service Provider Association (“US ISPA”), which represents major ISPs, portal companies, and network providers, advised Congress on the original statute, and we now offer our views on several of the provisions that are scheduled to expire at the end of 2005.

US ISPA supports making permanent several of these provisions. US ISPA supported many of these provisions when it participated in the original drafting of the Patriot Act. It views them as uncontroversial yet necessary in order to ensure legal clarity and consistency for the role ECPA and the Patriot Act assign to ISPs and other telecommunications providers.

### **SECTION 202 – AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES (Amended 18 U.S.C. § 2516(1)(c)).**

Section 202 allows law enforcement agents to obtain wiretap orders when investigating a violation of the Computer Fraud and Abuse Act (“CFAA”),<sup>3</sup> typically some form of computer “hacking.” Prior to the Patriot Act’s enactment, the government could tap hackers’ email, but not their telephones, when investigating computer intrusions. (To conduct an intercept of electronic communications, the government need only be investigating a federal felony. To conduct a voice intercept, the government must be investigating one of a long list of enumerated crimes, and the list did not include hacking.)

---

<sup>1</sup> The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (“USA PATRIOT”) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (“Patriot Act”).

<sup>2</sup> Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2232, 2510-2521, 2701-2711, 3117, 3121-3126 (2000 & Supp. 2003)).

<sup>3</sup> 18 U.S.C. § 1030.

Wiretaps have long been critical to investigations of computer intrusions, but the lack of authority to carry out voice intercepts was rarely a concern because hackers usually communicated electronically. With the advent of Voice over IP technology, however, even intercepts that are mainly aimed at electronic communications may pick up some voice communications as well.

Section 202 simply added hacking to the list of crimes that justifies a voice intercept.<sup>4</sup> This addition allows investigators to continue to use intercepts in hacking investigations without fear that the presence of voice packets in the communications stream will make the intercept order invalid.

ISPs and their customers are among the principal victims of hackers. It is vital that the government be able to combat computer fraud and abuse practices, especially those such as phishing and pharming, which lead to identity theft. US ISPA supports providing law enforcement with the proper tools to fight hackers and other computer criminals. Section 202 preserves a tool upon which the government already relies heavily. The provision should be made permanent.

**SECTION 209 – SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS (Amended 18 U.S.C. §§ 2510(1), 2703(a), 2703(b)).**

Section 209 permits law enforcement authorities to obtain the contents of voice-mail under the same authorization required for obtaining stored email: All stored content may be obtained with a search warrant or, if the content has been in storage longer than 180 days, with a subpoena. In essence, Section 209 makes the Stored Communications Act technology-neutral. As was true with Section 202, technology has begun to erase the difference between stored voice and stored data communications.

Giving both types of stored content files the same protection is essential, especially with the increasing convergence of communications technology. For example, in many communications providers' systems, voice-mail messages are stored as audio files in emails – and it is nearly impossible for a provider to determine which email packets contain audio files storing voice-mail messages and which contain data. If Section 209 sunsets, however, there will be very real consequences for those ISPs called upon to produce the contents of electronic communications to the government. ISPs responding to routine law enforcement warrants and court orders for stored communications inadvertently could provide to law enforcement email files with audio attachments that contain the human voice. Without Section 209, ISPs under this scenario would run the risk of violating federal civil and criminal law.<sup>5</sup>

---

<sup>4</sup> Section 2516(1) provides that law enforcement officials may authorize applications for, and judges may grant orders “authorizing or approving the interception of *wire or oral* communications . . . when such interception may provide or has provided evidence of” the enumerated predicate felonies. *Id.* at 2516(1) (emphasis added). Meanwhile, Section 2516(3) states that law enforcement authorities may obtain orders for the “interception of *electronic* communications . . . when such interception may provide or has provided evidence of *any* Federal felony.” *Id.* at § 2516(3) (emphasis added).

<sup>5</sup> *Id.* at 2701.

The consistent treatment of electronic and wire communications in electronic storage is therefore critical to ISPs and other telecommunications providers. Accordingly, US ISPA supports making Section 209 permanent.

**SECTION 212 – EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB (Amended 18 U.S.C. §§ 2702, 2703).**

Section 212 corrected two problems with prior law governing disclosures to law enforcement of subscriber information. Under prior law, service providers could provide law enforcement with the content of subscriber’s communications for purposes of self-protection, but there was no similar rule for disclosure of non-content records. Section 212 made clear that service providers could disclose such information when seeking the help of law enforcement in response to attacks on their networks.

Second, prior to section 212, service providers could not provide subscriber communications or other information even in emergencies that posed a threat to life or limb. Section 212 permitted electronic communication providers to voluntarily disclose information about subscribers to law enforcement “if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person” requires or justifies disclosure.<sup>6</sup> Under this provision, ISPs may disclose both information about the subscriber and the content of the subscriber’s communications.

This provision is essential and should be made permanent. In fact, the portion of Section 212 that allows emergency disclosure of communications content was made permanent in 2002,<sup>7</sup> while the portion allowing emergency disclosure of subscriber information is still subject to sunset. This discrepancy should be cured by making all of section 212 permanent.

Permanently extending Section 212 will allow ISPs to continue to voluntarily disclose subscriber data in addition to the contents of communications when they believe an emergency exists warranting such disclosure. In the experience of US ISPA members, law enforcement has not used the emergency provisions with great frequency. But when an emergency arises, the availability of the provision can be crucial in protecting subscribers and others. Typically, ISPs disclose subscriber communications or other information to law enforcement in cases involving missing children.

In January 2004, for example, a 15 year-old kidnap victim – the daughter of a local bank manager – was found in Uruguay thanks to information that a large ISP disclosed under the Section 212 emergency provision. The kidnapper used email to communicate with the family for

---

<sup>6</sup> *Id.* at 2702(b)(8), (c)(4).

<sup>7</sup> Homeland Security Act of 2002, Public L. No. 107-296, Title II, § 225(d)(1)(C), codified at 18 U.S.C. § 2702(b)(8). The Homeland Security Act also established a requirement that law enforcement authorities that receive emergency disclosures from ISPs shall file reports with the Attorney General describing each disclosure from each ISP. *Id.* at § 225(d)(2).

a ransom. More recently, an ISP's emergency disclosure helped the Louisiana Cyber Crimes Taskforce locate a girl who had been lured to Texas by a man she met on the Internet.

These are harrowing experiences for all concerned, including the ISPs, who often must act very quickly. If Section 212 is not made permanent, an ISP would be able to provide the content of electronic communications in an abduction or missing child case, but it would not be able to provide the technical data that would be most useful in locating the child or the abductor. Consistent treatment is essential so that ISPs are not subject to liability for providing assistance to law enforcement in a life-or-death matter. Allowing this provision to expire will not end the emergencies that ISPs already see all too often. But it will expose ISPs to the agonizing choice between protecting themselves from the risk of liability or responding to a genuine crisis where a child's life or safety is at risk as minutes tick by. That is not a fair choice, and ISPs should not be forced to make it. For these reasons, US ISPA supports the permanent extension of Section 212.

**SECTION 215 – ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (“FISA”) (Amended 50 U.S.C. §§ 1861-1862).**

While Section 215 has been controversial, some proposed reforms to that provision have attracted wide support. US ISPA joins in supporting the Justice Department's proposal that if Section 215 is extended or made permanent, it should be modified to make explicit that parties served with FISA orders under FISA Section 1861(d) may discuss such orders with their attorneys and may challenge such orders in court in the same way that a party might challenge a subpoena *duces tecum*.<sup>8</sup> In order to most efficiently fulfill a FISA request, ISPs need to be able to share the request with counsel as necessary. Without the ability to share the request, ISPs are hindered in their ability to be fully responsive to law enforcement needs. That ability should not be encumbered by a vague prohibition on disclosure. In addition, ISPs cooperate with law enforcement whenever possible, but there may be occasions on which a FISA order recipient will seek to challenge an order as overly broad or burdensome. Although such a challenge has not yet been needed, and although ISPs believe they have the ability under existing law to challenge a FISA order if necessary, amending Section 215 to explicitly give FISA order recipients the ability to bring a challenge before the FISA court will bring needed clarity to the Act.

US ISPA also supports extending the immunity that Section 215 created for those who comply with FISA orders pursuant to Section 1861(e). Maintaining such immunity provisions are essential for all entities upon whom the burden of complying with FISA orders falls.

---

<sup>8</sup> *Hearing on Reauthorization of the USA PATRIOT Act Before the House Permanent Select Comm. on Intelligence*, 109th Cong. (2005) (statement of James B. Comey, Deputy Attorney General, U.S. Dept. of Justice) (stating that “[t]he Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court” and supporting “amendments to section 215 to clarify these points”), *available at* <http://intelligence.house.gov/Media/PDFS/ComedyStatement051105.pdf> (last visited May 26, 2005). Currently, the FISA Act prohibits a subject of a FISA Order from disclosing the contents of that order except as necessary for complying with the order, and it contains no provision allowing a subject of an order to contest such an order. 50 U.S.C. § 1861(d).

**SECTION 217 – INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS (Amended 18 U.S.C. §§ 2510(18)-(21), 2511(2)).**

Section 217 allows an ISP to authorize law enforcement authorities to intercept the communications of a suspected computer trespasser on the ISP’s network. The provision also allows victims of computer hacking to request assistance from law enforcement.

US ISPA supports the extension of Section 217 because its amendments to the Wiretap Act provide ISPs with a valuable tool in enlisting the assistance of law enforcement to combat hackers while also preserving the privacy of legitimate communications. Without this provision, ISPs would not be able to work closely with law enforcement while under attack. Before this provision was enacted, law enforcement was reluctant to assist ISPs who were watching intruders as the intruders criss-crossed the ISPs’ systems. Law enforcement was afraid that, if it worked too closely with an ISP performing an intercept, the courts would say that the ISP was really acting as law enforcement’s agent, so that the lawful ISP intercept would become, in effect, an unlawful government intercept. By allowing ISPs to cooperate with law enforcement intercepts, Section 217 has allowed ISPs to more effectively protect the security of their networks and of their customers. In order to protect network infrastructure and maintain a safe and secure online experience for our users, therefore, US ISPA supports making Section 217 permanent.

**SECTION 225 – IMMUNITY FOR COMPLIANCE WITH FISA WIRETAP (Added 50 U.S.C. § 1805(h)).<sup>9</sup>**

Section 225 grants electronic communication providers protection from civil suits when complying with a FISA wiretap order. US ISPA believes that this provision should be made permanent in order to guarantee continued cooperation between law enforcement and electronic communication providers. ISPs and other third parties who cooperate in carrying out criminal wiretaps have always received a statutory immunity.<sup>10</sup> This is also true for ISPs and other third parties who assist the government in carrying out pen/trap orders for criminal investigations.<sup>11</sup> The same immunity is granted under FISA when a national security investigator asks a communications provider to assist in fulfilling pen/trap orders.<sup>12</sup> By an oversight, however, there

---

<sup>9</sup> Section 225 added Section 1805(h) to FISA, and Section 1805(h) was later re-designated as Section 1805(i). The wiretap immunity provision states: “No cause of action shall lie in any court against any provider of a wire or electronic communication service . . . (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search.” 50 U.S.C. § 1805(i).

<sup>10</sup> 18 U.S.C. § 2511(2)(a)(ii).

<sup>11</sup> *Id.* at § 3124(d).

<sup>12</sup> 50 U.S.C. § 1842(f).

was no immunity for providers who assisted in carrying out a FISA *wiretap* order. That oversight was cured by Section 225.

This immunity is indispensable and uncontroversial, and we request that Congress make Section 225 permanent.

\* \* \*

US ISPA respectfully submits these comments to the committee and looks forward to working with you and staff on these issues. We welcome any further questions on these positions.