WHITE PAPER:

WHAT SHOULD ISPs DO WHEN THEIR NETWORKS BECOME CRIME SCENES?

February 1, 2011

Prepared by:

Joel M. Margolis

CALEA Consulting, LLC

for

Subsentio, Inc.

EXECUTIVE SUMMARY

The federal government has recently introduced an unusual number of proceedings governing the responsibilities of Internet service providers ("ISPs") to control criminal activity on their networks. The criminal acts could be cyber-crime -- including cyber-attacks, cyber-fraud, and illegal on-line content -- or traditional crimes like murder and robbery, where evidence of the crime is found in ISP communications.

To the extent the four federal proceedings (the "Network Control Proceedings") become law they would significantly reshape relationships between ISPs, law enforcement agencies ("LEAs"), and ISP customers. Each of these groups reflects an important public interest: ISPs require control over their networks; LEAs must conduct criminal investigations to protect public safety; and customers are entitled to communicate in private. How to balance these competing interests is the subject of this white paper.

The Network Control Proceedings

The most ambitious of the Network Control Proceedings is the Federal Communications Commission's recent order on net neutrality (the "FCC Order"). The FCC Order requires ISPs to be more transparent in their network control practices and generally prohibits ISPs from engaging in website blocking or discrimination against competing services. However, the FCC Order permits the providers to engage in "reasonable network management." An ISP could use its reasonable network management powers to defend against a cyber-attack or protect customers from unwanted content.

A second Network Control Proceeding is the proposed Combating On-Line Infringement and Counterfeiting Act ("COICA"). If enacted, COICA would create a procedure for law enforcement and ISPs to block websites that sell pirated content and knock-off goods.

Another Network Control Proceeding may substantially revise the Communications Assistance for Law Enforcement Act ("CALEA"). The purpose of CALEA is to help LEAs responsible for lawful electronic surveillance keep pace with evolutions in network technology. The statute specifically requires service providers to equip their networks so they deliver certain technical capabilities for lawful surveillance. The law also maintains the right of service providers to control their own networks and protects subscriber privacy.

CALEA has not been updated since it was enacted in 1994 and compliance with the law has been lax. Many service providers bypass the requirements of CALEA by negotiating alternate lawful surveillance arrangements with LEAs. These *ad hoc* arrangements fall under the pre-CALEA "technical assistance" clause (the "Technical Assistance Clause"). The Technical Assistance Clause was included in the Electronic Communications Privacy Act ("ECPA"), the law that protects communications privacy and in limited circumstances authorizes lawful surveillance. The Technical Assistance Clause imposed a general requirement on telecommunications carriers to assist lawful surveillance. However, the Clause did not contain specific technical requirements,

preserve the rights of carriers to control their networks, or protect customer privacy. As communications networks grew more sophisticated, the Clause lost its effectiveness. That is when Congress enacted CALEA.

"CALEA II" would, among other things, broaden the scope of statutory coverage and give LEAs a more reliable means of converting encrypted messages into clear text but would not change the continuing reliance on the Technical Assistance Clause.

Finally, Congress may amend ECPA. As noted above, ECPA generally protects the privacy of electronic communications but provides certain exceptions for LEA access to the communications of criminal suspects. The complex exceptions have grown confusing for service providers and LEAs alike. The "ECPA II" amendment would, among other things, add another exception to the list, this time to let providers make voluntary disclosures (as opposed to disclosures mandated by LEA due process) of a criminal suspect's stored records, but not stored content, to LEAs as needed to combat cyber-attacks and cyber-fraud.

Inconsistencies Among the Network Control Proceedings

The Network Control Proceedings have progressed on separate legislative and regulatory tracks. As a result, they are not designed to work together. The misalignments among the legal initiatives may pose conflicts for the policy interests involved. An ISP may find its right of network control eroded, an LEA may be frustrated in its implementation of lawful electronic surveillance, or customer privacy rights may be infringed.

For example, it is unclear whether the reasonable network management standard articulated in the FCC Order gives ISPs the right to block the kind of rogue websites targeted by COICA. COICA envisioned that ISPs would conduct such blocking only in response to a court ruling. The FCC Order may also conflict with CALEA II by endorsing the right of customers to use applications of their choice. Sophisticated users can design encryption applications that evade lawful surveillance. Those applications could prevent CALEA II from meeting its goal of overcoming surveillance-frustrating encryption.

COICA may also undercut the policy goals of the other Network Control Proceedings. The proposed bill aims to require "reasonable measures" to block websites dedicated to "infringing activities." But if those loose terms are not strictly defined, the law may inadvertently block lawful websites. The FCC Order declared that all lawful sites should remain freely available to consumers, and ECPA upholds the right of users to surf the web in private.

Because the Technical Assistance Clause lacks the technical specifics of CALEA, as well as safeguards for network control and subscriber privacy, widespread reliance on the Clause as a substitute for CALEA has shortchanged the goals of the CALEA statute. Consequently, LEAs still struggle to keep pace with evolutions in network technology,

ISPs cannot be sure what surveillance capabilities they are required to deliver, and over-deliveries of data to LEAs could compromise privacy. CALEA II shows no sign of breaking these non-CALEA habits.

ECPA II permits ISPs subject to cyber-attacks or cyber-fraud to make voluntary disclosures to LEAs of only stored records. By contrast, the reasonable network management standard in the FCC Order imposes no such limits on an ISP's right to defend against cyber-attacks. The legislative proposal also adds another legal wrinkle to a statute that is already notoriously complex.

The Network Control Proceedings Should be Harmonized

With a few common-sense adjustments, the Network Control Proceedings could be harmonized. The goal of this harmonization should be to give ISPs, LEAs and customers a fair balance of rights and responsibilities.

The FCC should clarify that reasonable network management refers only to acts of network control that relate directly to network management. Unwanted content should be addressed by other laws, such as COICA, where a court can determine whether a website is illegal before the site is blocked. The FCC should also clarify that although customers have broad freedom to use applications of their choice, that freedom should not extend to user-initiated encryption applications designed to evade lawful surveillance.

Consistent with the FCC clarification of website access, Congress should define the COICA term "infringing activities" in a manner that ensures only illegal websites are blocked. Likewise, legislators should define "reasonable measures" specifically enough to avoid the kind of unaccountable practices tolerated under the Technical Assistance Clause.

Lawmakers could fulfill CALEA's goals of network control, public safety and user privacy by giving the statute priority over the Technical Assistance Clause. Simply put, entities subject to CALEA should comply with CALEA, and no alternate provisions should apply. The Technical Assistance Clause could be reserved for entities not subject to CALEA or entities subject to CALEA enforcement proceedings, where LEAs must use alternate technologies to implement a given court surveillance order.

As for ECPA II, a right of voluntary disclosure that includes both stored records and stored content would give ISPs the complete power they need to combat cyber-attacks and cyber-fraud, as contemplated by the FCC Order. A broad disclosure right would also be more consistent with the existing terms of ECPA, which already permit voluntary ISP disclosures of both records and content in other crime-related situations.

Table of Contents

WHITE PAPER:

WHAT SHOULD ISPs DO WHEN THEIR NETWORKS BECOME CRIME SCENES?

I. INTRODUCTION

Suppose an Internet Service Provider ("ISP") discovers a dangerously high volume of Internet traffic traversing its broadband network. Many of the ISP's customers may start complaining of failures in their Internet access service. Perhaps the provider's network engineers cannot readily tell whether the disruption is a cyber-attack or just an aberrant spike in congestion.[1] What should the provider do? Start analyzing the private communications of its subscribers to diagnose the IT threat? Notify a law enforcement agency ("LEA") and send it the communications associated with the suspicious activity? Take no action, out of respect for user privacy, until the cause of the problem is known?

ISPs must control their network traffic, especially when those networks are attacked. The more difficult question is when and how the service providers should involve law enforcement. Three competing interests are involved. ISPs want to operate their networks as they see fit. LEAs need ISP cooperation to investigate certain crimes. And ISP customers expect their private communications to remain private.

---

[1] BitTorrent, a technology designed for peer-to-peer file sharing of high-volume content, may be shared lawfully in a way that causes network congestion or used to launch an illegal cyber-attack. "'BitTorrent' Exploit could be used to Stage Massive Cyber Attacks, The Raw Story, December 30, 2010, http://www.rawstory.com/rs/2010/12/bittorrent-exploit-stage-massive-botnet-cyber-attacks/.

The federal government has launched a host of initiatives addressing the responsibilities of ISPs to combat criminal activity on their networks. These efforts may produce as many as four new sets of law.[2] This white paper will refer to the four inquiries as the "Network Control Proceedings" or the "Proceedings." Unfortunately, none of the Network Control Proceedings appears to be well-coordinated with the other three. As a result, each may inadvertently undercut the others.

This paper recommends a way to reconcile the Network Control Proceedings for the benefit of all sides: ISPs, LEAs and customers. The recommended plan is necessarily a compromise, acknowledging that every gain for one interest is a loss to another. Hopefully the proposal will help forge a consensus on these sensitive policy matters.

Section II of this paper describes the types of criminal activity that arise on ISP networks. Section III summarizes the Network Control Proceedings. Section IV highlights the potential inconsistencies among the Proceedings. Section V suggests a way to harmonize the four laws. Section VI proposes certain legislative language to implement the harmonization. And Section VII offers some concluding thoughts.

II. TYPES OF CRIME ON ISP NETWORKS

An ISP has responsibilities for two categories of crime. The first is known as "cyber-crime." The commonly known cyber-crimes are cyber-attacks, cyber-fraud and illegal on-line content. The second category of ISP responsibility involves traditional crimes like murder and robbery that leave footprints on an ISP's digital turf. The following explains the nature of these crimes and how they are investigated today.

A. Cyber-Crime

Although there is no single definition of cyber-crime it is generally regarded as any crime committed "using a computer and the Internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs."[3] The following describes the types of cyber-crimes seen on ISP networks.

---

[2] A fifth proceeding is also pending but is too new and speculative to be addressed in this paper. In the House Judiciary Committee, the Subcommittee on Crime, Terrorism and Homeland Security began hearings on January 25, 2011 regarding the concept of imposing a data retention mandate on ISPs and perhaps other Internet-based entities. *See* hearing information at http://judiciary.house.gov/hearings/hear_01252011.html.

[3] TheFreeDictionary.com. http://www.thefreedictionary.com/cybercrime.

1. Cyber-Attacks

A cyber-attack is generally defined as a computer command:

> targeting vulnerable computers and making them malfunction or resulting in disrupted flows of data that disable businesses, financial institutions, medical institutions, and government agencies.[4]

One common type of cyber-attack is a distributed denial of service ("DDOS") attack. In a DDOS attack a robot network of infected computers called a "bot-net" directs an overwhelming blast of IP queries to an Internet domain, knocking out a web site, a company, or even a utility.[5] The security firm McAfee reports that more than half the world's critical infrastructure organisations have admitted to being targeted by cyber-attacks.[6]

The main law that protects against cyber-attacks is the Computer Fraud and Abuse Act of 1984 ("CFAA").[7] Under the CFAA "computer trespassing" (hacking) may be prosecuted as a felony. ISPs may apply traffic-analyzing technology to investigate cyber-attacks.[8]

Less certain is whether an ISP may voluntarily disclose evidence of a cyber-attack to an LEA. The disclosure of customer communications is generally prohibited by the Electronic Communications Privacy Act of 1986 ("ECPA"), a statute designed to protect communications privacy. [9]

One exception to the ECPA disclosure ban permits service providers to divulge communications as needed for the "rendition of [their] service" or to protect their "rights or property."[10] But this pre-Internet exception was intended for traditional telephone companies and cellular carriers to conduct limited, case-by-case inquiries into easily-

---

[4] http://computer.yourdictionary.com/cyber-attack.
[5] "McAfee: Big Business Under Constant Cyber-Attack," PCMag.com, January 29, 2010, http://www.pcmag.com/article2/0,2817,2358610,00.asp.
[6] "Critical Infrasturcture Under Continual Cyber Attack, Says Report," Computerweekly.com, January 28, 2010, http://www.computerweekly.com/Articles/2010/01/28/240112/Critical-infrastructure-under-continual-cyber-attack-says.htm?printerfriendly=true.
[7] 18 U.S.C. § 1030.
[8] *Id*. at § 2511(2)(i).
[9] *Id*. at § 2701 *et. seq*. and § 2510 *et. seq*. Technically, ECPA is an amendment to the Wiretap Act. 18 U.S.C. § 2510 *et. seq*. But today the two laws are commonly referenced collectively as "ECPA."
[10] *Id*. at §§ 2702(b)(5), 2702(c)(3).

definable harms, such as theft of service[11] or obscene calls.[12] The carve-out did not contemplate the need for continuous ISP vigilance to defend against sophisticated, network-crashing codes. The provision certainly did not anticipate the kind of malfeasance that could freeze-up a home computer without harming the rights or property of the service provider itself.[13]

2. Cyber-Fraud

A cyber-crime is usually called "cyber-fraud" when it targets computer users, as opposed to the computers themselves.[14] One common type of cyber-fraud, called "phishing," can be used as a means of identity theft. In this scam, the criminal creates a fake web site to trick a customer into disclosing his or her computer password, social security number, credit card number, or bank account information. Other types of cyber-fraud use deception to steal national security secrets, trade secrets, or insights on a person's private life. According to the FBI's latest annual report on the subject, cyber-fraud complaints in 2009 rose 22.3% over 2008 and caused over $559 million in damages.[15] Like cyber-attacks, cyber-fraud is prosecuted as a felony under the CFAA.

A lawful relative of cyber-fraud is regulated by the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (the "CAN-SPAM Act").[16] The CAN-SPAM Act permits an e-mail marketer to circulate unsolicited commercial e-mails ("spam"), as long as the sender complies with certain rules of transparency and gives recipients the ability to unsubscribe. Violations of the Act are subject to criminal prosecution.

The CAN-SPAM Act imposes no obligations on ISPs. However, ISPs actively weed out spam from their networks. They do so to protect customers from the unwanted messages and reduce network congestion. The providers detect the spam using deep packet inspection ("DPI") technology, which can filter IP communications based on key words and file names.

3. Illegal On-Line Content

ISPs are not required to block websites that display child pornography. However, if an ISP encounters evidence of such a crime it must report the matter to the National

---

[11] U.S. v. Harvey, 540 F. 2d 1345 (8th Cir. 1976).
[12] *See, e.g*. *Sistok v. Northwestern Telephone Systems, Inc*., 189 Mont. 82 (1980).
[13] "Cyber–Attacks More Aggressive Than Ever," MSNBC.com, March 28, 2007. http://www.msnbc.msn.com/id/17680243/.
[14] Cyber Fraud, Scams, and Hoaxes – Definition and Prevention, Cyber Top Cops, the Cyber Security Experts, http://www.cybertopcops.com/anti-fraud.php.
[15] "IC3 2009 Annual Report on Internet Crime Released," FBI National Press Office, March 12, 2010, http://www.ic3.gov/media/2010/100312.aspx.
[16] 15 U.S.C. § 7701 *et. seq*.

Center for Missing and Exploited Children ("NCMEC").[17] NCMEC is a private, non-profit clearinghouse which coordinates with law enforcement to protect children from various crimes, including child pornography.[18]

B. Traditional Crime

To investigate traditional crimes such as murders and robberies, an LEA may need to read copies of a criminal suspect's stored communications records (e.g. billing records reflecting who the suspect called, and who called the suspect, at different times and dates). Alternatively, the LEA may need to see stored communications content (e.g. the text of emails, buddy lists, or calendars). In these situations the LEA would send the suspect's ISP the applicable subpoena, warrant, or court order for the targeted materials, and upon receipt of the "due process" the ISP would be required to disclose the items.[19] If the disclosed records or content reveal incriminating evidence, the LEA may follow up with a more powerful court order to monitor the suspect's broadband sessions in real time.[20] The live monitoring is called "lawful electronic surveillance" or "lawful interception."

The LEA authority to implement the above criminal procedures is governed by ECPA. By comparison, the technical support an ISP must provide an LEA for lawful surveillance is governed by the Communications Assistance for Law Enforcement Act ("CALEA").[21] ECPA and CALEA are the objects of two of the Network Control Proceedings.

Notice ISP assistance to LEAs for traditional crimes is mandatory, whereas ISP assistance to LEAs for cyber-crimes is mostly voluntary. By the same token, the government regulates the technical measures used to implement lawful surveillance but not the technical how-to of fighting cyber-crimes. Accordingly, new mandates on ISPs to assist LEAs should consider the burdens they impose at both the stage of legal authority and the subsequent stage of technical implementation.

III. THE NETWORK CONTROL PROCEEDINGS

The following summarizes the four Network Control Proceedings, where federal authorities are defining the boundaries of ISP network control over ISP-related crime.

---

[17] 18 U.S.C. §§ 2702(b)(6), 2702(c)(5).
[18] *See* NCMEC's website at http://www.ncmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362.
[19] 18 U.S.C. § 2702.
[20] *Id*. at § 2518.
[21] 47 U.S.C. § 1001 *et. seq*.

A. The FCC Order

The proceeding with the broadest implications for ISP network control was launched by the Federal Communications Commission (the "FCC") and culminated in the Open Internet Order (the "FCC Order").[22] The FCC Order established rules of Internet neutrality, or "net neutrality," to promote the free and fair development of the Internet. As expected, the controversial ruling has been challenged in court.[23]

The FCC Order imposed three rules on ISPs.[24] The first rule, "transparency," requires ISPs to disclose information about their network management practices so consumers can make informed choices on how to use the ISP services, as well as the applications, content and devices of their choice.[25] Next is the "no blocking" rule. It states that a fixed (i.e. landline or cable) ISP may not block lawful content, applications, services, or non-harmful devices.[26] Finally, rule three prohibits fixed ISPs from engaging in "unreasonable discrimination" in the transmission of lawful traffic.[27]

The above rules are subject to the ISP's right of "reasonable network management."[28] A network management practice is reasonable if appropriate and tailored to a legitimate network management purpose considering the network architecture and technology.

Reasonable network management includes measures to ensure network security and integrity, address traffic harmful to the network, curb traffic unwanted by users, or reduce or mitigate network congestion. Network integrity measures include those meant to defend against cyber-attacks.[29] Unwanted traffic includes spam[30] and illegal websites such as those that peddle child pornography.[31] ISP practices not directly

---

[22] *Preserving the Open Internet, Report and Order* in GN Docket No. 09-191, WC Docket No. 07-52, FCC 10-201, released December 23, 2010.
[23] "Verizon Sues FCC Over Net-Neutrality Rules," Washington Post, January 20, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/20/AR2011012005853.html?wprss=rss_technology/techpolicy, "Accused of Violating Net Neutrality, MetroPCS sues FCC," Wired.com, January 25, 2011, http://www.wired.com/epicenter/2011/01/metropcs-net-neutrality-challenge/.
[24] *FCC Order* at paras. 43-114. The FCC limited the scope of the Order to ISPs, in part for jurisdictional reasons and in part because ISPs, as the gatekeepers of Internet access, are uniquely positioned to control the Internet's growth. FCC Order at para. 50.
[25] *Id.* at paras. 53-61.
[26] *Id*. at paras. 62-67. A milder version of the rule applies to mobile ISPs.
[27] *Id*. at paras. 68-79.
[28] *Id*. at paras. 80-92.
[29] *Id.* at para. 88.
[30] *Id*. at para. 55.
[31] *Id*. at para. 89.

related to network management, such as those addressing the transmission of unlawful content, were left to other laws.[32]

B. The COICA Bill

Next in importance to the issue of ISP network control over Internet-related crime is U.S. Senate Bill S. 3804, the Combating On-Line Infringement and Counterfeiting Act ("COICA").[33] COICA would give law enforcement the authority to shut down web sites found to be "dedicated to infringing activities."

What constitutes an infringing activity is a controversial topic, but the purpose of the bill is to target so-called "rogue" web sites that violate copyright laws (e.g. by selling illegal copies of music, movies, or games) or traffic in counterfeit goods (e.g. by selling cheap imitations of prescription drugs without a prescription). COICA would supplement the Digital Millennium Copyright Act of 1998,[34] which in pertinent part immunizes ISPs from copyright infringement liability as long as they cooperate with copyright holders to curb the copyright abuses. COICA is similar to the anti-child pornography law in that it would shutter websites based on their illegal content.

The section of COICA relevant to ISPs would require the providers, upon service of due process, to "take technically feasible or other specified reasonable measures to prevent such infringing activities."[35] Specifically, the ISP would block users from accessing the infringing site by preventing the site's domain name (e.g. www.infringingmusic.com) from resolving to the site's Internet protocol address (e.g. 172.18.253.1). An ISP would not be required to modify its network to comply with the law.

On November 18, 2010 the Senate Judiciary Committee unanimously approved the COICA bill.[36] Committee Chairman Senator Patrick Leahy pledged to advance the bill further this year.[37]

C. The CALEA Reform Proposal

Also important in the realm of ISP network control over crime is a CALEA reform initiative from the Department of Justice ("DOJ").[38] Although no draft "CALEA II" has

---

[32] *Id*. at para. 82.
[33] *See* draft bill at http://www.govtrack.us/congress/billtext.xpd?bill=s111-3804.
[34] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).
[35] COICA at § 2(B).
[36] Senate Panel Passes Controversial Online Piracy Bill, Datamation, November 18, 2010, http://itmanagement.earthweb.com/secu/article.php/3913811/Senate-Panel-Passes-Controversial-Online-Piracy-Bill.htm.
[37] *Id*.
[38] "Wiretapping and Other Eavesdropping Devices and Methods," New York Times, October 19, 2010,

been made public, Congress may start the proceeding as soon as this year.[39] As mentioned above, CALEA regulates the technical capabilities that service providers deliver to LEAs conducting lawful electronic surveillance. The purpose of CALEA is to preserve the ability of LEAs to implement lawful surveillance despite evolutions in network technology.[40] Specifically, CALEA requires telecommunications carriers to equip their networks so they can provide an LEA with the call content and call-identifying information ("CII") of a communication subject to a court surveillance order.[41] The mandate also maintains carrier control over the design of network equipment[42] and protects subscriber privacy.[43]

CALEA's privacy-protection safeguards ensure that lawful intercepts are implemented by a carrier only when appropriately ordered by a court and only when further approved by a specially-authorized officer or employee of the carrier company. Moreover, the intercept must be accomplished in a way that does not disturb the communications of any users other than the criminal suspect identified in the court order. For these reasons, privacy-minded members of the public have good reason to prefer that lawful intercepts be conducted in compliance with CALEA.

The 16-year-old CALEA statute was enacted before the widespread adoption of broadband service. In 2005 the FCC updated the law to cover facilities-based broadband Internet access and two-way interconnected voice over Internet protocol ("VoIP").[44] However, other advanced services such as Skype's peer-to-peer VoIP remained uncovered.

CALEA has also sustained widespread lapses in compliance.[45] In 2008 the Office of the Inspector General issued a report on the status of CALEA implementation.[46] The report described an FBI survey on the number of industry switches upgraded with the

---

http://topics.nytimes.com/top/reference/timestopics/subjects/w/wiretapping_and_other_eavesdropping_devices_and_methods/index.html?scp=1&sq=CALEA&st=cse.

[39] "Judiciary Chair Planning IP, Privacy Bills," InternetNews.com, January 11, 2010. http://www.internetnews.com/government/article.php/3920326/Judiciary+Chair+Planning+IP+Privacy+Bills.htm.

[40] H.R. Rep. No. 103-827, pt. 1, at 14-15 (1994).

[41] 47 U.S.C. § 1002(a)(1)-(4). CII in the context of a broadband data session would not literally identify a "call" but would include the suspect's inbound and outbound signaling information. *See* 47 U.S.C. § 1001(2).

[42] *Id*. at § 1002(b)(1).

[43] *Id.* at § 1004.

[44] *CALEA Broadband Coverage Order, First Report and Order* in ET Docket No. 04-295, 20 F.C.C.R. 14989 (2005).

[45] *See* note 38, *supra*.

[46] Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, Audit Report 08-20, March, 2008, Office of the Inspector General, http://www.justice.gov/oig/reports/ FBI/a0820/results.htm.

required CALEA capabilities. According to the survey, "nearly 40% of their switches could not be used to produce CALEA-compliant electronic surveillance results."[47]

CALEA II would primarily expand the scope of CALEA-covered entities to include providers such as Skype and other advanced IP players like Google, RIM, and Facebook.[48] The goal is to level the competitive playing field so CALEA is not limited to the context of traditional carriers. Among other things, the bill would also modify the CALEA provision that intended service providers to help law enforcement unscramble encrypted suspect communications.[49] Without these reforms, LEAs say, their lawful surveillance mission will be frustrated.

The CALEA reform would not affect a pre-CALEA provision in ECPA known as the technical assistance clause (the "Technical Assistance Clause"). The Technical Assistance Clause requires anyone served with a surveillance order to provide the investigating LEA with "all information, facilities, and technical assistance necessary to accomplish the interception …."[50] The early-era provision lacks the technical specifics of CALEA and contains no safeguards for carrier network control or privacy. Nevertheless, many service providers that do not comply with CALEA make *ad hoc* arrangements with LEAs to provide whatever assistance the parties agree is appropriate under the Technical Assistance Clause. As a result, compliance with the Clause has become a *de facto* substitute for CALEA compliance.

D. The ECPA Reform Proposal

Also high on the Congressional agenda is a plan to modernize ECPA. In fact, hearings on the statute were held last year in the House Judiciary Committee's Subcommittee on the Constitution, Civil Rights and Civil Liberties.[51] Although the text of the bill has not been released, the Capitol Hill hearings indicate the amendment could significantly impact an ISP's relationship with LEAs.

As noted above, ECPA protects the privacy of electronic communications, including ISP communications, but permits various exceptions. Some of the exceptions are for LEAs when those entities meet certain legal qualifications to monitor a suspect's communications, as described above. ECPA has not been significantly amended in 14 years, and the statute is considered a notoriously burdensome patchwork of confusing standards.[52] One federal court remarked that ECPA is "famous (if not infamous) for its

---

[47] *Id.*
[48] *See* note 38, *supra.*
[49] *Id*. *See* 47 U.S.C. § 1002(b)(3).
[50] 18 U.S.C. § 2518(4).
[51] *See* hearing information at http://judiciary.house.gov/hearings/hear_100923.html.
[52] "1986 Privacy Law Is Outrun by the Web," New York Times, January 9, 2011, http://www.nytimes.com/2011/01/10/technology/10privacy.html?_r=3&pagewanted=2&ref=technology.

lack of clarity."[53] The Digital Due Process Coalition ("DDPC"), a group of major Internet providers, think tanks, and privacy groups, has urged Congress to reform the convoluted law. DDPC's approach to the reform is:

> [t]o simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.[54]

Among other things, DDPC proposes that LEAs should be held to a single ECPA standard of "probable cause" when asking service providers for a suspect's emails, regardless of how long or where the messages have remained in electronic storage.[55] Some experts favor this proposed simplification.[56]

Rumors suggest some members of Congress want the ECPA amendment to include a measure for cyber-security. In particular, if an ISP has a good faith belief that its network is subject to a cyber-attack or cyber-fraud, the new wording would let the provider make a voluntary disclosure of suspect communications records, but not content, to an LEA. The goal is to facilitate the kind of information sharing considered necessary to handle these cyber-crimes.[57]

---

[53] *Steve Jackson Games, Inc. v. United States Secret Serv*., 36 F. 3d 457, 462 (5th Cir. 1994).

[54] *See* the Digital Due Process website, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

[55] *Id.*

[56] *See, e.g.,* Written Testimony of Albert Gidari, Partner, Perkins Coie LLP, Hearing on Electronic Communications Privacy Act Reform, May 5, 2010, http://www.perkinscoie.com/files/upload/LIT_10-05_Written_Testimony_of_Albert_Gidari.pdf. *See also*, Written Testimony of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University, Hearing on Electronic Communications Privacy Act Reform and the Revolution in Cloud Computing, September 23, 2010, http://judiciary.house.gov/hearings/pdf/Felten100923.pdf.

[57] "Nation's Cybersecurity Suffers From a Lack of Information Sharing," Government Computer News," March 3, 2010, http://gcn.com/articles/2010/03/03/cybersecurity-policy.aspx.

IV. INCONSISTENCIES AMONG THE NETWORK CONTROL PROCEEDINGS

The four Network Control Proceedings all address the competing policy interests of ISPs, LEAs, and customer privacy. But because the initiatives are progressing on separate tracks, they are not designed to work together. The inconsistencies between them could create policy conflicts. In particular, the misalignments could frustrate the proceedings from developing into laws, provoke litigation, or leave interested parties more confused than ever about their rights.

A. Inconsistencies Posed by The FCC Order

The FCC Order properly reinforces the ECPA rights and property clause.[58] It is also compatible with ECPA II because both pronouncements help ISPs combat cyber-attacks. In other respects, however, the FCC Order may conflict with the other Network Control Proceedings.

1. The Scope of Reasonable Network Management is Unclear

The FCC Order gives ISPs the right of reasonable network management when defending against cyber-attacks and unwanted content such as spam and pornographic sites. On the other hand, the reasonable network management standard does not apply to matters that do not relate directly to network management. Those other matters, including the transmission of unlawful content, were left to other laws.

An ISP could validly claim spam is both unwanted and directly related to network management because spam causes network congestion. But cyber-fraud and illegal websites may not relate directly to network management. The CFAA already empowers ISPs to combat cyber-fraud. But the question remains, what measures may an ISP take against illegal websites? May providers voluntarily develop DPI tools to combat them in the same manner as spam? Or would such practices violate the FCC's no-blocking rule?

The use of DPI against illegal websites is also questionable from an ECPA perspective. One court recently ruled that an ISP's use of DPI constituted an unauthorized interception when used for third-party Internet advertising.[59] On the other hand, the

---

[58] Actually, the reasonable network management standard is broader than the rights and property clause. The older law protects only the service provider's own network whereas the newer one could be used to protect customer devices. But the incongruity would not upset the balance of network control rights enshrined in ECPA because ECPA is a federal statute, and federal statues supersede administrative agency rulings such as the FCC Order.

[59] *Mortensen v. Bresnan Communications, LLC*, No. CV 10-13-BLG-RFC (D. Mont. Dec. 13, 2010).

use of DPI against an illegal site may fall under the ECPA exception for the protection of rights and property. Alternatively, DPI would not be defined as a "device" of interception if used "in the ordinary course of business."[60] Managing traffic congestion may be deemed a task in the ordinary course of business.

2. The No Blocking Rule May Thwart Efforts to Address Encryption

The FCC's no-blocking rule prohibits an ISP from blocking any lawful application a customer may use. One application -- encryption -- is perfectly lawful. It is also vital to secure the privacy of a variety of communications from financial transactions to health care data to many other personal records. VoIP networks use encryption for security reasons.[61]

If CALEA-covered entities supply the encryption function for their communications networks, CALEA already requires them to perform the clear-text conversion for purposes of lawful surveillance.[62] However, in any network that permits customers to use their own encryption programs, the provider has no CALEA obligation to unscramble the messages and may be technically unable to do so. This trend has made encryption a growing problem for LEAs.[63]

Details on LEA surveillance capabilities are not made public, but two points are known. Lawfully intercepted communications that cannot be decrypted are useless to criminal investigators. Also, the announcement of the CALEA II initiative included a statement about improving CALEA's encryption clause. These facts speak for themselves. Thus, to the extent the FCC Order promotes free choice in encryption applications it may frustrate CALEA II.

B. Inconsistencies Posed by COICA

Theoretically, COICA would target only unlawful content and therefore pose no conflict with the FCC Order, which protects lawful content. But the proposal must overcome at least two risks to meet that goal.

---

[60] 18 U.S.C. § 2510(5)(a)(2).
[61] "iPhone Security News - iPhone Voice Communications Encryption Security App Now Available," Free Press Release, December 30, 2010, http://www.free-press-release.com/news-iphone-security-news-iphone-voice-communications-encryption-security-app-now-available-1293757031.html.
[62] 47 U.S.C. § 1002(b)(3).
[63] "Encryption Advocates Resist Legal Limits," CNNTech, September 18, 2001, http://articles.cnn.com/2001-09-18/tech/encryption.defense.idg_1_encryption-bin-pgp-security?_s=PM:TECH

1. The Term "Infringing Activity" May Be Overbroad

The term "infringing activity," if not carefully defined, may capture websites that feature infringing material inadvertently. For example, You-Tube sometimes receives unauthorized videos but removes them when presented with valid "take-down" notices from the copyright holders. An overbroad definition of "infringing activity" would contravene the FCC principle of customer choice and undercut the ECPA goal of customer privacy.

2. Technical Solutions May Be Overbroad

COICA would require ISPs to block infringing sites using "reasonable measures." This vague language could permit unaccountable technologies and practices, just as the above-described Technical Assistance Clause led to *ad hoc* departures from CALEA compliance.

C. Inconsistencies Posed by CALEA II

The policy concerns of CALEA are the same as those of the other Network Control Proceedings: to ensure public safety, maintain carrier network control and protect privacy. Unfortunately, the widespread lack of CALEA compliance, along with an overreliance on the non-CALEA Technical Assistance Clause, has shortchanged these goals. Unless CALEA II is modified to put CALEA compliance back on track, it could pose several policy conflicts with the other Proceedings. The following explains the harms of non-CALEA compliance under the Technical Assistance Clause.

1. The Technical Assistance Clause Disrupts a Carrier's Network Control and Creates Competitive Disparities

Regardless of whether a service provider complies fully with CALEA, it remains subject to the additional technical requirements of the Technical Assistance Clause. Moreover, the double burden is an open-ended one because the Clause broadly requires providers to deliver whatever information, equipment or facilities are "necessary" for the given interception.[64] One example of such a non-CALEA capability is "cell phone pinging," a technique that a cellular carrier can use to determine the location of a suspect phone.[65] Carriers have delivered this capability to LEAs for years. The same kind of non-CALEA arrangement could cause an ISP to divert its DPI capability from a business use to a lawful surveillance case. These unpredictable requests disrupt the carrier's control over its network, despite the intent of CALEA and the reasonable network control standard.

---

[64] *United States Order Authorizing Roving Interception*, 349 F. 3d 1132, 1144 (2003).

[65] "Locating Mobile Phones through Pinging and Triangulation," PM Pursuit Magazine, July 1, 2008, http://pursuitmag.com/locating-mobile-phones-through-pinging-and-triangulation/.

Even if an LEA does not impose a double burden of technical assistance on a CALEA-covered service provider, the task of complying with CALEA, by itself, places the provider at a competitive disadvantage to its non-compliant competitors. Compliant entities spend time, effort, and money on the objective of meeting the federal mandate. Their non-compliant counterparts focus resources on their revenue-producing business goals. Considering the proponents of CALEA II want to level the playing field of CALEA coverage, they should likewise level the playing field of CALEA compliance.

2. The Technical Assistance Clause Hinders LEA Access to Quality, Timely Solutions and Increases LEA Costs

LEAs have also been disappointed by the lack of CALEA compliance. In the many cases where a service provider lacks a CALEA surveillance solution, the LEA has few choices. It must rely on whatever surveillance capabilities the provider happens to have, attach its own surveillance equipment to the network, buy new equipment, borrow hardware or software from another LEA, or forego the needed surveillance. Even if an LEA obtains its own intercept device, chances are it will hardly match the quality of a solution fashioned by the provider's own equipment vendor and designed for its own network architecture. The make-shift device may not even deliver a complete set of CALEA capabilities. Equally troubling, it may miss suspect communications traveling on back roads in the network. And in the case of advanced networks, an LEA may not even know what kind of gear to use. These haphazard outcomes, where LEAs are left struggling to keep pace with evolutions in network technology, are just the kind of foul-ups that CALEA was supposed to prevent.

CALEA encourages quality standards by giving legal "safe harbor" status to any carrier that deploys a CALEA solution in conformance with a published industry technical standard. [66] Published standards are more likely to be tailored to individual services (e.g. broadband data, VoIP) and service platforms (e.g. wireline, wireless, cable), each of which operates with its own set of CII. The standards enable the identification and formatting of CII in ways that LEAs can interpret. And they ensure that LEAs can correlate the CII to the given communications content.

The non-CALEA approach also delays investigations because it takes more time to transport an LEA solution to a network than it does to activate a solution already in place. A loss of even an hour could be decisive in a life-or-death emergency.

Finally, it can be expensive for an LEA to build its own solutions. LEA budgets are already strained. Most LEAs can ill afford the extra cost of crafting different surveillance devices for all the different network types.

---

[66] 47 U.S.C. § 1006.

3. The Technical Assistance Clause Compromises Privacy

The Technical Assistance Clause also compromises privacy. When a carrier provides an LEA with non-CALEA capabilities such as cell-phone pinging the assistance may not violate the applicable court order but does enable the access of private information in *ad hoc* ways. Consequently, there is no detached authority such as a CALEA technical standard-setting body to ensure the CII capabilities are truly call-identifying and not something more.

By the same token, when a surveillance solution is developed by an LEA it is not published like a safe harbor standard. Therefore the LEA technology is not independently reviewable to confirm it meets CALEA's privacy goal.

Another privacy concern arises in non-CALEA intercepts when a carrier over-delivers information to an LEA. For example, if the court order requires the carrier to disclose only a suspect's signaling information, many carriers deliver both signaling and content, leaving it to the LEA to "minimize" the output by filtering out the content.[67] Likewise, for court orders that target a suspect's VoIP communications, some carriers deliver the packet stream for the suspect's entire broadband session, which may include not only VoIP but text messages, video, and browsing activities. LEA minimization is perfectly legal. Still, more efficient intercepts, such as those produced by safe harbor solutions, would avoid the need for that fall-back approach.

D. Inconsistencies Posed by ECPA II

The ECPA reform initiative is essentially compatible with the FCC Order. ECPA II would permit an ISP to disclose voluntarily a cyber-attack to an LEA, and the FCC's reasonable network management standard would consistently let the ISP block the offending traffic. Even if the supposed cyber-attack turned out to be a case of accidental network congestion, the "good faith" provision of ECPA II would protect the mistaken ISP from liability.

However, ECPA II falls short of the FCC's reasonable network management standard. The legislative proposal would allow ISP disclosures of only one type of data: records. The reasonable network management standard gave ISPs broad flexibility to combat cyber-attacks using any technique that did not block lawful content, discriminate against competitors, or limit consumer choice. The FCC took no position on the right of ISPs to fight other cyber-crimes but didn't curtail those rights either.

Cyber-attacks can cause catastrophic harm. Cyber-fraud can also be very damaging. These crimes are difficult to anticipate, identify, classify, and control. And they involve both records and content. If the criminal packet stream is encrypted, an ISP may not be

---

[67] *See* 18 U.S.C. § 2518(5).

able to separate records from content. In any event, LEAs may need both types of data to solve the given crime.

ECPA II also overlooks the movement to simplify the ECPA statute. ECPA consistently permits an ISP to make voluntary disclosures of both records[68] and content[69] when necessary to investigate possible crimes in all currently addressed contexts. Therefore it would be inconsistent to limit voluntary cyber-crime disclosures to just records.

V. THE NETWORK CONTROL PROCEEDINGS SHOULD BE HARMONIZED

In the spirit of the Digital Due Process Coalition, this paper proposes to simplify, clarify, and unify the Network Control Proceedings in a manner that provides clarity for the laws that govern ISP responsibilities, protects the privacy of their subscribers, and serves the needs of law enforcement. The goal is to give ISPs, customers and LEAs a fair balance of rights and responsibilities when dealing with crime on ISP networks.

A. Clarify The Reasonable Network Management Standard

The FCC should clarify that the reasonable network management standard protects only acts of network control that relate directly to network management. Measures against unwanted content are best left to other laws. In particular, websites dedicated to infringing activities should be governed by COICA, where the drastic alternative of blocking would occur only under the judicial supervision of due process.

Clarification is also needed to resolve the policy conflict of user-initiated encryption. The FCC should declare that while customers should be generally free to use applications of their choice, including strong encryption programs, that freedom should not extend to home-made encryption tools designed to evade lawful surveillance. Otherwise the Internet would effectively place criminals above the law by enabling them to communicate their schemes beyond the reach of the criminal justice system.

B. Permit COICA Website Blocking Only in Narrow Circumstances Under Due Process

ISPs have nearly all the control they need to fight crime on their networks. They may access communications in transit to protect their rights and property from cyber-attacks, cyber-fraud, and related matters such as spam. They may also access stored content and records related to crime under a wide variety of circumstances.

One type of ISP control that remains unclear is the power to block infringing websites. COICA would require an ISP to block infringing sites pursuant to court order. The

---

[68] 18 U.S.C. § 2703(c).
[69] 18 U.S.C. §§ 2703(c), 2511(3)(b)(iv).

danger of such a law, as noted above, is with the terms of "infringing" and "reasonable measures." This paper does not attempt to improve on the definitions already set forth in the bill. However, care should be taken to adopt terms that strictly limit the blocking activity to unlawful sites. Otherwise the legislation may effectively erode the FCC principle of customer choice and permit the kind of unaccountable technologies and practices tolerated under the Technical Assistance Clause.

COICA should also ensure that ISP site blocking occurs only pursuant to due process. That would ensure that only illegal sites are blocked and avoid claims of unauthorized interception.

Finally, if COICA becomes law ISPs should review their privacy statements to ensure they cover the COICA blocking obligations. An update to the privacy statement may be needed to comply with the FCC Order's transparency rule.

C. Prioritize CALEA Technical Support for Lawful Surveillance

CALEA II could be reconciled with the other Network Control Proceedings simply by fulfilling the goals of the original CALEA statute. Specifically, CALEA should be given primacy over the Technical Assistance Clause. Service providers subject to CALEA should not be subject to additional technical assistance mandates.

That one change could reduce confusion over LEA assistance obligations, help level the regulatory playing field, provide better quality assistance to LEAs, and improve privacy protection consistent with ECPA II. In particular, the renewed focus on CALEA would promote safe harbor solutions. Those solutions would insulate providers from liability. They would be more likely to give LEAs meaningful data. And they could be reviewed to guard against undue infringements on privacy.

The Technical Assistance Clause could still be valuable in two scenarios. First, the non-CALEA Clause could apply to service providers not subject to CALEA or CALEA II. Second, the Clause could apply where a CALEA-covered entity is subject to an enforcement action under CALEA Section 108, and an LEA must use alternate technologies to compensate for the lack of compliance.[70]

The impact of the instant proposal on ISPs would depend on their current CALEA compliance status. Those that already comply with CALEA would encounter no further burdens and would gain the competitive benefit of a level playing field as more covered entities comply. Non-compliant ISPs would have to bring their networks into compliance but they too would receive key benefits. They would shed the double burden of technical assistance to LEAs and satisfy customers concerned with public safety and privacy.

---

[70] 47 U.S.C. § 1007.

D. Permit Disclosures of Both Records and Content to Combat Cyber-Attacks and Cyber-Fraud

As noted above, ISPs enjoy a variety of rights of disclosure to report criminal activity on their networks. ECPA II would supplement those laws with a right of voluntary disclosure to LEAs as needed to combat cyber-attacks and cyber-fraud. Such an enhancement would fortify the sagging defenses of the old rights and property clause. However, the proposed right would extend only to records.

ECPA II would be more consistent with the exiting ECPA disclosure laws if it would permit disclosures of both records and content. A broader disclosure right would also fit better with the FCC Order. That decision did not distinguish between records and content when addressing cyber-attacks.

Admittedly, content tends to reveal more personal information than mere records. Nevertheless, the nature of cyber-attacks and cyber-fraud appears to warrant the broader approach to disclosure. These cyber-crimes are uniquely elusive and damaging, making the disclosure of content in these situations a public safety necessity. In cases where the suspicious string of packets is encrypted, it may not be possible for an ISP to separate records from content. Moreover, disclosures that stop cyber-fraud could produce a large net gain in privacy protection, considering the privacy harm threatened by that particular crime. In any event, LEAs would gain no more authority from the broader approach because the disclosures would be voluntary, not compelled by due process.

VI. PROPOSED PROVISIONS TO HARMONIZE THE NETWORK CONTROL PROCEEDINGS

One of the recommendations in the previous section was to clarify the terms of CALEA implementation. Another was to grant ISPs a broad right of voluntary disclosure when faced with cyber-attacks and cyber-fraud. The following suggests certain legislative language to achieve these ends.

A. Language Promoting CALEA Compliance for Lawful Surveillance

The proposed CALEA fix could be legislated as shown in the following redline edit:

§ **2518**. Procedure for interception of wire, oral, or electronic communications

(4)(e) …

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the

services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.; except that if such provider of wire or electronic communication service, landlord, custodian or other person is subject to Chapter 9, Title 47 of the United States Code, such information, facilities and technical assistance shall be furnished solely pursuant to Chapter 9, Title 47 of the United States Code. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

B. Language Authorizing Broad Disclosures for Cyber-Attacks and Cyber-Fraud

The proposed right of voluntary disclosure could be established with minimal edits to ECPA as shown in the following redline draft:

§ **2702**. Voluntary disclosure of customer communications or records

….

(b)(5) as may be necessarily incident to the rendition of the service, ~~or to~~ the protection of the rights or property of the provider of that service, or to protect against cyber-attacks or cyber-fraud;

….

(c)(3) as may be necessarily incident to the rendition of the service, ~~or to~~ the protection of the rights or property of the provider of that service, or to protect against cyber-attacks or cyber-fraud;

Of course, legislative drafters would need to supply formal definitions for the terms “cyber-attack” and “cyber-fraud.”

VII. CONCLUSION

This paper began with the question, how should an ISP respond to a dangerously high volume of traffic on its network? To answer this question, the Network Control Proceedings offer helpful guidance. Each Proceeding is somewhat inconsistent with the others. Yet if the initiatives are properly harmonized, they could help defend against ISP-related crime without frustrating any of the interests involved. The following illustrates how the harmonized plan could work.

At the sign of a possible cyber-attack, an ISP could analyze the suspicious packets as appropriate to diagnose the network threat. The service provider may also notify the appropriate LEA, voluntarily disclosing both the records and content involved.

Based on the ISP's voluntary disclosure of content, the LEA may discover e-mails that reveal evidence of cyber-fraud, such as a phishing scheme. The LEA might then ask a court for an order to intercept the criminal suspect's communications.

Assuming the court order is granted, the LEA would serve it on the ISP. The ISP would then provision the required surveillance, giving the LEA nothing more or less than the CALEA-required content and CII for the communications specified in the order.

The lawful surveillance may indicate the suspect is not a lone wolf but an associate in a cyber-crime ring. Further legwork after the surveillance may indicate the gang runs a website dedicated exclusively to the sale of pirated films. A thorough visit to the website could confirm that hunch. Then the LEA could return to the judge for an order to have the infringing site blocked. If the order is granted, the LEA would serve it on the ISP and the ISP would implement the block.

It is difficult to craft criminal laws, especially those involving the complex and competing demands of the Internet. ISPs must manage their network traffic. LEAs sometimes require information from that traffic to protect public safety. And customers need privacy when exchanging traffic. No single one of these interests can expect to overcome the others. Still, with a little coordination among lawmakers, they could strike a fair balance for all.

Should readers have any comments on this white paper, please direct them to Joel M. Margolis at joel.margolis@subsentio.com.

About Subsentio

A Trusted Third Party, Subsentio, Inc. is a key partner with both service providers and law enforcement agencies. The company specializes in the professional design, application, and testing of lawfully authorized electronic surveillance solutions for wireless, cellular, Internet, and VoIP service providers. Based in Centennial, Colorado, Subsentio promptly provisions court orders for clients in the national, regional, and rural service provider markets. Further information may be found at www.subsentio.com.

About Joel M. Margolis

Joel M. Margolis is the owner of CALEA Consulting, LLC. The firm provides advice on federal legislative and regulatory mandates governing the law enforcement assistance obligations and related privacy requirements of telecommunications carriers, Internet service providers, and VoIP providers.

Joel has 26 years of government affairs expertise in communications law, including lengthy backgrounds in both industry and government. Most recently, he was a Senior Director at Neustar, Inc., where he headed the legal and policy functions of a business unit that supplied service providers with lawful surveillance solutions, records production solutions, and related compliance programs. Prior to that he served as Assistant Deputy Chief Counsel of the Drug Enforcement Administration in the Department of Justice. There he was DEA's delegate to certain DOJ working groups which formed the positions of U.S. law enforcement on issues of communications law. Previously he was the Senior Regulatory Counsel of Nextel Communications, Inc. He represented Nextel in rulemaking proceedings before the Federal Communications Commission and developed the company's compliance programs for federal mandates such as CALEA (lawful surveillance), E911 (emergency calling) and CPNI (subscriber privacy).

Joel has written on communications industry obligations to assist law enforcement and related issues of subscriber privacy. He often appears as a panelist at industry conferences where the above issues are explored.

Joel received his Juris Doctor degree from American University. He is a member of the bars of the District of Columbia and Maryland.