Navigating Communications Regulation in the Wake of 9/11

Jamie S. Gorelick*

John H. Harwood II**

Heather Zachary ***

* Jamie Gorelick is a partner at Wilmer Cutler Pickering Hale and Dorr LLP. She is Co-Chair of the Defense, National Security and Government Contracts Department, having previously served as a member of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), as Deputy Attorney General of the United States and as General Counsel of the Department of Defense.

** John Harwood is also a partner at Wilmer Cutler Pickering Hale and Dorr LLP. Mr. Harwood is Chair of the Communications and E-Commerce Department of the firm.

*** Heather Zachary is an associate at Wilmer Cutler Pickering Hale and Dorr LLP in the Communications and E-Commerce Department of the firm.

The Authors thank Samir Jain, Ronald I. Meltzer, and Randolph D. Moss, all partners at Wilmer Cutler Pickering Hale and Dorr, for their substantial contributions to, and valuable comments on, drafts of this Article.

In no industry has the impact of the events of September 11, 2001 ("9/11") been felt more strongly than in the communications industry. After 9/11, as the American people demanded a greater sense of security, Congress and the executive branch agencies reacted with new laws, new regulations, and new practices designed to protect our nation's critical communications infrastructure and enhance the ability of law enforcement

and intelligence agencies to investigate those who would do us harm.

The U.S. communications industry has long been a partner of the government in its efforts to carry out appropriate governmental functions, so long as communications providers could do so consistent with their responsibilities to customers and to shareholders. That partnership, based upon rules developed over decades, has been strained by the vast changes since 9/11. In the few years since the attacks of that day, the industry has had to digest innumerable new and untested obligations. At the same time, the government has struggled to develop procedures for addressing the legitimate privacy and other concerns implicated by its new powers. The reach of these changes—from new authorities to demand customer information, to more stringent scrutiny of proposed mergers—has affected nearly every aspect of a communications provider's daily work. The review that follows attempts to look across the regulatory environment at the scope of these changes to identify the issues that have arisen for both the government and industry participants.

I. THE GOVERNMENT'S ENHANCED SURVEILLANCE AUTHORITY

Through the Patriot Act[1] and other post-9/11 legislation, Congress substantially expanded the government's powers to conduct electronic surveillance and obtain information about users of communications services. All providers of communications services are receiving requests for assistance, including demands for information about their customers, that are far greater in number and scope than in the past. These changes present burdens as well as questions about the standards that law enforcement agencies must meet in order to demand assistance or information, and about the scope of the information that law enforcement may obtain. And these questions in turn leave communications providers open to possible liability and the risk of harm to their relationships with their customers.

A. Changes to the Surveillance Statutes

Title III of the 1968 Omnibus Crime Control and Safe Streets Act ("Title III")[2] grants the government authority to intercept the *content* of telephone or electronic communications only in narrowly defined circumstances. The government's right to obtain addressing and other *noncontent* information relating to communications subject to Title III is

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001) (codified at scattered sections U.S.C.) ("Patriot Act").

2. 18 U.S.C. §§ 2510–22 (Supp. 2002).

regulated by the Pen Registers and Trap and Trace Devices chapter of Title 18 ("Pen/Trap Statute").[3] The Electronic Communications Privacy Act ("ECPA")[4] governs disclosure of *stored* electronic communications.[5] Finally, the Foreign Intelligence Surveillance Act of 1978 ("FISA")[6] governs surveillance for foreign intelligence-gathering purposes.

The Patriot Act and other post-9/11 legislation expanded the government's surveillance powers through amendments to each of these statutes. Those amendments (1) expand the scope of the surveillance statutes to reach new communications providers, (2) enlarge the statutes' coverage to include new surveillance targets, (3) lower the threshold that the government must meet in order to engage in domestic and foreign intelligence surveillance, (4) and allow communications providers to submit voluntarily to government surveillance in limited situations. We discuss each of these developments in turn.

1. Application to New Providers

Although the surveillance statutes on their face encompass nearly all forms of wire and electronic communications,[7] before the Patriot Act some cable Internet providers argued that they were barred by the Cable Communications Policy Act ("Cable Act")[8] from cooperating with law

3. *Id.* §§ 3121–27. A traditional pen register device is attached to a copper telephone line and records the outgoing telephone numbers "dialed or otherwise transmitted" by the target. 18 U.S.C. § 3127(3) (2000). Similarly, a trap and trace device records the telephone numbers of calls received by the target. *Id.* § 3127(4). Although traditional pen registers and trap and trace devices are used only for telephone calls, they have analogues with respect to Internet communications. A device that reads the header information of emails or the routing information of other computer-to-computer communications is referred to as a pen/trap device. COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS at IV.C (July 2002), *at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm [hereinafter DOJ MANUAL]. *See also* 18 U.S.C. § 3127(3)–(4) (Supp. 2002) (incorporating such devices into the statutory definitions of "pen register" and "trap and trace device"). We use the term "pen/trap device" to refer to all three types of devices.

4. *See* 18 U.S.C. §§ 2701–12 (Supp. 2002).

5. Communications that are in "electronic storage" at an "electronic communication service" or held by a "remote computing service" are subject to the protections of ECPA. *Id.* § 2702(a). Such communications include stored email, computer data, and electronic images.

6. *See* 50 U.S.C. §§ 1801–62 (Supp. 2002).

7. *See, e.g.*, 18 U.S.C. § 2510(1) (Supp. 2002) (defining "wire communications" under Title III to include "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception"). Title III contains a similarly broad definition of electronic communications. *See id.* § 2510(12).

8. 47 U.S.C. § 551 (2000).

enforcement requests for surveillance assistance.[9] In its original form, the Cable Act precluded cable providers from giving the government "personally identifiable information" about cable subscribers except after notice to the subscriber and an opportunity for an in-court adversarial hearing.[10] After 9/11, the Cable Act was amended to clarify that cable providers are subject to the surveillance statutes.[11] In addition to opening cable television and cable Internet providers to surveillance requests, this amendment also brings other communications companies within the scope of the surveillance statutes, including Web TV providers and any other provider that structures its business in such a way as to qualify as a "cable operator" under Title VI of the Communications Act.[12]

2. New Classes of Surveillance Targets and Increased Access to Information

Congress coupled its application of the surveillance statutes to new communications providers with an expansion of the substantive reach of those statutes. Recent amendments have expanded the government's power under certain statutory provisions to obtain documents and specific details about a surveillance target's communications. Other statutory changes permit the government to pursue new classes of surveillance targets for both foreign intelligence and domestic law enforcement purposes.

The post-9/11 amendments clarify that the Pen/Trap Statute applies to a wide range of communications technologies, not just telephone communications.[13] They confirm that the government may intercept

9. *See* DOJ MANUAL, *supra* note 3, at III.G.3 (noting that "[s]ome cable companies asserted that the stringent disclosure restrictions of the Cable Act governed not only their provision of traditional cable programming services, but also their provision of Internet and telephone services").

10. 47 U.S.C. § 551(h) (2000).

11. Patriot Act § 211, 47 U.S.C. § 551 (Supp. 2002). Now the Cable Act's restrictions apply only to government requests for information about the cable television programming a customer purchases, such as "pay-per-view" movies. *See id*. § 551(c)(2) (providing that a cable provider may release personally identifiable information about a subscriber "if the disclosure is . . . to a government entity as authorized under chapters 119 [Title III], 121 [ECPA], or 206 [Pen/Trap Statute] of Title 18, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator").

12. *Id.* § 522(5) (defining "cable operator").

13. *See* Patriot Act § 216, 18 U.S.C. §§ 3121(c), 3123, 3124, 3127 (Supp. 2002). Even before the Patriot Act, the government sometimes used the Pen/Trap Statute to obtain information about communications on computer networks, but no federal district or appellate court had explicitly ruled on the propriety of this practice. *See* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS), FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Apr. 6, 2005).

addressing information in Internet communications under the same standard that applies to collection of routing information for traditional phone calls.[14] The government now may install software in addition to mechanical pen/trap devices.[15] This permits the government to use "packet sniffer" programs that extract information about a surveillance target's Internet communications.[16]

The amount of basic subscriber information obtainable through an administrative subpoena under ECPA has expanded.[17] Under prior law, the government could obtain a surveillance target's name, address, telephone billing records, telephone number, and length and type of service.[18] Now it may obtain as well the means and source of payment that a surveillance target uses to pay for an account, including the target's credit card or bank account number.[19] It also may obtain records of the target's session times and durations[20] and any network address temporarily assigned to the target.[21] Similarly, under FISA, the government now may require any person or company to produce "any tangible thing[]," including books, papers, or documents,[22] and is no longer limited to business records held by a small class of companies.[23]

New categories of surveillance targets also have been added. Title III always has required the government to demonstrate probable cause to believe an individual "is committing, has committed, or is about to

14. The Pen/Trap Statute originally permitted the government to obtain only "electronic or other impulses which identify the numbers dialed or otherwise transmitted" on a telephone line or "incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C. § 3127(3)–(4) (2000). The government now may obtain "dialing, routing, addressing, or signaling information" so long as such information does not include the contents of the communication. 18 U.S.C. § 3127(3) (Supp. 2002). In addition, references in the Pen/Trap Statute to a "line" were amended to state "line or other facility." *See, e.g.*, 18 U.S.C. §§ 3123–24 (2000 & Supp. 2002).

15. *See, e.g.*, 18 U.S.C. § 3121(c) (Supp. 2002). The Pen/Trap Statute initially defined a pen register or a trap and trace device simply as "a device." 18 U.S.C. § 3127(3)–(4) (2000). Now the statutory definition includes "a device or process." 18 U.S.C. § 3127(3)–(4) (Supp. 2002).

16. *See* discussion of packet sniffer programs *infra* Part I.B.2.

17. *See* Patriot Act § 210, 18 U.S.C. § 2703(c)(2) (Supp. 2002).

18. 18 U.S.C. § 2703(c)(1)(C) (2000).

19. 18 U.S.C. § 2703(c)(2)(F) (Supp. 2002).

20. *Id.* § 2703(c)(2)(C).

21. *Id.* § 2703(c)(2)(E).

22. Patriot Act § 215, 50 U.S.C. § 1861(a)(1) (Supp. 2002).

23. Under the prior version of this section, the government was entitled to obtain "records" only from "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility." 50 U.S.C. § 1862(a), (b)(2), (d)(1) (2000).

commit" one of the predicate felony offenses listed in the statute.[24] Since 9/11, Congress has added many new crimes to the list of predicate offenses, including crimes related to terrorism,[25] computer fraud,[26] and biological weapons.[27] And while FISA still requires the government—when it seeks to obtain "foreign intelligence information" through electronic surveillance or a physical search—to show probable cause to believe that the target of surveillance is a "foreign power or an agent of a foreign power,"[28] this phrase now includes so-called lone wolf terrorists.[29] Now, any non-U.S. person who participates in activities related to international terrorism is deemed to be an "agent of a foreign power" under FISA.[30]

3. Lower Thresholds for Authorization

Amendments to the surveillance statutes also make it easier for the government to obtain information. Congress has lowered many of the standards that the government must satisfy in order to engage in domestic or foreign intelligence surveillance.

The government now has a reduced burden when seeking to obtain pen/trap orders under FISA.[31] Law enforcement may obtain an order for a pen/trap device in any investigation to protect against international terrorism or clandestine intelligence activities and may obtain information about the communications of even U.S. citizens so long as the investigation is not conducted solely on the basis of activities that are protected by the First Amendment.[32]

---

24. *See* 18 U.S.C. § 2518(3)(a) (requiring the government to relate its surveillance request to one of the crimes enumerated in 18 U.S.C. § 2516).

25. Patriot Act § 201, 18 U.S.C. § 2516(1) (Supp. 2002). These offenses include crimes of violence committed against Americans overseas, *id*. § 2332, multinational terrorism, *id.* § 2332b, and providing material support to a terrorist, *id.* § 2339A.

26. Section 202 of the Patriot Act added felony violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, to the list of predicate offenses. Patriot Act § 202, 18 U.S.C. § 2516(1)(c) (Supp. 2002).

27. These offenses were added in the recently passed Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6907, 118 Stat. 3638, 3774 (2004) (to be codified at 18 U.S.C. § 2516(1)) ("Intelligence Reform Act").

28. *See, e.g.*, 50 U.S.C. § 1805(a)(3) (2000 & Supp. 2002).

29. Intelligence Reform Act § 6001 (amending 50 U.S.C. § 1801(b)(1) (Supp. 2002)). *See generally* ELIZABETH B. BAZAN, INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: "LONE WOLF" AMENDMENT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Cong. Research Serv., Report for Congress, 2004), *at* http://www.fas.org/irp/crs/RS22011.pdf (discussing implications of amendment).

30. Intelligence Reform Act § 6001 (to be codified at 50 U.S.C. § 1801(b)(1)(C)).

31. Patriot Act § 214, 50 U.S.C. § 1842 (Supp. 2002).

32. 50 U.S.C. § 1842(a)(1) (Supp. 2002); *id.* § 1842(c)(2) (requiring applications for pen/trap orders to contain "a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is

Two other provisions also have been changed to this lower standard. Under ECPA, the Federal Bureau of Investigation ("FBI") may, simply by sending a "national security letter" to a communications provider,[33] compel disclosure of a surveillance target's transactional records and personally identifiable information.[34] The newly amended statute requires the FBI to certify only that the requested information is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and that no U.S. person has been targeted solely on the basis of activities protected by the First Amendment.[35] And under FISA the government may obtain physical access to business records by making the same showing.[36]

The government now has a lower threshold to meet when it seeks to obtain the content of a surveillance target's voicemail as well. Previously, access to electronically stored wire communications, including voicemail, fell under Title III,[37] which required a showing that, among other facts, normal investigative procedures had been tried and had failed or appeared to be too dangerous.[38] Under the recent amendments, access to voicemail

relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"). The monitored communications no longer must be of an individual thought to be engaged in such activities, nor must the activities potentially violate U.S. or other criminal laws. 50 U.S.C. § 1842(c)(2)–(3) (2000).

33. Patriot Act § 505, 18 U.S.C. § 2709 (Supp. 2002).

34. Those records include a customer's "electronic communication transactional records," 18 U.S.C. § 2709(a) (Supp. 2002), and his or her "name, address, length of service, and local and long distance toll billing records," *id.* § 2709(b)(1).

35. *Id*. § 2709(b)(1). The FBI no longer must certify that it has reason to believe either that the information sought pertains to a person or entity that is a foreign power or an agent of a foreign power or that communications facilities registered in the name of that person or entity have been used to communicate with someone engaged in international terrorism or clandestine intelligence activities. *Compare id. with* 18 U.S.C. § 2709(b)(1)–(2) (2000). We discuss below the holding of a federal court in New York that this provision is unconstitutional. *See infra* Part I.B.2.

36. 50 U.S.C. § 1861(a)(1) (Supp. 2002); *see also id.* § 1861(a)(2)(B), (b)(2). Prior to the amendment, the government was entitled to access business records upon a showing of specific facts giving it reason to believe that the records sought pertained to a person who was a foreign power or an agent of a foreign power. 50 U.S.C. § 1862(b)(2) (2000).

37. 18 U.S.C. § 2510(1) (2000). The definition of wire communications included "any electronic storage of such communication." *Id.*

38. *See id.* § 2518(3)–(5) (providing that the government may intercept the contents of a communication only after showing, in an application for a court order, that (1) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"; (2) there is probable cause to believe that that the communication facility subject to surveillance is being used in a crime or that the facility is "leased to, listed in the name of, or commonly used by" the target of the surveillance; and (3) the surveillance will be conducted in a way that minimizes the interception of

may be obtained pursuant to the less demanding standards of ECPA,[39] through a traditional search warrant supported by a showing of probable cause.[40] Similarly, under FISA, the collection of foreign intelligence information now need be merely "a significant purpose" and not "the purpose" of requested surveillance.[41]

The surveillance statutes now contain streamlined procedures facilitating the government's surveillance efforts. The government is entitled to nationwide service of court orders and search warrants issued pursuant to ECPA[42] and the Pen/Trap Statute.[43] Under the new amendments, a federal court with jurisdiction over the crime being investigated has authority to issue orders and search warrants that are valid anywhere within the United States.[44] Similarly, recognizing that likely targets of investigations may frequently change communications providers to avoid surveillance, Congress amended FISA and the Pen/Trap Statute to permit the issuance of generic surveillance orders that can be served on any third party needed to assist with surveillance.[45]

Finally, the government now has additional means of persuading

communications that do not provide evidence of a crime).

39. Section 209 of the Patriot Act removed voicemail from Title III and made it subject to ECPA instead. *See* Patriot Act § 209, 18 U.S.C. §§ 2510, 2703 (Supp. 2002).

40. Patriot Act § 209, 18 U.S.C. § 2703(a)–(b) (Supp. 2002). Investigators face an even lower burden when obtaining voicemail that an intended recipient already has opened. DOJ MANUAL, *supra* note 3, at III.D.4.

41. Patriot Act § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)). A specially convened appeals court recently held that the government probably had such power even before the Patriot Act amended the statute. *See In re* Sealed Case, 310 F.3d 717, 723 (F.I.S. Ct. Rev. 2002) (noting that "it is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents . . . . It does not seem that FISA, at least as originally enacted, even contemplated that the FISA court would inquire into the government's purpose in seeking foreign intelligence information.").

42. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A) (Supp. 2002) (providing that search warrants or court orders for content and customer records can be issued by any court "with jurisdiction over the offense under investigation").

43. *Id.* § 3123(a)(1). *See also id.* § 3127(2). Previously, the reach of such court orders and search warrants was limited by the jurisdiction of the court issuing them. *See, e.g.*, 18 U.S.C. § 3123(a) (2000) (Pen/Trap Statute); *id.* § 2703(a), (b), (c)(1)(B) (ECPA).

44. *See* 18 U.S.C. § 3123(a)(1) (Supp. 2002); *id.* § 3122(a); *id.* § 2703(a), (b)(1)(A), (c)(1)(A).

45. *See* Patriot Act § 206 (amending FISA, 50 U.S.C. § 1805(c)(2)(B) (2000)); *id.* § 216 (amending the Pen/Trap Statute, 18 U.S.C. § 3123(a) (2000)). Under the prior regime, the government was required to obtain a new order whenever a surveillance target changed phone companies. FISA required the government to specify the location of the surveillance and provided only for orders directing a "specified" communications carrier to assist with a surveillance request. *See* 50 U.S.C. § 1805(c)(1)(B), (c)(2)(B) (2000). Similarly, the applicable section of the Pen/Trap Statute did not provide for roving surveillance. *See* 18 U.S.C. § 3123(a) (2000).

communications providers to comply with surveillance requests. The surveillance statutes contain "safe harbors" designed to protect carriers that comply with requests. These provisions generally absolve carriers of liability to the extent that they act in "good faith reliance on" an authorization such as a search warrant or court order.[46] They also provide, for example, that "[n]o cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter."[47] Although these provisions have always existed, recent amendments have expanded their scope to reach new situations. ECPA's safe harbor provision now applies to a provider's actions in complying with government evidence-preservation requests.[48] Similarly, the Pen/Trap Statute now conveys statutory immunity when a provider complies with a pen/trap "order," rather than the express "terms of" such an order.[49]

4. Expanded Voluntary Disclosure

Amendments to the surveillance statutes have added to the circumstances in which communications providers may voluntarily disclose information to law enforcement. One of these is the "computer trespasser" exception.[50] Under this provision, victims of computer attacks may authorize the government to intercept the wire or electronic communications of a computer trespasser that are sent to, through, or from

46. "A good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization" is a complete defense to an ECPA violation or "any civil or criminal action brought under . . . any other law." 18 U.S.C. § 2707(e) (Supp. 2002). The other surveillance statutes contain similar provisions. *See, e.g.*, *id.* § 2520(d)(1) (Title III); *id.* § 3124(e) (Pen/Trap Statute).

47. *Id.* § 2703(e). Nearly identical provisions appear in the other surveillance statutes. *See, e.g.*, *id.* § 2511(2)(a)(ii) (Title III); *id.* § 3124(d) (Pen/Trap Statute).

48. *Id.* § 2707(e)(1) (referring to 18 U.S.C. § 2703(f), which sets out a procedure whereby the government can direct a provider to preserve evidence until a court order can be obtained).

49. *Id.* § 3124(d) (providing that "[n]o cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title").

50. A "computer trespasser" is defined as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer." 18 U.S.C. § 2510(21)(A) (Supp. 2002). Section 217 of the Patriot Act amended Title III to provide for this new exception. *See* Patriot Act § 217 (amending 18 U.S.C. §§ 2510-11 (2000)).

the victim's computer.[51] Another new voluntary disclosure exception permits communications providers to divulge customer records to the government (or any other entity) when necessary to protect the rights or property of the provider.[52] Yet another permits communications providers to disclose customer records or the contents of a communication to any governmental entity in emergency situations when the provider reasonably believes that there is an immediate danger of death or serious physical injury if the information is not disclosed. [53] Through these exceptions, a communications provider may offer information to the government even in the absence of any other statutory authorization.

B. Effects on Communications Providers

These enhancements to the government's surveillance authority present a variety of challenges and risks for communications providers. Many of the amendments introduce additional complications into already complex statutes, making it more difficult for providers to discern what their obligations are. And missteps may harm providers' reputations and could lead to civil damages and even other sanctions.

1. Practical Consequences of the Government's Enhanced Surveillance Powers

Because the surveillance statutes now clearly apply to cable providers,[54] many cable television, cable Internet, and other cable system-based communications providers are facing surveillance requests for the first time. And providers that have previously dealt with such requests are now facing government demands for assistance that are more frequent and

51. *Id.* § 2511(2)(i). *See also* R.J. Cinquegrana and Richard M. Harper II, *The USA PATRIOT Act: Effects on American Employers and Businesses*, 46 BOSTON BAR J., May–June 2002, at 12 [hereinafter BOSTON BAR JOURNAL].

52. *See id.* § 2702(c)(3) (ECPA). Although this is a new voluntary exception, communications providers already had authority to disclose the *contents* of a communication if necessary to protect the rights or property of the provider. *Id.* § 2702(b)(5).

53. Section 212 of the Patriot Act amended section 2702 of ECPA to permit disclosure of certain communications in emergency situations. *See* 18 U.S.C. § 2702(b)(6)(C) (Supp. 2001). Section 2702 was later amended by the Homeland Security Act; it now permits a communications provider to disclose the content of a communication "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8) (Supp. 2002). Similarly, customer records may be disclosed under ECPA "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." *Id.* § 2702(c)(4).

54. 47 U.S.C. § 551(c)(2) (Supp. 2002).

broader in scope than ever before.[55]

The increased number and scope of surveillance requests has necessitated an increase in the capacity and capability of communications networks. This raises the contentious question of who pays for such network modifications.[56] Similarly, aiding the government with individual surveillance requests is expensive. A report by the Director of the Administrative Office of the United States Courts states that the average cost of a Title III wiretap in 2003 was $71,625.[57] Although companies can seek reimbursement of the amounts expended in assisting the government,[58] the process is administratively burdensome and the amount paid as compensation often does not capture the full costs of assisting with wiretaps and other types of surveillance.[59] Government surveillance requests issued under FISA may be handled only by employees who have successfully undergone a background check by the FBI and who carry a

55. In 2003, the FISA court approved 1724 applications for electronic surveillance and/or physical searches, a 40 percent increase over the preceding year. *Compare* Letter from William E. Moschella, Assistant Attorney General, to L. Ralph Mecham, Director of the Administrative Office of the United States Courts (Apr. 30, 2004), *available at* http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf *with* Letter from John Ashcroft, Attorney General, to L. Ralph Mecham, Director of the Administrative Office of the United States Courts (Apr. 29, 2003), *available at* http://www.fas.org/irp/agency/doj/fisa/2002rept.pdf [hereinafter 2002 FISA Report] (stating that the FISA court approved 1228 applications). In 2002, the FISA court approved 1228 applications for electronic surveillance and/or physical searches, a 31 percent increase over 2001. *Compare* 2002 FISA Report *with* Letter to J. Dennis Hastert, Speaker of the House of Representatives, from John Ashcroft, Attorney General (Apr. 29, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/2001rept.html (stating that the FISA court granted 934 applications in 2001). The number of non-FISA applications for federal wiretap orders rose 16 percent from 2002 to 2003. LEONIDAS RALPH MECHAM, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS, at 5 (Apr. 2004), *available at* http://www.uscourts.gov/wiretap03/2003WireTap.pdf [hereinafter 2003 WIRETAP REPORT]. The year before, the number of federal wiretap authorizations increased by 2 percent. *Id.* at 32, tbl. 7. These non-FISA wiretap reports do not contain information about other methods of surveillance, such as physical searches or installations of pen/trap devices.

56. *See infra* Part II.B.5 for a discussion of this issue.

57. 2003 WIRETAP REPORT, *supra* note 55, at 11.

58. 18 U.S.C. § 2518(4) (Supp. 2002) (Title III); *id.* § 3124(c) (Pen/Trap Statute); *id.* § 2706(a) (ECPA).

59. *See* The Comm. Assistance for Law Enforcement Act and Broadband Access and Servs., *Comments of CTIA—The Wireless Association*, ET Dkt. No. 04-295, at 18–21 (Nov. 8, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516793514 (asserting to the FCC that "[t]he government would have the Commission reduce the reimbursement obligation to a mere line charge, as if technical assistance simply involved activating another phone" and explaining that carriers are generally paid a flat rate that may not take into consideration all of the rules that impose financial burdens on communications providers).

current National Security Clearance.[60] The increase in surveillance requests has, therefore, required companies to hire more security-cleared employees.

Because the amendments to the surveillance statutes are far-reaching and complicated, they also require companies to revise their procedures for responding to surveillance requests. And the government's increased power to compel disclosure of information has also required companies to modify their privacy policies.[61] This is especially true of providers offering services over cable, because the Cable Act amendments reduced the level of privacy expected by cable subscribers. Policy changes are not likely to be popular with customers, but the serious consequences of violating established privacy policies make them necessary.[62]

2. Considerations When Responding to Government Surveillance Requests

In responding to government surveillance requests, companies try to be responsible corporate citizens. But the challenges they face—in customer concern and otherwise—are substantial. In particular, it is often difficult for providers to distinguish between content and noncontent information in the context of Internet communications, making it hard for them to determine how much information they must disclose. The safe harbor provisions in the surveillance statutes protect carriers from liability when they offer the government information beyond that which is lawfully called for, if they do so "in accordance with" or in "good faith reliance on" a court order or other type of authorization.[63] But if an order does not

60. 50 U.S.C. § 1802(a)(4)(B) (Supp. 2002); *see also* A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow"*, 1996 U. CHI. LEGAL F. 15, 41 (1996) (explaining that "federal law requires that telephone companies have someone on their staff with a SECRET clearance to receive and comply with FISA court-ordered wiretaps" (emphasis in original)).

61. *See, e.g.*, Doe v. Ashcroft, 334 F. Supp. 2d 471, 494 n.118 (S.D.N.Y. 2004) (noting that compliance with the amended national security letter provision is problematic for some communications providers because they have "contractually obligated themselves to protect the anonymity of their subscribers").

62. For example, a number of angry JetBlue customers filed a lawsuit after learning that the airline breached its own privacy policy by giving five million passenger itineraries to a defense contractor for use in developing passenger profiles used to identify possible terrorism suspects. Annie I. Anton et al., *Inside JetBlue's Privacy Policy Violations*, IEEE SECURITY & PRIVACY, Nov.–Dec. 2004, *available at* http://www4.ncsu.edu/~qhe2/publications/jetblue_ieee_sp04.pdf.

63. *See, e.g.*, 18 U.S.C. § 3124(d) (Supp. 2002) (providing that "[n]o cause of action shall lie in any court against any provider of a wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with a court order"); *id.* § 2707(e) (immunizing providers who act in "good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization").

clearly reach particular information, the communication provider's good faith must be reasonable under the circumstances.[64] There also are other consequences that carriers cannot protect themselves against through reliance on the safe harbor provisions alone. Even futile lawsuits premised on a provider's violation of the surveillance statutes or its own privacy policy are costly and inconvenient to defend. And a provider viewed as not protecting customer privacy also will suffer damage to its reputation and customer relationships.

Although the meaning of "content" is usually obvious with respect to conventional telephone conversations, its meaning is not clear in the context of human-to-computer communications. When surfing the Internet, a person "sends commands to his computer directing it to send commands to the host computer, asking the host to send back packets of data that will be assembled by his computer into a web page."[65] Such a command can be viewed in two different ways: "either the command is the 'content' of the communication between the user and his computer or it is merely 'addressing information' that the user entered into his computer to tell the computer where it should go and what it should do, much like [a] pen register. . . ."[66] Because the recent amendments to the surveillance statutes do not shed light on which view is correct, communications providers responding to government requests are left to answer this question themselves.

Of course, ambiguities regarding what constitutes "content" are not new. Even ordinary digits dialed after a phone call has been connected can convey content.[67] When a target calls an automated banking system, the passwords and account numbers entered can be considered content.[68] Similarly, digits dialed into alphanumeric pagers often convey substantive messages to the recipient.[69] Citing such examples, the United States Court of Appeals for the District of Columbia Circuit has noted that it is still an open question whether the government must seek a Title III warrant to obtain such information.[70]

64. *See infra* note 81.

65. Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW.U. L. REV. 607, 646 (2003) [hereinafter *Big Brother*] (citations omitted).

66. *Id.*

67. United States Telecom Ass'n v. FCC (USTA), 227 F.3d 450, 462 (D.C. Cir. 2000). Such digits are called "post-cut-through dialed digits." *Id.*

68. *Id.*

69. *Id.* For example, when leaving an urgent message for a pager customer, a caller might enter the digits 911.

70. *See id.*

These issues are arising more frequently since 9/11. As discussed, the Patriot Act clarified that the Pen/Trap Statute applies to Internet communications. The government now may obtain "dialing, routing, addressing, or signaling information" so long as such information does not include the contents of the communication.[71] But Congress did not define what these terms mean in the context of Internet communications.[72] Critics contend that the websites a surveillance target visits might be viewed as falling within the scope of "dialing, routing, addressing, or signaling information," but they argue that such information constitutes "content" because the websites a person visits inevitably reveal something about the substance of the communication.[73]

Even if providing a list of the domain names that a target visits does not implicate content, a question arises as to how far down in a website's URL the government is entitled to look. For example, a visit to www.target.com might not reveal much, but a visit to www.aclu.org/contribute/contribute.cfm might show that the target made a contribution to the American Civil Liberties Union, and a visit to http://shopping.yahoo.com/p:Communist%20Manifesto:1979236207 could reveal that the target purchased a copy of the *Communist Manifesto* online. Another question is whether the government may collect the terms that a target enters into a search engine.[74]

Some guidance on the distinction between "contents" and "address information" can be found in 18 U.S.C. § 2510(8), which defines the

71. 18 U.S.C. § 3127(3)–(4) (Supp. 2002).

72. In debates on the Patriot Act, Senator Leahy chastised the FBI and the Department of Justice for failing to provide clear definitions of these terms, arguing that "[w]e should be clear about the consequence of not providing definitions for these new terms in the pen/trap device statutes . . . We are leaving the courts with little or no guidance of what is covered by 'addressing' or 'routing.'" 147 CONG. REC. S10990-02, S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). ECPA presents similar difficulties. That statute provides that the government need not have a search warrant to obtain "record[s] or other information pertaining to a subscriber to or customer of [a communications] service (not including the contents of communications)." 18 U.S.C. § 2703(c)(1) (Supp. 2002). Like the Pen/Trap statute, ECPA does not elaborate on what information about Internet communications falls within this category.

73. Susan W. Dean, *Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law under the Patriot Act*, 5 TUL. J. TECH. & INTELL. PROP. 97, 105 (2003) [hereinafter *Government Surveillance*]. Similarly, such information might qualify as "record[s] or other information pertaining to a subscriber to or customer of [a communications] service (not including the contents of communications)" under ECPA. 18 U.S.C. § 2703(c)(1) (Supp. 2002).

74. Center for Democracy and Technology, *Anti-Terrorism Act Expands Government Surveillance Authorities, Weakens Privacy Protection with No Clear Benefit to Security*, at 2 (Sept. 21, 2001), *available at* http://www.cdt.org/security/010921cdt.pdf.

meaning of "contents" for purposes of Title III.[75] And several cases that discuss the meaning of content with respect to traditional types of communications also shed light on its meaning in the context of Internet communications.[76] Nonetheless, these aids are helpful only to a limited extent, and it remains unclear exactly what is meant by "dialing, routing, addressing, or signaling information."[77]

Such ambiguity in the text of the statutes poses a potential problem for communications providers seeking to balance the privacy of their customers against law enforcement's demands for information. Some warrants and court orders issued to communications providers do not provide enough specificity about the types of information that the government is seeking. For example, an ECPA order might request that the provider turn over any "relevant routing information" or a pen/trap order might request all "dialing, routing, addressing, or signaling information."[78] In some circumstances, therefore, the communications provider will be left to decide for itself what information to hand over to the government.

A provider that discloses too much information in "good faith" should not face civil or criminal liability under the surveillance statutes.[79] As noted, the safe harbor provisions in those statutes protect communications providers by immunizing them from liability when they act in "good faith reliance on" a court order or other form of statutory authorization.[80] So long as providers make reasonable, good-faith efforts to separate content from other types of information, these provisions should be sufficient to

75. That section provides that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (Supp. 2002).

76. *See, e.g.*, Hill v. MCI, 120 F. Supp. 2d 1194, 1195–96 (S.D. Iowa 2000) (holding that "invoice/billing information and the names, addresses, and phone numbers of parties [Plaintiff] called" are not "contents" under Title III or ECPA); Gilday v. Dubois, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (holding that information about the identity of the caller, the number called, and the date, time, and length of a phone call are not "contents" under Title III). Very few cases discuss the meaning of content in the context of Internet communications, and even they are not particularly instructive. *See, e.g.*, Jessop-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (providing that an Internet service provider did not violate ECPA by revealing "basic identity information" about an account holder because such information did not constitute "content").

77. 18 U.S.C. § 3127(3)–(4) (Supp. 2002).

78. *See, e.g.*, DOJ MANUAL, *supra* note 3, at app. B (sample ECPA order).

79. Courts can impose severe sanctions for violations of the surveillance statutes. *See, e.g.*, 18 U.S.C. § 2520(b)–(c) (Supp. 2002) (providing for civil damages for Title III violations); *id.* § 2511(1), (4) (providing for criminal penalties under Title III); *id.* § 2707(b)–(c) (providing for civil damages for ECPA violations).

80. *See, e.g.*, *id.* § 2520(d)(1) (immunizing providers from Title III penalties if they demonstrate a "good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization").

protect them if they accidentally disclose too much information to the government. It merits emphasis that a provider must act reasonably. A provider's subjective good-faith belief that its actions are lawful is not enough to immunize it from liability.[81]

Even when they apply, the safe harbor provisions cannot protect a provider from the expense and nuisance of defending futile lawsuits brought by customers who complain that the provider has violated the surveillance statutes or its own privacy policy by disclosing the content of communications without authorization.[82] And a company viewed as careless with customer information will suffer harm to its reputation and position in the marketplace. Thus, providers may wish to take steps beyond the safe harbor provisions and seek to ensure that they are not disclosing content to the government when law enforcement is entitled only to addressing information.

Attempting to avoid these difficulties, a number of companies have outsourced the difficult task of isolating noncontent information. When faced with a pen/trap order for Internet routing information, some providers are giving the government permission to install packet sniffers that are specially designed to monitor Internet communications.[83] These devices

81. A court recently held that a provider's subjective good faith reliance on a search warrant is not enough to entitle the provider to protection under ECPA's safe harbor provision. Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 647–48 (E.D. Va. 2004). Rather, the provider must demonstrate that its reliance was objectively reasonable under the circumstances. *Id.*; *see also* Davis v. Gracey, 111 F.3d 1472, 1484 (10th Cir. 1997) (holding that, "[t]o be in good faith," law enforcement's reliance on a search warrant "must have been objectively reasonable"). Similarly, a number of courts have held that subjective good faith alone is not sufficient to immunize parties from liability under Title III. *See, e.g.*, Jacobson v. Rose, 592 F.2d 515, 523 (9th Cir. 1978) (holding that a telephone company is entitled to protection only if it "can demonstrate (1) that [it] had a subjective good faith belief that [it] acted legally pursuant to a court order; and (2) that this belief was reasonable").

82. The safe harbor provisions in the surveillance statutes likely protect communications providers from liability arising from violations of their privacy policies. For example, ECPA provides that "*[n]o cause of action* shall lie in any court against any provider . . . for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter." 18 U.S.C. § 2703(e) (Supp. 2002) (emphasis added). It also provides that "[a] good faith reliance on" certain types of lawful authorization "is a complete defense to any civil or criminal action brought under this chapter or any other law." *Id.* § 2707(e). These provisions cannot, however, prevent customers from filing suits arguing that the safe harbors should not apply because the provider did not act reasonably in complying with a government surveillance request.

83. In two recent reports to Congress, the government said that it had installed packet sniffers thirteen times in fiscal 2002 and 2003. *See* FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE, CARNIVORE/DCS 1000 REPORT TO CONGRESS, at 1 (Feb. 24, 2004), *available at* http://www.epic.org/privacy/carnivore/2002_report.pdf (stating that the FBI used packet sniffers on five occasions in fiscal year 2002); FEDERAL BUREAU OF

"tap" a line of Internet traffic at a particular point in the network and analyze each of the packets flowing through that location.[84] When law enforcement possesses a Title III order, a packet sniffer can be used to intercept the full content of a target's Internet communications.[85] By contrast, when the government is entitled only to pen/trap information, the packet sniffer can be set to ignore content and monitor only the addressing and routing information of the target's communications.[86] The government has employed different types of packet sniffers over the years. Originally, it used a device called Carnivore, which the FBI had developed.[87] More recently, the government has instead used commercially available packet sniffing products.[88]

There is a nascent debate about whether the use of packet sniffers is constitutional.[89] But for communications companies, the question whether

INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE, CARNIVORE/DCS-1000 REPORT TO CONGRESS, at 1 (Dec. 18, 2003), *available at* http://www.epic.org/privacy/carnivore/2003_report.pdf (stating that the FBI used packet sniffers on eight occasions in fiscal year 2003).

84. *Big Brother*, *supra* note 65, at 649.

85. *Id.* at 654, 656.

86. *See Government Surveillance*, *supra* note 73, at 111.

87. The FBI has stated that it used Carnivore about 25 times between 1998 and 2000. Ted Bridas, Associated Press, *FBI Stops Using Carnivore Wiretap Software* (Jan. 19, 2005), *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=57702375.

88. *See id.*; *see also* Kevin Poulsen, *FBI Retires Carnivore*, THE REGISTER, Jan. 15, 2005, *at* http://www.theregister.co.uk/2005/01/15/fbi_retires_carnivore/.

89. *See, e.g.*, Robert Berkowitz, *Packet Sniffers and Privacy: Why the No Suspicion Required Standard in the USA PATRIOT Act is Unconstitutional*, 7 Comp. L. Rev. & Tech. J. 1, 3 (2002) [hereinafter *Packet Sniffers*]. Similarly, one court and some commentators have questioned the constitutionality of other amendments to the surveillance statutes. The United States District Court for the Southern District of New York recently ruled that ECPA's "national security letter" provision violates the Constitution. Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004) (holding that 18 U.S.C. § 2709 is unconstitutional). That decision is now on appeal. Privacy advocates have argued that the new roving wiretap provision also is unconstitutional. That provision allows the government to acquire a generic warrant that can be used to compel cooperation from any relevant communications provider. It is asserted that such authorizations do not comply with the Fourth Amendment's requirement that a search warrant "particularly describ[e] the place to be searched." U.S. Const. amend. IV; *see* Electronic Frontier Foundation, *EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities (Oct. 31, 2001)*, *available at* http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (last updated Oct. 27, 2003) (arguing that "[s]uch roving wiretap authority raises serious Fourth Amendment problems because it relaxes the 'particularity' requirements of the Warrant Clause"). However, the government has compelling arguments that a roving wiretap order is appropriately circumscribed when it focuses on the person utilizing the communications device and that such an order narrowly addresses the challenge of changing technology. *See, e.g.*, *International Terrorism: Threats and Responses: Hearing on H.R. 1710 Before the House Comm. on the Judiciary*, 104th Cong. 250, 243 (1995) (statement of

to allow the government to use packet sniffers is a practical one.[90] Because these devices give law enforcement access to the entire contents of a surveillance target's Internet communications,[91] some have argued that communications providers allowing the use of packet sniffers are providing the government with information that goes beyond the scope of a pen/trap order.[92] This, in turn, might violate the surveillance statutes' prohibitions on disclosing content except when the government has authorization to obtain such material.

Some argue that packet sniffers are not materially different from preexisting forms of surveillance and that government "minimization" efforts are sufficient to eliminate any potential violation of the surveillance statutes. When a traditional wiretap order is granted for incriminating conversations over a phone line, an agent listens to at least part of every conversation over that line, including those between the target and innocent third parties in which no incriminating details are discussed, and engages in minimization measures designed to reduce the privacy intrusion.[93]

Jamie S. Gorelick, Deputy Attorney General, U.S. Department of Justice) (stating that there is existing precedent for multipoint wiretaps and nothing about such wiretaps violates the Constitution); *id.* at 281 (statement of William P. Barr, Former Attorney General, U.S. Department of Justice, and General Counsel, GTE Corp.) (stating that roving wiretap authority is a constitutional response to changing technology and explaining that an *individual*—and not a telephone—has a protected privacy interest). More than one court has agreed with the government's position. *See, e.g.*, *United States v. Petti*, 973 F.2d 1441, 1445 (9th Cir. 1992) (holding that roving wiretaps satisfy the Fourth Amendment's particularity requirement because they do not permit a "wide-ranging exploratory search" and there is "virtually no possibility of abuse or mistake"); *United States v. Bianco*, 998 F.2d 1112, 1123–24 (2d Cir. 1993) (holding that the "roving intercept statute also addresses the fourth amendment's requirement that the place to be searched be particularly described by identifying that location in terms of where a specified individual engages in certain conversation") (internal quotation marks omitted).

90. Claimed constitutional flaws in the surveillance statutes are unlikely to pose a threat to communications providers at this point. The safe harbor provisions probably protect communications providers that comply with government surveillance requests even when those requests are later ruled unconstitutional. Courts are unlikely to conclude that a provider's compliance with existing law is unreasonable, especially in light of the risk of contempt charges for disregarding a court order to assist with surveillance.

91. Mark Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1071–72 (2001) [hereinafter *What Big Eyes*] (noting that "Carnivore operates in one of two modes, either 'full,' which reveals the entire message, including both content and addressing information; or 'pen,' which reveals just the addressing information in the electronic message. . . . In effect, the operation of Carnivore in conformity with the law is entirely at the discretion of the operator, since the operator's actions are untraceable and unaccountable").

92. *See, e.g.*, *Packet Sniffers*, *supra* note 89, at 3.

93. *See, e.g.*, 18 U.S.C. § 2518(5) (2000 & Supp. 2002) (providing that Title III wiretaps "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception"). These measures include

But packet sniffers arguably are different, and the courts have yet to face whether they are too different. When faced with a traditional pen/trap order, communications providers generally have not given the government access to the full contents of a target's phone conversations and expected it to overlook everything but the call-routing information. Rather, they have provided access only to "electronic or other impulses" on a phone line and expected the government to confine its surveillance to the "dialing and signaling information utilized in call processing."[94]

In fact, permitting the use of packet sniffers may be challenged even when the government is entitled to intercept the full content of a surveillance target's communications. When installed on a system, packet sniffers can analyze the communications of not just the individual target but of *every single person* on a server—i.e., including those the government has no cause to believe have information bearing on a criminal or national security investigation.[95] As one commentator explains, when a packet sniffer "is installed on a system, it taps everyone's e-mail on the ISP, not just the suspect's e-mail."[96] In this way, these devices are different from prior forms of surveillance, which generally did not require the government to have access to every communication of *all* of a provider's many customers. Giving the government access to so many innocent subscribers' communications raises different questions than traditional wiretaps that might incidentally capture an innocent third party's conversation with the target of the surveillance.

contemporaneous minimization, where interception of a call is stopped after it is clear that no evidence will be obtained. *See, e.g.*, United States v. Hoffman, 832 F.2d 1299, 1307–08 (1st Cir. 1987). They also include limiting interceptions of communications to times when named targets of surveillance are on the premises where a tapped phone is located. *See, e.g.*, United States v. London, 66 F.3d 1227, 1231, 1236 (1st Cir. 1995). In some cases, "after-the-fact" minimization is permissible when an intercepted communication is in a foreign language; officers interpreting and transcribing previously taped conversations simply stop listening and move on after they determine that a given call is beyond the scope of the investigation. *See, e.g.*, United States v. Padilla-Pena, 129 F.3d 457, 463–64 (8th Cir. 1997).

94. 18 U.S.C. § 3121(c) (2000) (containing the Pen/Trap Statute's minimization requirements prior to 9/11).

95. *See, e.g.* Erich Luening, *FBI Takes the Teeth out of Carnivore's Name*, CNET News.com (Feb. 9, 2001), *available at* http://news.com.com/FBI+takes+the+teeth+out+of+Carnivores+name/2100-1023_3-252368.html ("The investigative agency built the tool to monitor the Internet communications of suspects under its surveillance, but the system, housed on computers at Internet service providers, also can collect e-mail messages from people who are not part of an FBI probe."); Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 LAW LIBR. J. 601, 607 (2002) [hereinafter *Surveillance Overview*] (noting that "[c]oncern has been raised about [Carnivore's] capability to read all e-mail on the network without limitation to e-mail sent to or from the target of a judicially authorized search.").

96. *Government Surveillance*, *supra* note 73, at 112–13.

Accordingly, a communications provider permitting the government to use packet sniffers might face suits brought by surveillance targets or other customers contending that the routing of their communications through a packet sniffer violated the surveillance statutes. A communications company facing such suits should be able to rely successfully on the safe harbor provisions, but that issue is not settled—courts have yet to define the scope of these defenses as they apply to packet sniffers. Thus, a plaintiff might argue that a communications provider does not act in "good faith" when, faced with a pen/trap order, it permits the use of a packet sniffing program. This is because, arguably, the provider would be knowingly granting the government access to more than the noncontent information that is responsive to a pen/trap order. Further, in permitting the use of packet sniffers, companies are allowing the government to examine emails exchanged between third parties not named in the surveillance order. A plaintiff could argue that this too falls outside the coverage of the safe harbor provisions. And even a plaintiff acknowledging that the provider may have had a good-faith belief that its actions were lawful might contend that this belief was not a reasonable one.[97]

Communications providers should, therefore, carefully consider whether and how to permit the use of packet sniffers on their networks. Although the task of separating content from other information about Internet communications—or separating a surveillance target's communications from those of other customers—is not a simple one, companies might nonetheless choose to do so themselves rather than run the risk of a suit premised on the government's use of a packet sniffer. And companies electing to use packet sniffers may wish to modify their privacy policies if they do not already provide notice that customers' communications may be routed through such devices.[98]

3. Voluntary Disclosures

Another issue for communications providers is the extent to which they should use the voluntary disclosure provisions recently added to the surveillance statutes. In the absence of a warrant, court order, or other document compelling cooperation, it is sometimes difficult for companies to determine whether they are permitted to provide information to law

97. As discussed above, some courts have held that a provider must have a *reasonable* good-faith belief that it acted lawfully.

98. Some commentators argue that Internet service providers have already violated their privacy policies by allowing the use of packet sniffers on their networks. *See, e.g.*, Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 394 (2003) [hereinafter *Privacy Under Attack*].

enforcement. Some of the voluntary disclosure provisions are vague,[99] making it possible for providers unintentionally to go beyond the scope of the exceptions. Providers that disclose too much information may face claims that they have facilitated illegal searches when they inappropriately rely on the voluntary disclosure provisions.[100] And even when the surveillance statutes do permit disclosure, otherwise lawful voluntary disclosures may be contrary to individual companies' privacy policies. Thus, companies should ensure that they have updated their privacy policies before volunteering information to the government under the new exceptions.

Even when the surveillance statutes and company privacy policies clearly permit a communications provider to release information voluntarily, there may be some unwanted consequences of doing so. No provision in the statutes entitles companies to "uninvite" the government after an investigation has begun.[101] In fact, the government may find sufficient evidence during the voluntary phase of an investigation to return to the communications provider armed with a court order compelling further cooperation. Additional issues arise when the voluntary disclosure is made pursuant to the "computer trespasser" amendment.[102] Often, to investigate a hacking incident fully, the government must remove the affected server and take it to a lab for analysis.[103] Companies should also weigh the possibility that, after they have invited the government to investigate an incident, their computer equipment might be impounded,

99. For example, one exception permits disclosure of such information "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." 18 U.S.C. § 2702(c)(3) (Supp. 2002).

100. *See, e.g.*, *Surveillance Overview*, *supra* note 95, at 617. While the safe harbor provisions sometimes excuse improper disclosures when the provider makes a "good faith determination" that one of the voluntary disclosure exceptions applies, the scope of the safe harbor in such situations has not yet been conclusively resolved. *See, e.g.*, 18 U.S.C. § 2707(e)(3) (Supp. 2002) (providing a safe harbor under ECPA for providers that make "a good faith determination" that disclosure is permitted by one of the enumerated voluntary exceptions); *id.* § 2520(d) (same under Title III). And as discussed above, some courts have held that a provider's subjective good faith belief that its actions are lawful does not alone immunize that provider from liability; the provider's belief must also be *reasonable*. *See, e.g.*, Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 647–48 (E.D. Va. 2004).

101. Tracy Mitrano, *Civil Privacy and National Security Legislation: A Three Dimensional View*, EDUCASE REV. Nov./Dec. 2002, at 53, 59 (noting that providers making voluntary disclosures should consider what kind of control they will have to "contour or terminate an investigation once it has begun").

102. *See* 18 U.S.C. § 2511(2)(i) (Supp. 2002).

103. *See, e.g.*, DOJ MANUAL, *supra* note 3, at II.B.1.b. In fact, just recently investigators removed a hacked computer from the George Mason campus. *See* Yuki Noguchi, *George Mason Officials Investigate Hacking Incident*, WASH. POST, Jan. 13, 2005, at E01, *available at* http://www.washingtonpost.com/wp-dyn/articles/A51882005Jan12.html.

adversely affecting their ability to do business.[104] Finally, successful hacking incidents can shake customer confidence. One expert estimates that, by calling attention to a hacking incident, a company "will typically lose between ten and one hundred times more money from shaken consumer confidence than the hack attack itself represents."[105] Given this possibility, companies may elect to handle such incidents internally instead of making a voluntary disclosure to law enforcement. This of course has negative consequences for the type of information-sharing that is necessary for the effective protection of our communications networks.

In sum, the recent amendments to the surveillance statutes have made life more challenging for communications providers. Not only must they deal with more and broader surveillance requests, but they must navigate a number of complex statutory provisions that leave much room for interpretation. Although the meaning of these amendments will likely become clearer in time, at this point companies must work to discern how best to act, as responsible citizens and as service providers, under the new regime.

II. COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

Enacted in 1994, the Communications Assistance for Law Enforcement Act ("CALEA") does not modify or expand the scope of the government's surveillance authority.[106] Instead, it requires providers of certain communications services to design and update their networks to facilitate lawful electronic surveillance. Congress enacted CALEA in response to complaints from law enforcement that surveillance was becoming increasingly difficult due to the development and proliferation of

104. At a hearing before the Senate Appropriations committee, one security expert stated that computer hacking is often not reported because "[o]ne common fear is that a crucial piece of equipment, like a main server, say, might be impounded for evidence by over-zealous investigators, thereby shutting the company down." Thomas C. Greene, *Dot-com Firms Are Hacking Each Other*, THE REGISTER, Feb. 18, 2000, *available at* http://www.theregister.co.uk/2000/02/18/dotcom_firms_are_hacking_each/ [hereinafter *Hacking Each Other*]. *See also* DOJ MANUAL, *supra* note 3, at II.B.1.b (noting that "it may take days or weeks to find the specific information described in the warrant").

105. *Hacking Each Other*, *supra* note 104 (summarizing congressional testimony of security expert Mike Rasch).

106. As the D.C. Circuit has explained, "[b]ecause Congress intended CALEA to 'preserve the status quo,' the Act does not alter the existing legal framework for obtaining wiretap and pen register authorization, 'provid(ing) law enforcement no more and no less access to information than it had in the past.'" United States Telecom Ass'n v. FCC (USTA), 227 F.3d 450, 455 (D.C. Cir. 2000) (quoting H.R. REP. NO. 103-827, pt. 1, at 22 (1994)).

new communications technologies and services.[107] Since 9/11, communications providers have found their duties under CALEA to be growing, and recent developments portend of even more substantial obligations.

A. Obligations under CALEA

CALEA imposes requirements relating to communications providers' "capacity" and "capability" to accommodate electronic surveillance.[108] With respect to capability, providers must ensure that they can expeditiously intercept wire and electronic communications carried over their networks when those communications are subject to CALEA.[109] They must also be capable of giving the government access to call-identifying information that is "reasonably available" to them.[110] Providers are charged with supplying this information to the government in a way that protects the privacy of communications and call-identifying information that the government is not authorized to intercept.[111] Although the government must reimburse carriers for most capability-based modifications made to equipment, facilities, and services deployed before January 1, 1995,[112] CALEA does not provide for reimbursement with respect to newer equipment unless the Federal Communications Commission ("FCC") determines that compliance with the statute is not "reasonably

107. *Id.* at 454. In congressional hearings, federal law enforcement officers identified 183 "specific instances in which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance (wiretaps, pen registers and trap and traces)." *Id.* (quoting H.R. REP. NO.103-827, pt. 1, at 14–15 (1994)).

108. United States Telecom Ass'n v. FBI (USTA II), 276 F.3d 620, 622 (D.C. Cir. 2002).

109. 47 U.S.C. § 1002(a)(1) (2000).

110. *Id.* § 1002(a)(2). The statute does not define or interpret the term "reasonably available." Comm. Assistance for Law Enforcement Act and Broadband Access and Servs., *Notice of Proposed Rulemaking and Declaratory Ruling*, 19 F.C.C.R. 15,676 para. 9 n.13 (2004) [hereinafter *CALEA NPRM*]. However, regulations promulgated by the FCC provide that "[c]all identifying information is 'reasonably available' to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications." 47 C.F.R. § 64.2202 (2002). In the context of circuit-switched services, the FCC has defined "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2) (2000); 47 C.F.R. § 64.2202.

111. 47 U.S.C. § 1002(a)(4) (2000).

112. *Id.* § 1008(a). If the government refuses to pay for such modifications, the provider is deemed in compliance with CALEA's capability requirements. *Id.* § 1008(d).

achievable."[113]

With respect to capacity, CALEA sets up a process whereby communications providers and law enforcement cooperate to ensure that there will be sufficient surveillance capacity to satisfy the government's needs.[114] In response to FBI estimates of the capacity necessary to accommodate upcoming surveillance requests,[115] communications providers prepare statements of the modifications that must be made to their systems to provide such capacity.[116] If the FBI does not agree to provide reimbursement for the cost of installing capacity, the statute deems providers to be in compliance with their capacity obligations even if they fail to make the specified modifications.[117]

CALEA's assistance requirements apply to any "telecommunications carrier,"[118] defined as any person or entity that is "engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[119] This category includes any provider of a communications service that is "a replacement for a substantial portion of the local telephone exchange service" when the FCC concludes that it is in the public interest to classify the provider as a telecommunications carrier for purposes of CALEA.[120] Communications providers are exempt from CALEA's requirements "insofar as they are engaged in providing information services,"[121] which are defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications. . . ."[122]

113. *Id.* § 1008(b)(2).

114. *See id.* § 1003. A more detailed description of this process can be found in United States Telecom Ass'n v. FBI (USTA II), 276 F.3d 620, 622–23 (D.C. Cir. 2002).

115. 47 U.S.C. § 1003(a)(1) (2000) (initial notice of estimated actual and maximum capacity); *id.* § 1003(c) (notices of increased maximum capacity).

116. *Id.* § 1003(d).

117. *Id.* § 1003(e). In this way, communications providers' capacity obligations differ from their capability obligations. As discussed, CALEA requires the government to pay for capability-based modifications to equipment installed after January 1, 1995 only when compliance is not "reasonably achievable." *Id.* § 1008(b)(2).

118. *Id.* § 1002(a); *id.* § 1003(b), (d).

119. *Id.* § 1001(8)(A).

120. *Id.* § 1001(8)(B).

121. *Id.* § 1001(8)(C)(i); *see also id.* § 1002(b)(2) (providing that the capability requirements do not apply to "information services").

122. *Id.* § 1001(6)(A). That section further provides that "information services" include:

> (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but . . . does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

Id. § 1001(6)(B)–(C).

Communications providers that fail to meet CALEA's requirements are subject to fines of up to $10,000 per day of noncompliance.[123] But CALEA provides a safe harbor to communications companies if they conform their networks to "technical requirements or standards adopted by an industry association or standard-setting organization. . . ."[124] Providers whose failure to abide by such standards precludes them from assisting the government with lawful surveillance requests are subject to court-issued enforcement orders.[125] Such orders, however, may be issued only when alternative technologies or the facilities of other providers are not available for implementing surveillance requests.[126] Further, a provider cannot be penalized unless compliance is reasonably achievable through the use of available technology or would have been reasonably achievable had the provider taken timely action.[127] A number of other statutory defenses also are available.[128]

B. CALEA Issues Arising after 9/11

Congress made no meaningful changes to CALEA in response to 9/11. But a number of important regulatory developments have made life more challenging for communications companies. Further, several earlier, complicated issues are still under consideration.

1. Expansion of CALEA to New Services

The government has consistently argued that CALEA applies to more than the traditional circuit-switched telephone network. In a proceeding initiated last year, three federal law enforcement entities[129] petitioned the FCC[130] to conclude that CALEA requires providers of broadband access

123. *See* 18 U.S.C. § 2522 (c)(1) (2000) (providing for a penalty of up to $10,000 per day of noncompliance); *see also* 47 U.S.C. § 1007(a) (2000) (setting forth the circumstances under which a court may issue an enforcement order under 18 U.S.C. § 2522).

124. *Id*. § 1006(a)(2); United States Telecom Ass'n v. FCC (USTA), 227 F.3d 450, 455 (D.C. Cir. 2000).

125. 47 U.S.C. § 1007 (2000).

126. *Id.* § 1007(a)(1).

127. *Id.* § 1007(a)(2).

128. *See id.* § 1007(c) (stating that a provider need not meet the government's demand for assistance if the request exceeds the level of capacity for which the government has agreed to reimburse the provider).

129. The law enforcement agencies were the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration ("law enforcement").

130. *See* United States Department of Justice, Federal Bureau of Investigation and United States Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Joint Petition for Expedited Rulemaking*, RM-10865 (Mar. 10, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&

services[131] and managed Voice over Internet Protocol ("VoIP") services[132] to design their networks to accommodate electronic surveillance.[133] Critics of law enforcement's position argue that these services are "information services" outside the scope of CALEA.[134]

The first round in this fight went to law enforcement.[135] In a notice of proposed rulemaking issued last August, the FCC tentatively concluded that a number of new service providers are subject to CALEA's assistance requirements, including "facilities-based providers of any type of broadband Internet access service" and "'managed' Voice over Internet Protocol" services. [136] Asserting that this should not be the FCC's final decision on the matter, some parties have argued that the application of CALEA to such services is inconsistent with that statute.[137] Regardless of the ultimate resolution of this particular question, this proceeding is another reflection of the difficult questions facing communications providers after 9/11.

id_document=6516082660 [hereinafter *CALEA Petition*]. All public records in RM-10865 have been moved to ET Docket No. 04-295 in the FCC's electronic comment filing system.

131. The law enforcement petition defines "broadband access services" as "the platforms currently used to achieve broadband connectivity (*e.g.*, wireline, cable modem, wireless, fixed wireless, satellite, and broadband access over power line) as well as any platforms that may in the future be used to achieve broadband connectivity." *CALEA NPRM*, *supra* note 110, para. 32.

132. VoIP is a means of transmitting voice communications over an IP-based network like the Internet. The law enforcement petition defines "managed" VoIP services as "those services that offer voice communications calling capability whereby the VoIP provider acts as a mediator to manage the communication between its end points and to provide call set up, connection, termination, and party identification features, often generating or modifying dialing, signaling, switching, addressing or routing functions for the user." *Id.* para. 37.

133. *CALEA Petition*, *supra* note 130, at 15–17.

134. *See, e.g.*, United States Department of Justice, Federal Bureau of Investigation and United States Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Cellular Telecommunications & Internet Association Comments*, RM-10865, at 3–4 (Apr. 12, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516087738; Comm. Assistance for Law Enforcement Act and Broadband Access and Servs., *Comments of the Electronic Frontier Foundation*, ET Dkt. No. 04-295, at 12–15 (Nov. 8, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516793563.

135. *CALEA NPRM*, *supra* note 110, para. 41 (noting that "[w]e tentatively conclude that Congress intended the scope of CALEA's definition of 'telecommunications carrier' to be more inclusive than that of the Communications Act").

136. *Id.* para. 1.

137. The comments of parties supporting and opposing the law enforcement petition can be found under proceeding number 04-295 at http://gullfoss2.fcc.gov/prod/ecfs/comsrch_v2.cgi.

2. New Standards for Broadband Technologies

After the FCC resolves the threshold question of which types of communications services CALEA applies to, a decision will need to be made regarding the precise nature of the CALEA obligations of the providers that offer those services. This inquiry is far more complex in the context of packet-switched services than it is with respect to traditional phone service because there are many different types of broadband access and many different forms of information involved in Internet communications. Moreover, there are considerable technological differences even across different providers of the same service and different versions of the same application.

A number of communications providers are currently playing an important role in helping to answer these questions.[138] Traditional telecommunications providers, VoIP providers, Internet service providers, and manufacturers are negotiating with law enforcement to devise the standards that will apply to the packet-switched technologies that the FCC concludes are subject to CALEA. Although final standards governing packet-based communications have not been issued, the participants have made considerable progress.[139] For example, packet-mode standards were recently developed for call-identifying information required in connection with government requests for call interception for certain services such as VoIP.[140] The only thing that is clear at this point, however, is that many communications providers are likely to be subject to stricter standards than those they have faced in the past.

3. Deadline for Compliance

There is concern among communications providers that the FCC will impose a deadline for CALEA compliance that leaves insufficient time for

138. *See, e.g.*, United States Department of Justice, Federal Bureau of Investigation and United States Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Comments of the Alliance for Telecommunications Industry Solutions*, RM-10865 (Apr. 12, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516087739 (describing the status of ATIS efforts to develop industry standards); *see also id.* at 2 (stating that "ATIS membership spans all segments of the industry, including local exchange carriers, interexchange carriers, manufacturers, competitive local exchange carriers, data local exchange carriers, wireless providers, cellular providers, broadband providers, software developers and internet service providers").

139. In the NPRM, the FCC describes a standard that has been approved by many participants but "has not completed its editing and publication cycles." *Id.* para. 95 n.226.

140. *Id.* para. 94.

completion of the industry standards process.[141] If that happens, companies will not enjoy a safe harbor with respect to their obligations under the statute.[142] Providers also complain that, even if there is time for the publication of industry standards, an early compliance deadline will leave insufficient time for manufacturers and carriers to devise solutions consistent with those standards to bring providers into compliance with the statute.[143]

In the past, this issue has not alarmed providers because the FCC has been reasonable in granting waivers of compliance deadlines. CALEA invites petitions for extensions and provides that they should be granted if the FCC "determines that compliance with the assistance capability requirements under section 1002 of this title is not reasonably achievable through application of technology available within the compliance period."[144] The FCC has generally looked with favor on such petitions.[145] In the CALEA NPRM, however, the FCC said that extensions would be available only in cases where the petitioning communications provider deployed the equipment, facility, or service in question prior to October 25,

141. *See, e.g.*, United States Department of Justice, Federal Bureau of Investigation and United States Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Comments of Verizon on Law Enforcement's Joint Petition for Expedited Rulemaking Concerning the Communications Assistance for Law Enforcement Act*, RM-10865, at 19 (Apr. 12, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516087744 [hereinafter *Verizon Comments*] (arguing that "CALEA clearly makes industry standards and safe harbors a focal point of compliance. Much of the work that manufacturers and carriers must do to achieve CALEA-compliance cannot begin without an industry-approved standard"); *CALEA NPRM*, *supra* note 110, para. 142.

142. 47 U.S.C. § 1006(a)(3) (2000) (providing that "[t]he absence of technical requirements or standards for implementing the assistance capability requirements . . . shall not . . . relieve a carrier, manufacturer, or telecommunications support services provider of the obligations imposed by [section 1002 or 1005] of this title, as applicable").

143. *See, e.g.*, United States Department of Justice, Federal Bureau of Investigation and United States Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, *Comments of SBC Communications, Inc. in Response to the Commission's Public Notice Seeking Comment on the Joint Petition for Expedited Rulemaking*, RM-10865, at 13 (Apr. 12, 2004) (noting that "once a standard has been developed, achieving the next milestone will turn on whether and how quickly manufacturers are able to develop a solution that works with existing infrastructure"), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516087696; *see also Verizon Comments*, *supra* note 141, at 19–20.

144. 47 U.S.C. § 1006(c)(2) (2000).

145. As the FCC recognized in the NPRM, "[t]o date, the Commission has granted hundreds of section 107(c) extension petitions in consultation with the FBI to permit carriers to phase-in CALEA compliance . . . The extension process has been relatively simple." *CALEA NPRM*, *supra* note 110, para. 89.

1998.[146] The FCC noted that this interpretation would likely preclude extensions of deadlines for packet-mode compliance because most, if not all, packet-based equipment, facilities, and services were installed after that date.[147] Most carriers would, therefore, find themselves relying not on extensions, but on the alternate relief offered in section 1008(b) of the statute, which requires the government to pay for any modifications made to newer equipment when a provider successfully petitions the FCC for a determination that compliance is not "reasonably achievable."[148] But the FCC warned in the NPRM that carriers will face a very high burden to obtain such relief and tentatively concluded that this burden "would not be met by a petitioning carrier that merely asserted that CALEA standards had not been developed, or that solutions were not readily available from manufacturers."[149] Noting these additional obstacles, the FCC explained that "many carriers could find it difficult to obtain either CALEA compliance extensions or exemptions in connection with packet requirements. As a result, they may become immediately subject to enforcement action."[150] Because the fine for noncompliance can be as high as $10,000 per day, it is not surprising that some communications providers are concerned.

As discussed above, carriers can invoke a variety of defenses when faced with an enforcement action in court. An order mandating network changes cannot be issued unless compliance is reasonably achievable through the use of available technology.[151] Thus, if manufacturers have not yet developed appropriate devices to facilitate surveillance of packet-switched communications, providers might avoid liability. Similarly, providers are not subject to enforcement actions when the government can obtain information from another source.[152] A broadband provider might argue that law enforcement should seek assistance from another provider that is better equipped to handle a surveillance request. Relying on such defenses, however, is clearly a second-best solution. The industry is advocating that the FCC adopt a compliance deadline that offers communications providers sufficient time in which to bring their systems into compliance with CALEA's new requirements.

Whether the FCC should adopt its own enforcement mechanism is

146. *Id.* para. 97.
147. *Id.*
148. 47 U.S.C. § 1008(b) (2000).
149. *CALEA NPRM*, *supra* note 110, para. 98.
150. *Id.* para. 99.
151. 47 U.S.C. § 1007(a)(2) (2000).
152. *Id.* § 1007(a)(1).

also at issue in the ongoing rulemaking proceeding. Law enforcement asserts that bringing a civil action in district court should not be its only means of enforcing CALEA and argues that the FCC should establish rules permitting the agency itself to issue notices of apparent liability.[153] The FCC has expressed interest in this proposal, tentatively concluding that it "has general authority under the Communications Act to promulgate and enforce CALEA rules."[154] The agency has called for comment on whether it should establish a separate enforcement mechanism and, if so, what rules should govern such a proceeding.[155] Were the FCC to adopt an independent enforcement mechanism, it is unclear whether the statutory defenses would be available in a proceeding before the agency.[156] If stripped of those defenses, providers could find themselves subject to even greater obligations under CALEA.

4. Defining the Meaning of "Call-Identifying Information"

Issues regarding the definition of "call-identifying information" in CALEA closely mirror those surrounding the meaning of "content" for purposes of the surveillance statutes. These surfaced after the communications industry promulgated the first round of CALEA standards and the Department of Justice and the FBI challenged them as deficient.[157] In the United States Court of Appeals for the District of Columbia Circuit, the FCC adopted the government's position, arguing that call-identifying information includes—and CALEA requires communications carriers to provide—a surveillance feature described as "[p]ost-cut-through dialed digit extraction."[158] That feature refers to providing access to the numbers dialed by a surveillance target after a phone call has been connected.[159] In addition, the FCC asserted that carriers must make available to law enforcement noncontent information about packet-mode communications, such as Internet communications.[160] The court held that the FCC was entitled to require communications providers to design their networks to

153. *See CALEA NPRM*, *supra* note 110, para. 111.

154. *Id.* para. 114.

155. *Id.* para. 115.

156. *See id.* para. 114 (asking whether 47 U.S.C. § 1007, which contains the defenses to a civil action under CALEA, "impose[s] any limitations on the nature of the remedy that the Commission may impose").

157. United States Telecom Ass'n v. FCC (USTA), 227 F.3d 450, 455–56 (D.C. Cir. 2000).

158. *Id.* at 456.

159. *Id.* Such numbers can constitute call-identifying information when, for example, a surveillance target uses a calling card. *Id.*

160. *Id.* at 464.

yield different types of information about packet-mode communications.[161] And although the court held that the FCC had failed to fully explain why it viewed post-cut-through dialed digits as "call-identifying information,"[162] the FCC remedied this error on remand.[163]

Such disputes over the meaning of "call-identifying information" have taken on a new tenor since 9/11. First, although before 9/11 communications providers were litigating whether CALEA required them to grant law enforcement access to post-cut-through dialed digits and packet-mode communications, only since 9/11 have companies actually been required to *provide* such information.[164] Accordingly, communications providers are for the first time facing difficult questions about *which* post-cut-through dialed digits constitute content and what types of information in a packet constitute call-identifying information. Designing facilities to distinguish between the two types of information has proven far from simple.[165]

Similarly, VoIP was a nascent technology before 9/11. But carriers now are squarely facing the question of how to extract call-identifying information from a VoIP packet without reading the packet's content. This task is particularly difficult when a surveillance target's broadband service provider is not the same company that provides the target's VoIP service.

161. *Id.* at 465. At the same time, however, the court held that disclosure of call-identifying information about packet-mode communications might implicate privacy concerns. *Id.* at 464–65. It noted that the FCC's rules were permissible only because "nothing in the Commission's treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization. . . . CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is not authorized to be intercepted." *Id.* at 465 (internal quotation marks omitted). The court did not address whether it is possible for communications providers themselves to successfully extract call-identifying information from packets without violating the surveillance statutes or CALEA's privacy provision. *Id.* at 464–65.

162. *Id.* at 462.

163. Communications Assistance for Law Enforcement Act, *Order*, 16 F.C.C.R. 17,397 (2001).

164. "As of November 19, 2001," the FCC's regulations have required communications providers to be capable of offering law enforcement "communications and call-identifying information transported by packet-mode communications." 47 C.F.R. § 64.2203(b) (2002). Similarly, only since June 30, 2002 have communications providers been required to provide "dialed digit extraction," defined under the regulations as "[c]apability that permits a [law enforcement agency] to receive on the call data channel [] digits dialed by a subject after a call is connected to another carrier's service for processing and routing." *Id.* § 64.2202 (defining "dialed digit extraction"); *id.* § 64.2203(c)(6) (providing timing for provision of dialed digit extraction).

165. *See CALEA NPRM*, *supra* note 110, para. 68.

As the FCC has conceded, "[c]all-identifying information may be found within several encapsulated layers of protocols," and a facilities-based broadband service provider will not necessarily "examine or process information in the layers used to control packet-mode services such as VoIP. . . ."[166] An important question now under consideration is whether a broadband access provider should be required to supply call-identifying information when the provider generally does not process information found in the application level of an Internet communication.[167] Providers have argued that they should be required to offer only the call-identifying information that they have access to in the regular course of providing broadband access.[168] But the FCC may conclude that law enforcement can ask not only the application provider but also the broadband access provider to isolate call-identifying information found in the application layer of a packet. Broadband access providers then will face the difficult question of how to supply this information without giving the government access to the contents of packet-based communications.[169]

Isolating call-identifying information is not without risks. CALEA requires communications providers to protect the privacy of their customers,[170] and the United States Court of Appeals for the District of Columbia Circuit has warned that separating content from call-identifying information in the context of Internet communications raises important privacy issues.[171] Similarly, the FCC has noted that "privacy concerns could be implicated if carriers were to give to [law enforcement agencies] packets containing both call-identifying and call content information when only the former was authorized."[172] As noted, companies that unreasonably

166. *Id.* para. 65.

167. *Id.* paras. 67–68.

168. *See, e.g.*, Comm. Assistance for Law Enforcement Act and Broadband Access and Servs., *Reply Comments of the United States Internet Service Provider Association*, ET Dkt. No. 04-295, at 3 (Dec. 21, 2004), *at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516885862 (stating that "CALEA requires carriers to provide law enforcement with access only to CII that is 'reasonably available' to the carrier. . . . [S]uch information should be limited in the packet-mode context to CII that a carrier routinely uses in delivering services to its customers.").

169. *CALEA NPRM*, *supra* note 110, para. 65; *see also* United States Telecom Ass'n v. FCC (USTA), 227 F.3d 450 (D.C. Cir. 2000). This case noted the following:

> Telecommunication carrier petitioners claim that packet headers (call-identifying information) cannot be separated from packet bodies or payloads (call content). Accordingly, they and the privacy petitioners argue that any packet-mode data provided to a law enforcement agency pursuant to a pen register order will inevitably include some call content, thus violating CALEA's privacy protections.

United States Telecom Ass'n v. FCC, 227 F.3d at 464.

170. 47 U.S.C. § 1002(a)(4) (2000).

171. USTA, 227 F.3d at 464–65.

172. Communications Assistance for Law Enforcement Act, *Third Report and Order*, 14

misjudge the meaning of "call-identifying information" and turn over too much information to the government also might violate the surveillance statutes.[173] Even where a safe harbor applies, those provisions do not protect companies from other risks, such as harm to customer relationships brought on by a perceived failure to safeguard customer privacy. Because policymakers have, to date, simply not addressed many of the challenges carriers face in providing call-identifying information, communications providers themselves must work to overcome the technological and practical impediments to supplying call-identifying information under CALEA.

5. Who Bears the Burden of Paying for CALEA Compliance?

Yet another important question arising under CALEA is who must pay for the capital improvements necessary to bring carriers into compliance with the statute. As the FCC has recognized, "[t]he modifications and upgrades required . . . will potentially require significant capital expenditures on the part of carriers."[174] Although CALEA requires the government to reimburse carriers for most modifications made to equipment, facilities, and services deployed before January 1, 1995,[175] it does not require reimbursement for improvements made to newer equipment unless compliance with the statute is not "reasonably achievable."[176] What is meant by this term—and, accordingly, who pays for network enhancements—is particularly important to Internet service providers and VoIP providers, which often do not have the capital necessary to comply with their new CALEA obligations.

This issue is more pressing after 9/11. The law enforcement petition

F.C.C.R. 16,794, para. 48 (1999).

173. *See* discussion *supra* Part I.B.2. As discussed, however, the government does engage in minimization efforts designed to protect the privacy of communications that it is not authorized to intercept. *See supra* note 93.

174. *CALEA NPRM*, *supra* note 110, para. 117. One commenter noted:

> [C]ompanies must often establish separate departments, solely devoted to processing and responding to government requests. The large telephone companies and Internet service providers, for example, have entire staffs of clerks, attorneys, and former law enforcement agents (often as large as 30-50 employees) just to handle government subpoenas and court orders.

Stewart A. Baker, *The Regulation of Disclosure of Information Held by Private Parties*, *in* PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE: A REPORT OF THE MARKLE FOUNDATION TASK FORCE 161, 171 (Markle Foundation, 2002), *available at* http://www.markletaskforce.org/documents/Markle_Full_Report.pdf.

175. 47 U.S.C. § 1008(a) (Supp. 2002). If the government refuses to pay for such modifications, the provider is deemed in compliance with CALEA's capability requirements. *Id.* § 1008(d).

176. *Id.* § 1008(b)(2).

urges the FCC to establish new rules requiring that "'carriers bear the sole financial responsibility for development and implementation of CALEA for post January 1, 1995 communications equipment, facilities, and services,'" despite the complaints of providers that the cost of such modifications is exceedingly high.[177] Basically, law enforcement asks the FCC to eliminate the cost of a proposed modification as a factor in its analysis of whether that modification is "reasonably achievable" and argues that providers should be able to recover those costs from their customers.[178] Further, law enforcement has called into question communications providers' ability to recoup their capital expenditures through provisions in the surveillance statutes that require the government to pay for the cost of surveillance activities.[179] In their petition, the law enforcement entities argue that those provisions permit carriers to recoup only the incremental costs of providing surveillance, asserting that "permitting carriers to include their CALEA implementation costs in their administrative intercept provisioning costs would not only violate Title III . . . but would also make it increasingly cost-prohibitive for [law enforcement agencies] to conduct intercepts."[180] If the FCC resolves this question in favor of law enforcement, it could mean hundreds of millions of dollars in additional costs for communications companies.[181]

In short, questions remain to be answered with respect to CALEA. The FCC appears poised to expand the reach of the statute to include at least some packet-switched communications. And companies might face a number of costly burdens, including an expedited deadline to bring their networks into compliance with the statute at their own expense.

177. *CALEA NPRM*, *supra* note 110, paras. 119–20.

178. *See id.* para. 123.

179. Such provisions include, for example, 18 U.S.C. § 2706(a), which states the following:

> [A] governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information.

18 U.S.C. § 2706(a) (2000).

180. *CALEA NPRM*, *supra* note 110, para. 119; *see also id.* para. 132.

181. *See id.* para. 117 (noting that, although there are no "solid" estimates of the cost of updating facilities deployed after 1995, the government nearly has exhausted a $500 million fund that Congress appropriated for modifications to pre-1995 facilities).

III. CRITICAL INFRASTRUCTURE INFORMATION

Critical infrastructure has been defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[182] Government agencies and members of Congress have long maintained that the federal government and the private sector should cooperate in identifying vulnerabilities of, and potential threats to, the nation's critical infrastructure. Since 9/11, calls for such cooperation have intensified, prompting legislative and regulatory changes designed to encourage companies to share their critical infrastructure information with the government. Despite these changes, communications providers must consider the risks in disclosing sensitive critical infrastructure information.

A. Critical Infrastructure Initiatives

Even before 9/11, there was a push for the federal government to acquire information about the nation's critical infrastructure and for the government and the private sector to cooperate in ensuring the security of our national infrastructure, 85 percent of which[183] is privately owned. In 1996, President Clinton established the Commission on Critical Infrastructure Protection ("CCIP").[184] CCIP was charged with "assessing the vulnerabilities of the country's critical infrastructures and proposing a strategy for protecting them."[185] It issued a final report in 1997 proclaiming that "two-way sharing [of] information is indispensable to infrastructure assurance" and that "increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government will greatly assist efforts of owners and operators to identify their vulnerabilities and acquire tools needed for protection."[186] CCIP

182. Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8083 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.2); 42 U.S.C. § 5195c(e) (Supp. 2002).

183. *See* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 398 (2004), *available at* http://www.9-11commission.gov/report/index.htm [hereinafter 9/11 COMMISSION REPORT].

184. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

185. JOHN D. MOTEFF & GINA MARIE STEVENS, CONGRESSIONAL RESEARCH SERVICE, CRITICAL INFRASTRUCTURE INFORMATION DISCLOSURE AND HOMELAND SECURITY 1 (Report for Congress, 2003), *at* http://www.fas.org/irp/crs/RL31547.pdf [hereinafter MOTEFF & STEVENS].

186. *Id.* (quoting *Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection* (Oct. 1997)). One of the Authors, Jamie S. Gorelick, was co-chair (with former Senator Sam Nunn) of the Advisory Committee to the Commission.

proposed, for each industry sector, the creation of an Information Sharing and Analysis Center ("ISAC") where private sector representatives and the government would cooperate to compile critical infrastructure information, analyze it, and identify potential vulnerabilities.[187] In response to CCIP's proposal, President Clinton issued Presidential Decision Directive No. 63.[188] It required some key government officials to consult with private sector owners and operators of critical infrastructures to establish these private sector, information-sharing centers and encouraged the creation of the information analysis center proposed by CCIP.[189]

After 9/11, the focus on compiling and analyzing critical infrastructure information became far sharper. In October 2001, President Bush issued an Executive Order on Critical Infrastructure, which established a senior executive branch board to coordinate federal critical infrastructure efforts.[190] The President's Critical Infrastructure Protection Board was charged with engaging the cooperation of state and local governments and the private sector.[191] Shortly thereafter, as part of the Patriot Act, Congress enacted the Critical Infrastructures Protection Act of 2001.[192] It provides that "a public-private partnership involving corporate and non-governmental organizations" should work to ensure that "any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States."[193] It also establishes a National Infrastructure Simulation and Analysis Center responsible for, among other things, acquiring data from the private sector and using it to create and maintain models of critical infrastructure systems.[194]

Even under these post-9/11 enactments, government efforts to acquire such information have been only marginally successful. In part, this is because companies are hesitant to provide information when the government requests it. Companies have been concerned that information in the government's possession might be subject to public disclosure under

187. *Id.* at 2.

188. *Id.* (citing The White House, Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (May 1998), *available at* http://www.ciao.gov/resource/paper598.pdf).

189. *Id.*

190. Exec. Order 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

191. *Id.* § 5(a)–(c), 66 Fed. Reg. 53,064–65.

192. Patriot Act § 1016 (codified at 42 U.S.C. § 5195c (Supp. 2002)).

193. *Id.* § 1016(c) (codified at 42 U.S.C. § 5195c(c)).

194. *Id.* § 1016(d) (codified at 42 U.S.C. § 5195c(d)).

the Freedom of Information Act, which provides a mechanism for interested parties to force the government to release certain types of information.[195] And communications providers wish to avoid government disclosure of critical infrastructure information to third parties lest their competitors obtain their valuable proprietary information.[196] Companies also worry that the sharing of certain information might make them vulnerable to antitrust actions or expose them to other forms of liability.[197] Moreover, companies are concerned that they might undermine the market's confidence in their services by highlighting their systems' vulnerabilities.[198]

To encourage the sharing of information about critical infrastructure, Congress passed the Critical Infrastructure Information Act of 2002 as part of the Homeland Security Act.[199] In a section entitled "Protection of Voluntarily Shared Critical Infrastructure Information," the Act provides that critical infrastructure information "voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution or other informational purpose" is exempt from disclosure under the Freedom of Information Act.[200] The Act also contains a number of other prohibitions on the use and disclosure of such

195. Some companies worried that their sensitive information might be subject to disclosure even though the Freedom of Information Act ("FOIA") contains exemptions that arguably covered critical infrastructure information. *See* Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, 53 AM. U. L. REV. 261, 290–91 & n.162 (2003) [hereinafter *FOIA Post-9/11*] (citing industry concerns that sensitive information would be disclosed by the government under FOIA); *see also* 5 U.S.C. § 552(b)(4) (providing a FOIA exemption for "trade secrets and commercial or financial information obtained from a person and privileged or confidential"). As discussed below, a new FOIA exemption for critical infrastructure information disclosed voluntarily to the Department of Homeland Security ("DHS") now gives communications providers more assurance that their sensitive information will not be made publicly available. *See infra* text accompanying note 200.

196. *See FOIA Post-9/11*, *supra* note 195, at 289; MOTEFF & STEVENS, *supra* note 185, at 15.

197. *See FOIA Post-9/11*, *supra* note 195, at 289–90; MOTEFF & STEVENS, *supra* note 185, at 15.

198. MOTEFF & STEVENS, *supra* note 185, at 2, 15.

199. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

200. 6 U.S.C. § 133(a)(1) (Supp. II 2003). It is important to note that the only "covered Federal agency" is the Department of Homeland Security. *Id.* § 131(2). The new FOIA exemption does not protect information submitted to other government entities. Further, critical infrastructure information does not qualify for the new exemption unless it is marked with the statement, "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the Critical Infrastructure Information Act of 2002." *Id.* § 133(a)(2).

data.[201] Any federal employee who unlawfully uses or discloses critical infrastructure information is subject to firing, fines, and imprisonment for up to a year.[202] Under this statute, therefore, a communications company can provide infrastructure information to the Department of Homeland Security ("DHS") with some assurance that the secrecy of that information will be preserved.

Additional critical infrastructure provisions appear in the recently passed Intelligence Reform and Terrorism Prevention Act of 2004. One requires the DHS to prepare a report to Congress regarding critical infrastructure, including the status of the Department's efforts to complete vulnerability and risk assessments of the nation's critical infrastructure.[203] Another requires the Department to coordinate industry efforts to identify private sector resources and capabilities that could supplement government efforts to prevent or respond to a terrorist attack.[204] The purpose of these legislative developments is that companies' infrastructures may enjoy increased protection from terrorist and hacker attacks, but companies are also likely to face an increased expectation that they will share critical infrastructure information.

B. Factors to Consider When Disclosing Information

There is no simple guide to how companies should handle governmental requests for information on infrastructure vulnerabilities. Communications providers are eager to do what they can to help safeguard the nation's critical infrastructure against acts of terrorism and computer crime. And companies enjoy a number of benefits when they share critical infrastructure information. However, because such sharing is voluntary, they therefore weigh a number of factors when determining how much

201. *Id.* § 133(a)(1)(A)–(F). For example, disclosures about critical infrastructure information are not subject to judicial or agency rules regarding the ex parte disclosure of information to government officials. *Id.* § 133(a)(1)(B); Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8088 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.8(h)). Similarly, no government or private entity may use voluntarily disclosed critical infrastructure information in any civil action. 6 U.S.C. § 133(a)(1)(C); Protected Critical Infrastructure Information, 69 Fed. Reg. at 8074, 8088 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.8(i)).

202. 6 U.S.C. § 133(f) (providing that a federal employee who unlawfully discloses critical infrastructure information "shall be fined under Title 18, imprisoned not more than 1 year, or both, and shall be removed from office or employment"); Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8089 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.9(d) (same)).

203. Intelligence Reform Act § 7306(b)(1).

204. *Id.* § 7402.

information to offer.[205]

Communications companies derive important benefits from sharing critical infrastructure information. Because computer attacks are rarely confined to one provider's system, sharing information with the government and with other providers permits communications companies to better understand the nature of attacks on their networks. Such information sharing equips providers to protect their systems more effectively against future attacks. It also helps providers to identify other weaknesses in their networks and to devise potential remedies. And the reputations of companies are enhanced—both with government officials and with the public generally—by cooperating with government efforts to protect the nation's critical infrastructure against attack.

But other factors may act as counterweights. The government may release critical infrastructure information in a number of circumstances.[206] Providers also have no private right of action against those who release information in violation of the Homeland Security Act and must rely on other mechanisms for redressing unlawful disclosures of their

205. One commentator notes that, after considering some of these factors, critical infrastructure operators might continue to withhold information from the government despite the FOIA exemption. *See FOIA Post-9/11*, *supra* note 195, at 282.

206. The Homeland Security Act permits the DHS to disclose sensitive critical infrastructure information to designated parties in several situations. For example, information can be released to state and local governments. Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8087 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.8(b)). And there is no clear enforcement mechanism through which these governments can be punished if they disclose information in violation of the statute; the Act's penalty provision applies only to "officer[s] or employee[s] of the United States or of any department or agency thereof." 6 U.S.C. § 133(f) (Supp. II 2003); Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8089 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.9(d)). It is also permissible for the DHS to disclose a company's critical infrastructure information to foreign governments in certain circumstances. Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8088 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.8(j)). Further, critical infrastructure information may be released to government contractors, which are barred from disclosing the information to others but are not subject to the Act's penalties of imprisonment or fines if they do. *Compare id.* at 8087 (to be codified at 6 C.F.R. § 29.8(c)) (requiring federal contractors to sign corporate or individual confidentiality agreements and providing a general prohibition on disclosure), *with* 6 U.S.C. § 133(f) (Supp. II 2003) (providing that a federal employee who unlawfully discloses critical infrastructure information "shall be fined under [T]itle 18 . . . , imprisoned not more than 1 year, or both, and shall be removed from office or employment"), *and* Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8089 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.9(d) (same)). Finally, critical infrastructure information is subject to the Whistleblower Protection Act, and may be disclosed to the public when it evidences a violation of the law, an abuse of authority, or a substantial and specific danger to public health or safety. Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8088 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.8(f)(3)).

information.[207]

A second factor is the affirmation requirement set out in the regulations implementing the Critical Infrastructure Information Act. Persons and companies submitting critical infrastructure information must also affirm their understanding that any false representations may constitute a violation of 18 U.S.C. § 1001 and be punishable by a fine or imprisonment.[208] That statutory provision provides for harsh penalties for those who make false statements to the government or who conceal a material fact.[209]

Third, companies must be careful not to release more information to the government than is permitted. Privacy laws might bar the disclosure of some types of information. Contracts with other companies might bar the unilateral disclosure of infrastructure information when it constitutes proprietary information.[210]

After weighing these considerations, communications companies should put in place policies and procedures for responding to government inquiries regarding critical infrastructure. Some companies have decided that the risks of liability and public disclosure are simply too great, prompting them to decline to disclose *any* information. Other companies are sharing such information with each other and/or the government. Companies that elect to share information should take care in drafting their disclosure policies with respect to different types of information and ensure that their privacy notices to customers are consistent with their disclosures.

Finally, companies should be aware that the DHS's critical infrastructure disclosure protections are under pressure. Since the passage of the Homeland Security Act, a number of parties have supported legislation to reduce protections for critical infrastructure information.[211]

207. 6 U.S.C. § 134 (Supp. 2002); Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8084 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.3(e)).

208. Protected Critical Infrastructure Information, 69 Fed. Reg. 8074, 8085 (Feb. 20, 2004) (to be codified at 6 C.F.R. § 29.5(e)).

209. 18 U.S.C. § 1001 (2000). The statute applies to one who "knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry." *Id.* § 1001(a).

210. *Cf.* MOTEFF & STEVENS, *supra* note 185, at 2 (explaining that companies have been hesitant to share information because doing so might expose them to liability in the event that the government discloses confidential business information).

211. Groups that have expressed concern with the FOIA exemption for critical infrastructure information include the American Civil Liberties Union, the Electronic Privacy Information Center, Natural Resources Defense Fund, the Society of Professional Journalists, and the U.S. Public Interest Research Group. *Id.* at 15 n.49. Bills to limit the protections of the Homeland Security Act have been introduced, including the Restoration

Moreover, given the recent passage of the Intelligence Reform and Terrorism Prevention Act, agency proceedings will likely be underway soon to draft regulations implementing the Act.[212] Companies should keep abreast of any new developments in this area and participate in agency proceedings when necessary to protect their interests.

One industry spokesman has argued that "information sharing is a risky proposition with less than clear benefits."[213] Communications providers do face risks when sharing critical infrastructure information. But they also derive important benefits from such sharing, including a better understanding of how to address vulnerabilities in their networks. Thus, neither complete secrecy nor full disclosure is a viable course of action.

IV. APPROVAL OF FOREIGN INVESTMENTS IN U.S. COMMUNICATIONS COMPANIES

When a foreign entity seeks to acquire control of a U.S. business, the Committee on Foreign Investment in the United States ("CFIUS")—comprising a dozen U.S. government departments and agencies—may review the proposed transaction to ensure that it will not threaten the national security of the United States. If CFIUS investigates and recommends against the transaction, the President can block the transaction or order divestment. Relatedly, when a foreign entity seeks to acquire control of a U.S. communications company, the parties often must seek authorization from the FCC, and the FCC will not grant that authorization until U.S. law enforcement and security agencies (members of CFIUS) signify their acquiescence in the deal's closing.

Since 9/11, it has become more difficult for foreign entities to obtain approval for their acquisitions of communications companies. Recent developments suggest that there now are greater obstacles to cross-border investment in such companies and other entities with advanced technologies. Even when a company with substantial foreign ownership

of Freedom of Information Act of 2003, which was pending in both the House and Senate in 2003. The Restoration of Freedom of Information Act of 2003, S. 609, H.R. 2526, 108th Cong. (2003). *See* Ava Barbour, *Ready . . . Aim . . . FOIA! A Survey of the Freedom of Information Act in the Post-9/11 United States*, 13 B.U. PUB. INT. L.J. 203, 225 (2004) (discussing this legislation).

212. As discussed above, the Intelligence Reform Act requires the Department of Homeland Security to issue a report regarding critical infrastructure and to coordinate efforts to identify private-sector resources that could aid the government in preventing or responding to a terrorist attack. *See supra* text accompanying notes 203 and 204.

213. *FOIA Post-9/11*, *supra* note 195, at 289 (quoting *Securing Our Infrastructure: Private/Public Information Sharing: Hearing Before the S. Comm. on Governmental Affairs*, 107th Cong. 97–98 (2002) (statement of Harris N. Miller, President, Information Technology Association of America)).

obtains CFIUS approval of a transfer of control, the interested agencies in CFIUS often condition their approvals on the company's consent to and ongoing compliance with particular requirements or safeguards. To be sure, the agencies may be willing to tailor those conditions to some degree in light of the company's demonstrated business needs.

A. CFIUS Review Process

The Exon-Florio Amendment to the Defense Production Act of 1950[214] gives the President power to suspend or prohibit a foreign interest's acquisition of control over a U.S. business when "[t]here is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security."[215] The President's authority to proscribe transactions is extremely broad and is not subject to judicial review.[216]

The President has directed CFIUS to assist in the exercise of this authority.[217] CFIUS investigates transactions and makes recommendations to the President. Chaired by the Secretary of the Treasury, the committee is made up of members from a wide range of government agencies, including the Departments of Defense, Justice, and Homeland Security.[218]

Exon-Florio does not require the parties to a transaction involving a foreign entity's assumption of control to file a CFIUS notification. Any such filing is voluntary. But if a notice is not filed, the President may, even after the deal has closed, order divestment.[219] Because there is no statute of

214. Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat. 1425 (1988) (codified at 50 U.S.C. app. § 2170).

215. 50 U.S.C. app. § 2170(e)(1); 31 C.F.R. § 800.601(b)(1) (2002).

216. *Id.* § 800.601(b).

217. Exec. Order 12,661, 54 Fed. Reg. 779 (Dec. 27, 1988).

218. Before 9/11, CFIUS had eleven members: (1) the Secretary of the Treasury; (2) the Secretary of State; (3) the Secretary of Commerce; (4) the Secretary of Defense; (5) the Attorney General, representing the Department of Justice (including the FBI); (6) the Chairman of the Council of Economic Advisers; (7) the U.S. Trade Representative; (8) the Director of the Office of Management and Budget; (9) the Director of the Office of Science and Technology Policy; (10) the Assistant to the President for Economic Policy; and (11) the Assistant to the President for National Security Affairs. David A. Menard. *The Flexibility of Exon-Florio Amendment and the Expansion of Telecommunications Into the Global Economy*, 31 PUB. CONT. L. J. 313, 315 (2002).

219. 31 C.F.R. § 800.601(c)(2) (2002); *id.* § 800.401(b) (providing that CFIUS can trigger review of a transaction upon written notice to the parties to the transaction). *See also* Eric Simonson, *Specialized Areas of Concern in Acquisition Transactions*, *in* A GUIDE TO MERGERS & ACQUISITIONS 2005, at 317, 346 (PLI Comm. Law & Practice Course, Handbook Series No. 1461, 2005) [hereinafter *Areas of Concern*] (noting that "[w]hile there is no absolute rule requiring that the parties to a transaction provide such notice, the failure to do so means that CFIUS may commence an investigation at any time").

limitations on CFIUS review, the unwinding of a transaction can be ordered years after it has been completed.[220] By contrast, when parties to a transaction file a voluntary notification, they enjoy a "safe harbor" if their transaction survives CFIUS review.[221] After the committee concludes that an investigation is not warranted or the President declines to prohibit a transaction, that decision cannot be revisited at a later date.[222]

When parties decide to seek the CFIUS safe harbor, they initiate CFIUS review by filing a "voluntary notice."[223] CFIUS then has thirty days in which to decide whether to investigate the transaction.[224] If CFIUS decides to investigate, it must conclude that investigation within forty-five days and then make a recommendation to the President whether to permit the transaction to proceed.[225] The President must act on CFIUS's recommendation within fifteen days.[226] If CFIUS or the President fails to take a required action within any of these statutory deadlines, the government may not thereafter block the transaction or require divestiture under Exon-Florio.[227]

If any of the agencies represented on the committee has concerns about the transaction, negotiations may ensue.[228] In the course of this

220. 31 C.F.R. § 800.601(d) (2002); European Commission, *2004 Report on United States Barriers to Trade and Investment*, at 62 (2004), *available at* http://trade-info.cec.eu.int/doclib/docs/2005/march/tradoc_121929.pdf [hereinafter *European Commission*].

221. *See* Christopher R. Fenton, *U.S. Policy Towards Foreign Direct Investment Post-September 11: Exon-Florio in the Age of Transnational Security*, 41 COLUM. J. TRANSNAT'L L. 195, 209–10 (2002) [hereinafter *Transnational Security*].

222. 31 C.F.R. § 800.601(d)(2)–(3) (2002). There is an exception to this rule for circumstances where a party has submitted false or misleading information to CFIUS. *Id.* § 800.601(e).

223. *Id*, § 800.401(a). An investigation can also begin at the request of a CFIUS member. *Id.* § 800.401(b).

224. 50 U.S.C. app. § 2170(a); 31 C.F.R. § 800.404(a) (2002); *id.* § 800.502(a); *id.* § 800.503(a).

225. 50 U.S.C. app. § 2170(a); 31 C.F.R. § 800.504(a) (2002).

226. 50 U.S.C. app. § 2170(d); 31 C.F.R. § 800.601(a) (2002).

227. The government retains any other authority to challenge the transaction, such as pursuant to the Clayton Act, 15 U.S.C. §§ 12–27. *See* 50 U.S.C. app. § 2170(i) (providing that "[n]othing in this section shall be construed to alter or affect any existing power, process, regulation, investigation, enforcement measure, or review provided by any other provision of law"); 31 C.F.R. § 800.102 (2002) (providing that "[n]othing in this part shall be construed to alter or affect any existing power, process, regulation, investigation, enforcement measure, or review provided by any other provision of law").

228. *See* Kathleen A. Lacey et al., *International Telecommunications Mergers: U.S. National Security Threats Inherent in Foreign Government Ownership of Controlling Interests*, 4 TUL. J. TECH. & INTELL. PROP. 29, 49–50 (2002) [hereinafter *International Mergers*] (describing negotiations preceding CFIUS's approval of a foreign acquisition of a U.S. communications company).

process, companies often are required to agree to conditions sought by CFIUS members. Agreements arrived at through this process then become mandatory conditions to CFIUS approval.[229]

B. FCC Approval of License Transfers

A foreign entity seeking to acquire a U.S. communications company holding FCC licenses must secure the approval of not only CFIUS but also the FCC.[230] If the executive branch—i.e., CFIUS or its members—informs the FCC that consummation of the transaction would raise national security concerns, the FCC will defer acting on the parties' application for transfer of control until the executive branch agencies confirm that the parties have agreed to take satisfactory steps to address those concerns.[231] In practice, this means that the parties to the transaction must negotiate an agreement concerning security issues with the interested agencies, usually the Department of Justice, the FBI, and the DHS, and sometimes the Department of Defense. After the parties have submitted the executed agreement to the FCC, the FCC will (if all other requirements have been satisfied) give its consent to the transfer of control. The FCC also will condition its consent, and the new licensee's continued right to operate under the license, on the licensee's compliance with all of its obligations in the agreement with the executive branch agencies.

C. CFIUS and FCC Approval after 9/11

CFIUS and FCC approval requirements posed hurdles before 9/11 for foreign entities' acquisition of control of U.S. communications companies. Since 9/11, it has become more difficult for foreign businesses to make such purchases. To secure approval, foreign businesses may have to accept more conditions than in the past.

Part of the heightened challenge can be traced to an attitudinal change on the part of those who review transactions. CFIUS is triggered by transactions that may implicate "national security." Neither the Exon-Florio Amendment nor its implementing regulations define the meaning of this pivotal term.[232] And since 9/11 the types of transactions viewed as raising

229. *See* Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT'L L. 441, 498 (2003) [hereinafter *Wall Still Stands*].

230. 47 U.S.C. §§ 214, 310(b) (2000).

231. *See* Rules and Policies on Foreign Participation in the U.S. Telecommunications Market, *Report and Order and Order on Reconsideration*, 12 F.C.C.R. 23,891, paras. 59–62 (1997).

232. Instead, "the definition of 'national security,' and what constitutes a threat, turns on the broad discretion of the administration in power." *Transnational Security*, *supra* note

national security concerns have expanded.[233] Transactions that once might easily have passed muster at CFIUS are now being scrutinized more carefully. This is particularly true of foreign acquisitions of companies possessing telecommunications, computer, and Internet related assets.[234] Former government officials involved in CFIUS reviews have said that, since the terrorist attacks on 9/11, "the administration has stressed its concern about the potential vulnerability of the U.S. telecommunications infrastructure."[235] Noting such developments, the European Telecommunications Network Operators' Association ("ETNO") (the association of incumbent wireline operators in Europe) has asserted that "the current climate may encourage wide interpretation of the scope of Exon Florio, allowing censoring [of] a wide variety of business combinations under the guise of national security."[236] A similar claim has been made with respect to FCC approval, too. The European Commission has said:

> [T]he impact of the events of 11 September has been felt in the telecoms sector as US law enforcement agencies . . . have imposed strict corporate governance requirements on companies seeking FCC approval of the foreign takeover of a US communications firm in the form of Network Security Arrangements going further than before.[237]

One source of the change for companies seeking CFIUS approval is the executive order issued by President Bush in February 2003 making the Secretary of Homeland Security a member of CFIUS.[238] This addition increases the number of security-minded representatives on the committee and makes it potentially more difficult to obtain CFIUS approval. Former senior government officials who served on the committee have noted that the installation of the Secretary of Homeland Security dilutes the influence

221, at 198. However, CFIUS has noted that "transactions that involve products, services, and technologies that are important to U.S. national defense requirements will usually be deemed significant with respect to national security." Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 56 Fed. Reg. 58,774, 58,775 (Nov. 21, 1991).

233. Otis Bilodeau, *Security Hawks Gain Voice in Foreign Deals*, LEGAL TIMES, Apr. 28, 2003, at 1 [hereinafter *Bilodeau*] (noting that there has been a "broadening of what constitutes a national security concern"); *Wall Still Stands*, *supra* note 229, at 498 ("The scope of transactions deemed potentially harmful to national security has been expanding.").

234. *Wall Still Stands*, *supra* note 229, at 498.

235. *Bilodeau*, *supra* note 233, at 19.

236. European Telecommunications Network Operators' Association, *ETNO Reflection Document in Response to DG External Relations' Consultation "Strengthening the EU-US Economic Partnership"*, at 1 (2004) [hereinafter *ETNO*]; *see also id.* at 3 (noting that, "[i]n the wake of the 11th of September 200[1] the concerns behind the law have been amplified considerably").

237. *European Commission*, *supra* note 220, at 73.

238. Exec. Order 13,286, 68 Fed. Reg. 10,619, 10,631 (Feb. 28, 2003).

of those in favor of international investment.[239]

As a result of these changes, communications companies have found it more difficult to obtain approval for their transactions. For example, Hutchison Whampoa was blocked when it tried to acquire a share of bankrupt Global Crossing.[240] Hutchison had partnered with Singapore Technologies Telemedia ("STT"), a company owned in part by the government of Singapore. From the start, CFIUS expressed concern about Hutchison's possible ties to the Chinese government.[241] Both Hutchison and STT proposed a series of safeguards in an attempt to meet the committee's concerns: to place Global Crossing's U.S. assets within a "secure" U.S. subsidiary staffed and operated by U.S. citizens;[242] and when that failed, to limit Hutchison to the role of a passive investor.[243] Under the latter plan, four U.S. citizens would control Hutchison's ownership interest and sit on Global Crossing's ten-member board.[244] This did not satisfy CFIUS, which announced that it would undertake an investigation of the proposed transaction. At that point, Hutchison withdrew from the transaction. STT took over Hutchison's portion of the deal and submitted a new notice to CFIUS.[245] Eventually, the transaction was approved in September of 2003.

Even though it secured CFIUS approval, STT was required to agree to a number of conditions.[246] This is not unusual. ETNO has said:

> strict minimum requirements for any future acquisition will include extensive oversight by the US Government of key operations of the purchasing entity; strict visitation and communications policies for foreign nationals; stringent corporate governance requirements (such as the appointment of Security Directors and a Security Committee); appointment of a third party auditor; and increased screening of sensitive personnel (such as citizenship and security clearances for key

239. *Bilodeau*, *supra* note 233, at 1.

240. This proposed deal raised a number of eyebrows because Global Crossing operated an extensive fiber-optic network that the U.S. government used for some of its communications. Stephen Labaton, *Pentagon Advisor is Also Advising Global Crossing*, N.Y. TIMES, Mar. 21, 2003, at C1.

241. Drew Cullen, *China Fears Shatter Hutch Global Crossing Bid*, THE REGISTER, May 1, 2003, *available at* http://www.theregister.co.uk/2003/05/01/china_fears_shatter_hutch_global/ [hereinafter *China Fears*].

242. *Bilodeau*, *supra* note 233, at 19.

243. *Id.*

244. *Id.* Hutchison and STT proposed that those four positions be filled with very prominent Americans, including former Defense Secretary James Schlesinger and outgoing Merrill Lynch Chairman David Komansky. *Id.*

245. *See China Fears*, *supra* note 241.

246. Press Release, Global Crossing, Global Crossing Receives CFIUS Approval for ST Telemedia Investment (Sept. 19, 2003), *available at* http://www.globalcrossing.com/xml/news/2003/september/19.xml.

persons).[247]

In addition, the government has sought to raise the bar still more for foreign acquisitions of U.S. companies. One recent proposal by the Department of Defense would have made it mandatory for companies to file CFIUS notices in most cases.[248] Although that proposal was shelved,[249] other legislative and regulatory efforts to strengthen the CFIUS and FCC review processes will continue.[250]

D. Considerations When Seeking Approval

Although CFIUS review has become more difficult since 9/11, foreign groups still can acquire U.S. communications companies. By anticipating the challenges that they will face, foreign companies can substantially reduce the risk that CFIUS will trump their cross-border initiatives.

As discussed, CFIUS appears more inclined to find that, at least at first blush, foreign acquisitions of U.S. companies may present national security concerns. While this perception may tempt non-U.S. companies to try to avoid CFIUS scrutiny by not filing voluntary notifications, that tactic cannot succeed in the case of acquisitions of many communications companies. Whether or not a foreign business files with CFIUS, it must file applications for transfer of control of FCC licenses, and that necessarily means that the agencies in CFIUS will become aware of the proposed transaction. The FCC then will not approve the transfer until the executive branch participants sign off. Thus, the better course is for the purchaser to deal with CFIUS from the outset, including submitting a voluntary notice at the appropriate time and negotiating an agreement that meets CFIUS's concerns.

247. *ETNO*, *supra* note 236, at 3.

248. *See* Peter Spiegel, *Pentagon Retracts Plan for Review of Mergers*, FINANCIAL TIMES, Apr. 18, 2002, at 10 [hereinafter *Spiegel*]; ORGANIZATION FOR INTERNATIONAL INVESTMENT, PROHIBITIONS TO CROSS-BORDER ACQUISITIONS: DOD PROPOSAL TO MAKE EXON-FLORIO MANDATORY, *available at* http://www.ofii.org/issues/background/background_probhib.cfm (last visited Mar. 22, 2005) [hereinafter ORGANIZATION FOR INTERNATIONAL INVESTMENT].

249. *See Spiegel*, *supra* note 248; ORGANIZATION FOR INTERNATIONAL INVESTMENT, *supra* note 248.

250. *See* ORGANIZATION FOR INTERNATIONAL INVESTMENT, *supra* note 248 (noting that the "DOD reportedly has not given up on the measure or its interest in compulsory filings. It is our understanding that the proposal may resurface as congressional legislation"); *see Transnational Security*, *supra* note 221, at 232 (noting that "immense public and Congressional pressure to eliminate the security gaps that contributed to the United States' present state of vulnerability could translate into legislative insistence on a greater executive role").

Participants in certain types of transactions should take particular care in navigating the CFIUS approval process. The most obvious is when the acquiring company is owned or controlled by a foreign government.[251] Law enforcement and intelligence officials assert that control over U.S. communications facilities gives foreign governments too much knowledge about U.S. surveillance targets and techniques.[252] And control over key infrastructure could empower a hostile foreign government to shut down portions of the U.S. communications system.[253] Exon-Florio was amended to require a 45-day CFIUS investigation of *any* transaction implicating national security where a foreign government acquires a U.S. company.[254] And Hutchison's attempted purchase of a share in Global Crossing suggests that acquisitions involving foreign governments will now be viewed with a heightened level of scrutiny.[255]

CFIUS also takes a greater interest when the acquired company handles sensitive communications, including military or government communications.[256] The concern is that the foreign purchaser will be in a position to offer sensitive information to foreign governments or other parties.[257] The United States also is very protective of its cutting-edge

251. *See generally International Mergers*, *supra* note 228 (describing the special concerns raised when foreign governments seek control over U.S. communications companies).

252. *See id.* at 35. The *International Mergers* Article explains:

> Ownership and control of U.S. communications networks gives a foreign government the capacity to gain access to confidential information about the targets of U.S. national security and law enforcement investigations, the nature of those investigations, and the sources and methods used, as well as information about the extent to which the U.S. government is aware of foreign governments' intelligence activities.

Id. *See also id.* at 49–50 (noting that approval of a recent transaction was only offered after the acquiring company agreed to ensure that there would be no foreign government involvement in wiretapping over the company's facilities).

253. *Id.* at 36–37.

254. 50 U.S.C. app. § 2170(b); *see Transnational Security*, *supra* note 221, at 206–08 (describing the history of the amendment); *see also id.* at 207–08 (noting that such transactions must be reviewed when they "could affect" national security, while the general standard refers only to transactions that "threaten[] to impair the national security").

255. *See International Mergers*, *supra* note 228, at 48–56 (describing recent examples where foreign government control of the acquiring company was a significant hurdle to CFIUS approval).

256. *Areas of Concern*, *supra* note 219, at 351-52, 347.

257. *See Transnational Security*, *supra* note 221, at 236 (noting that "control over telecommunications and information technologies" could permit foreign entities to use such infrastructure "for the purpose of espionage [and] could lead to foreign access of classified government information that could hinder American military and diplomatic efforts"); *International Mergers*, *supra* note 228, at 36 (noting that "there are concerns that foreigners could use control of phone networks in the United States to conduct surreptitious electronic surveillance on business conversations and to steal trade secrets, or that foreign companies

technology. CFIUS looks carefully at transactions that might undermine the technological advantages of U.S. companies.[258] There also is a growing desire that foreign companies not be in a position to transfer state-of-the-art technology to a foreign government or an undesirable third party.[259]

Companies aware that their acquisitions are likely to arouse the interest of CFIUS can take a number of steps to minimize the burdensome requirements imposed as conditions to the approval of their transactions. Some difficulties can be avoided if attention is paid to the way in which a transaction is structured.[260] For example, ensuring that U.S. persons remain in key management positions after the transfer of control can help address some concerns.

Companies also can minimize the difficulty of obtaining approval by anticipating the concessions that they will be required to make and including such features in their transactions from the outset. It seems clear that a transaction will not be approved unless law enforcement has assurance that foreign control of a company will not inhibit its ability to use that company's facilities for surveillance.[261] Similarly, communications of U.S. persons may be routed overseas by foreign entities only in limited circumstances.[262] When such details are discussed early, there will likely be fewer roadblocks to approval.

Special issues arise when the company to be acquired possesses security clearances.[263] Although CFIUS may choose not to block such transactions, the acquired company may be stripped of its clearances[264]

might work on behalf of their own countries' intelligence services, using U.S. telecommunication devices to funnel information back to their home country").

258. *See* 50 U.S.C. app. § 2170(f)(5) (directing the President to consider "the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security"); *see Transnational Security*, *supra* note 221, at 234 (speculating that "CFIUS would be inclined to review, and perhaps restructure, the acquisition of a company that produces any of a number of new technologies").

259. *See Transnational Security*, *supra* note 221, at 215, 243–46.

260. *Id.* at 213 n.92 (noting that "[r]estructuring could also be initiated by the foreign company in anticipation of government disapproval").

261. *International Mergers*, *supra* note 228, at 35.

262. *Id.* at 35–36 & n.33 (noting that the FBI often fears that it will lose the ability to enforce surveillance orders "when entire or significant components of the communications systems operating in the United States are located outside our borders" and that, accordingly, the FBI insists on essential facilities and data being located within the United States).

263. *Areas of Concern*, *supra* note 219, at 351–52.

264. In those instances where a company is determined to be under "foreign ownership, control, or influence," as defined by the Department of Defense, the company is ineligible for a security clearance and its existing clearances may be revoked. *Id.* at 352.

unless safeguards for the protected information are put in place.[265] For example, foreign persons should not be placed in key management positions or on the company's board of directors.[266] Similar issues arise when the acquired company possesses certain types of export licenses.[267]

In sum, while CFIUS was becoming more visible in the years prior to 9/11, it now plays a lead role in regulatory clearances for foreign acquisitions of communications companies. Foreign entities seeking to deal successfully with CFIUS need to plan in advance and anticipate CFIUS's concerns. Companies contemplating a transaction that could trigger CFIUS review do well, first, to consider the changes that the post-9/11 environment has wrought in this interagency process and, second, begin the necessary consultations very early to address any national security concerns that CFIUS might have.

V. ECONOMIC SANCTIONS AND EXPORT CONTROLS

For decades, the United States has maintained extensive controls on the export and reexport of sensitive goods and technologies. The U.S. government also has imposed economic sanctions against designated countries and persons based on foreign policy and national security considerations. Since 9/11, the government has stepped up its enforcement activity against companies and individuals who violate these controls and sanctions. The export control regulations are complex and can present difficult compliance responsibilities.

A. Taxonomy of Export Control Rules

The Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces U.S. economic sanctions.[268] OFAC

265. *See id.* at 352–53 (noting that, "[b]y carefully structuring a transaction and the operations of the acquired business going forward, it is sometimes possible to obtain or maintain security clearances notwithstanding modest amounts of foreign ownership of a parent company").

266. *See id.* at 352.

267. *See, e.g.*, 31 C.F.R. § 800.402(c)(4) (requiring parties filing CFIUS notices to state whether the company to be acquired produces technical data or products subject to certain export controls). *See also* 22 C.F.R. § 122.4(b) (requiring companies that export certain defense articles to notify the Department of State's Office of Defense Trade Controls at least 60 days before a transfer of ownership or control to a foreign person).

268. OFAC regulations apply to "United States persons," i.e., all companies organized in the United States, including the overseas branches of those companies; all U.S. citizens or permanent residents located anywhere in the world; and all individuals, entities, and property located in the United States. *See, e.g.*, 31 C.F.R. § 560.314 (2002). U.S. economic sanctions imposed against Cuba and North Korea also apply to foreign subsidiaries of U.S. companies. *See, e.g.*, *id.* § 515.329. No U.S. person may "approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person

sanctions prohibit U.S. persons from engaging in transactions with designated countries such as Cuba, Iran, and Sudan.[269] They also restrict dealings with designated entities and persons. These "Specially Designated Nationals and Blocked Persons" include terrorists, proliferators of weapons of mass destruction, drug traffickers, traders of "conflict diamonds," and others acting as agents of designated countries.[270] The scope of OFAC sanctions varies according to the target. For example, Cuba is subject to embargoes on almost all imports, exports, reexports, travel, investments, and other financial dealings.[271] By contrast, Myanmar is subject to restrictions on certain types of new investments.[272]

The Commerce Department's Bureau of Industry and Security ("BIS") administers the Export Administration Regulations ("EAR"), which control exports and reexports of certain "dual use" (i.e., items suitable for both commercial and military applications) goods, software, or technology.[273] Various factors affect the application of EAR controls.[274] These include the nature of the item at issue and its classification under the EAR.[275] Another key factor is the ultimate destination of any applicable shipment;[276] there are restricted destinations and embargoed countries to which no exports may be made without a prior license.[277] In addition, the end-use or end-user of the product implicates possible licensing requirements.[278] For example, some shipments of technology that could have missile applications are proscribed because they involve a restricted

would be prohibited . . . if performed by a United States person or within the United States." *Id.* § 560.208.

269. *See* 31 C.F.R. pt. 515 (2002) (Cuba); *id.* pt. 560 (Iran); *id.* pt. 538 (Sudan).

270. *See, e.g.*, *id*. pt. 597 (foreign terrorist organizations); *id.* pt. 594 (global terrorism sanctions); *id.* pt. 596 (terrorism list governments); *id.* pt. 539 (weapons of mass destruction); pt. 536 (drug traffickers); *id.* pt. 598 (narcotics kingpins); *id.* pt. 591 (traders of conflict diamonds). The names of persons and organizations on these lists are published in the Federal Register and are available on OFAC's Specially Designated Nationals and Blocked Persons List (Mar. 3, 2005), available on the OFAC website at http://www.ustreas.gov/offices/eotffc/ofac/sdn/index.html.

271. *See, e.g.*, 31 C.F.R. § 515.201 (2002) (prohibited transactions); *id.* § 515.204 (imports); *id.* § 515.205 (blocked accounts); *id.* § 515.560 (travel restrictions).

272. *See, e.g.*, *id.* § 537.201 (new investments); *id.* § 537.404 (purchases of shares in development projects).

273. 15 C.F.R. § 730.1 (2002). The Export Administration Regulations can be found in 15 C.F.R. pts. 730–744. Unlike the OFAC rules, the jurisdiction of the EAR is not limited by the nationality of the person engaged in export activity. Rather, the rules cover the export or reexport of any item "subject to the EAR," as defined in 15 C.F.R. § 734.3.

274. *Id.* § 732.1.

275. *Id.* § 732.1(b)(1), (c).

276. *Id.* § 723.1(b)(2).

277. *See id*. pt. 738, Supp. 1 (containing chart highlighting problem countries).

278. *See id*. § 732.1(b)(3)–(4).

end-use;[279] in other cases, otherwise permissible exports are prohibited under the EAR because they are destined for use by a particular party.[280]

The BIS regulations also control the release or disclosure of technology[281] or software source code to foreign nationals located anywhere in the world, including foreign *employees* of U.S. companies in the United States.[282] When technology or software is released to a foreign national who is not a permanent resident of the United States or a "protected individual" under the Immigration and Naturalization Act,[283] that release is treated as an export to the national's home country under the "deemed export" rule.[284]

The Directorate of Defense Trade Controls ("DDTC") of the U.S. Department of State administers the International Traffic in Arms Regulations ("ITAR").[285] These regulations control exports, reexports, retransfers, and temporary imports of "defense articles" and "defense services," which are items on the U.S. Munitions Lists or goods and technologies specially designed or modified for military applications.[286] Like the EAR, the ITAR also have provisions governing deemed exports to foreign nationals.[287]

B. The Evolution of Economic Sanctions and Export Control Rules after 9/11

The Patriot Act and other post-9/11 legislation did not make significant changes to statutes authorizing the economic sanctions and export control regime. Nevertheless, recent developments present difficult compliance issues and impose new responsibilities.

279. *See, e.g.*, *id.* § 744.3 (restrictions on missile end-uses).

280. *See, e.g.*, *id.* § 744.13 (exports to specially designated terrorists).

281. Technology is defined extremely broadly, to include such things as "instruction, skills training, working knowledge, [and] consulting services." *See id.* § 772.1.

282. "Export" is defined to include the "release of technology or software subject to the EAR to a foreign national in the United States." *Id.* § 734.2(b)(1). *See* Gregory W. Bowman, *E-mails, Servers, and Software: U.S. Export Controls for the Modern Era*, 35 GEO. J. INT'L L. 319, 339 (2004) [hereinafter *Modern Era*].

283. The Immigration and Naturalization Act defines a "protected individual" as a citizen, national, lawful temporary resident, or person granted asylum or refugee status. 8 U.S.C. § 1324b(a)(3) (Supp. 2002).

284. 15 C.F.R. § 734.2(b)(2)(ii) (2002).

285. *See* Joseph J. Dyer, *Export Control: A Visa May Not Be Enough*, MD. BAR J., Mar.–Apr. 2004, at 36 [hereinafter *Visa Not Enough*].

286. 22 C.F.R. § 120.3 (2002).

287. *Id.* § 120.17(a)(4) (providing that the term "export" includes "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad").

Although the number of countries subject to restrictions has declined,[288] there has been a significant increase in the number of entities and persons who appear on U.S. government lists of parties subject to economic sanctions and export controls.[289] Not surprisingly, these expanding lists include government-identified sponsors of terrorism and persons and organizations furthering the proliferation of weapons of mass destruction.[290]

Transactions subject to EAR licensing requirements also have been affected post-9/11. BIS has become increasingly concerned about the export of sophisticated communications equipment, software, and technology. As a result, it tends to scrutinize license requests more closely and to impose more conditions on authorizations that are granted.[291] These conditions mean that companies must extend their compliance responsibilities beyond the point of export from the United States to factors relating to known ultimate uses of the item that is shipped.

In addition, there is an increased expectation that companies engaged in international transactions will implement internal screening procedures in their business operations to ensure compliance with OFAC sanctions.[292] This often includes the use of software to scan and interdict transactions involving prohibited end-users or sanctions targets on government watch lists.[293] For the most part, these programs help companies meet heightened

288. The United States has eased sanctions against Iraq, Libya, North Korea, Afghanistan, Sierra Leone, Liberia, the UNITA faction in Angola, and the countries that were once part of Yugoslavia. *See, e.g.*, Exec. Order 13,357, 69 Fed. Reg. 56,665 (Sept. 20, 2004) (lifting sanctions against Libya); Exec. Order 13,324, 69 Fed. Reg. 2823 (Jan. 15, 2004) (lifting sanctions against Liberia and Sierra Leone).

289. *See Modern Era*, *supra* note 282, at 344, 357; Philip K. Ankel & Glenn H. Kaminsky, *Exporting to Special Destinations and Persons: Terrorist-Supporting and Embargoed Countries, Designated Terrorists and Sanctioned Persons*, *in* COPING WITH U.S. EXPORT CONTROLS 2004, at 175, 181 (PLI Comm. Law & Practice Course, Handbook Series No. 3160, 2004) [hereinafter *Exporting to Special Destinations*].

290. *See Exporting to Special Destinations*, *supra* note 289, at 181. Continually updated lists of Specially Designated Global Terrorists ("SDGTs"), Foreign Terrorist Organizations ("FTOs"), and Specially Designated Terrorists ("SDTs") subject to OFAC prohibitions can be found at http://www.ustreas.gov/offices/eotffc/ofac/sanctions/t11ter.pdf (last visited Apr. 17, 2005).

291. *See generally* 15 C.F.R. pt. 744 (2002).

292. *See, e.g.*, Office of Foreign Assets Control, *Foreign Assets Control Regulations for the Financial Community*, at Part IV, *available at* http://www.treas.gov/offices/enforcement/ofac/regulations/facbk.txt (last visited Apr. 17, 2005) [hereinafter *Foreign Assets Control*] (discussing importance of internal compliance programs for financial institutions).

293. *See, e.g.*, Berne C. Kluber, *Global Distributions: The Effect of Export Controls*, 23 HOUS. J. INT'L L. 429, 452 (2001) ("Faced with the prospect of searching through a series of long, complex lists in different formats, many companies use interdiction software to help them screen customers and transactions.").

standards of care. However, increased screening also presents many burdens, such as undertaking additional due diligence to rule out uncertain screening results and "false positives." Although such procedures help mitigate civil penalties for failure to comply with sanctions, they do not immunize companies from liability.[294] Significant fines have also been imposed on companies that have implemented screening programs but nonetheless failed to uncover impermissible transactions.[295]

"Knowledge" standards and requirements also present compliance issues. Companies face legal liability if they "knowingly" export a commodity subject to the EAR to an end-user or for an end-use that is unauthorized.[296] The BIS may find "knowledge" for these purposes if a "red flag" should have alerted the exporter of a likely violation.[297] Examples of "red flags" include evidence that (1) "[t]he customer is willing to pay cash for a very expensive item when the terms of the sale call for financing"; (2) "[t]he shipping route is abnormal for the product and destination"; and (3) "[r]outine installation, training or maintenance services are declined by the customer."[298] But these examples are neither exhaustive nor necessarily applicable to certain transactions, and exporters bear the burden of determining whether a transaction violates the EAR.[299] The knowledge standard is ambiguous in certain respects, and might soon be revised.[300]

Finally, federal agencies will take enforcement action against companies for export violations committed by the companies they acquire, even when those violations predate the merger or acquisition.[301] A $1.76

294. *See Foreign Assets Control*, *supra* note 292, at Part IV.

295. *See, e.g.*, OFAC Civil Penalties Enforcement Information for January 07, 2005, *available at* http://www.treas.gov/offices/enforcement/ofac/civpen/penalties/01072005.pdf (last visited Apr. 17, 2005) (detailing recent sanctions actions taken against a number of companies with screening programs in place).

296. 15 C.F.R. § 736.2(b)(5) (2002); *see also Wall Still Stands*, *supra* note 229, at 492 (noting that "technology transfers that would not normally require export licensing could require a license because of the nature of the end-use or end-user").

297. These "red flag" indicators are published at 15 C.F.R. pt. 732, Supp. 3. They can be found at http://www.bis.doc.gov/Enforcement/redflags.htm.

298. 15 C.F.R. pt. 732, Supp. 3 (2002).

299. *Modern Era*, *supra* note 282, at 343; *see also* 15 C.F.R. pt. 732, Supp. 3 (providing that "Commerce has developed lists of such red flags that are not all-inclusive but are intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate the EAR").

300. The BIS is currently engaged in a proceeding aimed at further refining the knowledge standard. *See* Revised "Knowledge" Definition, Revision of "Red Flags" Guidance, and Safe Harbor, 69 Fed. Reg. 60,829 (proposed Oct. 13, 2004) (to be codified at 15 C.F.R. pts. 732, 736, 740, 744, 752, 764, 772).

301. Traditionally, successor liability was not believed to attach for export control violations. *See, e.g.*, BUREAU OF INDUSTRY AND SECURITY, ANNUAL REPORT FISCAL YEAR

million fine was levied against Sigma-Aldrich Corporation for export violations committed by a firm that the company purchased.[302] Similarly, Boeing Satellite Systems, Inc. was required to pay $32 million to settle charges brought against it for the acts of a company that it acquired.[303]

C. Ways To Minimize Potential Liability

Keeping up with complicated export rules and constantly changing government lists of sanctioned persons and prohibited end-users is challenging even for the most sophisticated of companies.[304] And the penalties for violating the rules are severe, including criminal prosecution, large monetary penalties, and loss of export privileges.[305] Companies exporting goods and technologies should design and implement comprehensive compliance policies and establish mechanisms for updating those policies as the rules change.[306] Given the complexity of the rules, this is no easy task.

As part of that undertaking, companies should develop effective

2003, Statement of the Secretary and Under Secretary, *available at* http://www.bxa.doc.gov/News/2004/03AnnualRept/#Letter (noting that a BIS enforcement case in 2003 "made new law" by "establish[ing] the precedent of successor liability for violations of the Export Administration Regulations").

302. BIS's decision is available at http://www.bis.doc.gov/Enforcement/CaseSummaries/Sigma_Aldrich_ALJ_Decision_02.pdf. Research Biochemicals Limited Partnership, the company that Sigma Aldrich acquired, allegedly made illegal exports of biological toxins. *Id.*

303. *Hughes, Boeing Pay $32M to Settle Charges Of Sensitive Technology Transfers to China*, 79 FED. CONT. REP. (BNA) No. 10, 281, 303 (Mar. 11, 2003). Kenneth Juster, Under Secretary of Commerce for Industry and Security, has stated that "corporations will be held accountable for violations of U.S. export control laws committed by companies that they acquire." Press Release, Bureau of Industry and Security, Sigma-Aldrich Pays $1.76 Million Penalty to Settle Charges of Illegal Exports of Biological Toxins (Nov. 4, 2002), *at* http://www.bxa.doc.gov/News/2002/SigmaAldrichPays4Acquisition.htm [hereinafter Sigma-Aldrich Press Release].

304. Nathan T.H. Lloyd, *Rebuilding a Broken Regime: Restructuring the Export Administration Act*, 37 VAND. J. TRANSNAT'L L. 299, 299 (2004) [hereinafter *Broken Regime*] (complaining in the abstract that "a multitude of statutes and regulations govern dual-use technology transfers, forming a bureaucracy that is impossible to adhere to for the private sector. . . .").

305. *See, e.g.*, 31 C.F.R. § 501.701 (2004) (OFAC criminal and civil penalties); 15 C.F.R. § 764.3(b)(2) (2002) (BIS criminal penalties, civil penalties, and denial of export privileges).

306. In addition to helping companies comply with the export control rules, such policies are essential in the event that a company violates those rules. The federal sentencing guidelines provide that the existence of a compliance program is a mitigating factor in assigning the penalty for a violation. UNITED STATES SENTENCING COMMISSION, GUIDELINES MANUAL § 8C2.5(f) (Nov. 1, 2004). *See also Wall Still Stands*, *supra* note 229, at 515 ("Should a violation occur, existence of a compliance program should serve as a mitigating factor in an investigation.").

screening policies to identify suspect transactions.[307] Difficult issues often arise in identifying and resolving "false positives." Further, internal screening measures should be continually updated because the government lists can frequently change.

Communications companies with export licenses conditioned on the end use or end user of the export can gain some measure of protection by acquiring an "end-user certificate" from the buyer stating that the product will not be used in a prohibited way.[308] As noted, exporters also should pay close attention to possible "red flags" that a product may be destined for a prohibited end-use or end-user.[309]

Due to the growing number of foreign nationals employed by U.S. companies in the technology sector, one of the most difficult issues for many communications providers is dealing with the "deemed export" rule. To avoid violations, companies must determine whether any of their products or services are subject to EAR or ITAR licensing requirements and, if so, the citizenship and visa status of each foreign person who has access to those products or services. In doing this, companies should be mindful of employment discrimination laws, which prohibit discrimination on the basis of national origin or citizenship status.[310] One solution is for companies to obtain BIS or DDTC licenses for those employees who are likely to require access to sensitive technologies.[311] However, obtaining such licenses may be time-consuming, and maintaining compliance with such authorizations can be difficult.[312]

Communications providers can also take steps to reduce or eliminate

307. *See* 15 C.F.R. pt. 732, Supp. 3. The Code specifically states:

> Employees need to know how to handle 'red flags'. Knowledge possessed by an employee of a company can be imputed to a firm so as to make it liable for a violation. This makes it important for firms to establish clear policies and effective compliance procedures to ensure that such knowledge about transactions can be evaluated by responsible senior officials.

308. *Broken Regime*, *supra* note 304, at 315.

309. *Id.*

310. *See, e.g.*, Cynthia J. Lange & Richard J. Pettler, *Recruiting Workers Post 9-11: How to Avoid Immigration Discrimination While Considering Export Control Concerns*, *in* 35TH ANNUAL IMMIGRATION & NATURALIZATION INSTITUTE, at 95, 98 (PLI Corporate Law and Practice Course, Handbook Series No. 1340, 2002) [hereinafter *Immigration Discrimination*].

311. *Visa Not Enough*, *supra* note 285, at 36.

312. *See, e.g.*, *Immigration Discrimination*, *supra* note 310, at 101 (noting that, "[d]epending on the nature of controls, nationality of the foreign national, and other applicable licensing policies, the adjudication process may take 2 to 18 months"); *Wall Still Stands*, *supra* note 229, at 528 (noting that "[w]hen deemed-export licenses are issued, they often are subject to conditions, such as restrictions on the foreign national's access to high-performance computers, advanced microprocessors, or certain semiconductor production equipment").

the possibility that they will be subject to successor liability for the prior misdeeds of the companies they acquire. Providers embarking on mergers or acquisitions should perform an export control compliance review as part of the due diligence work conducted prior to the transaction. This may permit them to identify potential liabilities and more accurately price the company they seek to acquire. Such a review might also reveal the need to add export-control-related indemnification provisions to transaction agreements. As one senior BIS official has noted, "when acquiring another firm, a company should scrutinize the export control practices of the acquired company in order to avoid the risk of incurring substantial liability along with the assets of the company."[313]

Finally, communications companies can protect their interests by keeping abreast of developments affecting export controls. As part of the war on terrorism, there are frequent proposals for new legislation and regulations to tighten existing economic sanctions and export controls and to limit the extent to which U.S. companies may communicate with their foreign subsidiaries.[314] For example, Senator Lautenberg recently proposed an amendment to the fiscal year 2005 defense authorization bill[315] that would have prohibited foreign subsidiaries or affiliates of U.S. companies from engaging in transactions with countries on the State Department's terrorism watch list.[316] Similarly, Senators Grassley and Baucus requested in February 2004 that OFAC provide further guidance as to the scope of permissible dealings between U.S. parent companies and their foreign subsidiaries.[317]

313. Sigma-Aldrich Press Release, *supra* note 303, (quoting Michael J. Garcia, Assistant Secretary of Commerce for Export Enforcement).

314. One commentator notes that "the events of and following September 11, 2001 . . . [have] led some observers to conclude that U.S. commercial export controls need to be strengthened, not eased, in light of the threat of terrorism and weapons proliferation." *Modern Era*, *supra* note 282, at 325.

315. *See* National Defense Authorization Act for Fiscal Year 2005, S. 2229, 108th Cong., 2d Sess. (2004).

316. Discussion of the amendment can be found at 150 CONG. REC. S5729, S5768, S5777 (daily ed. May 19, 2004). The amendment was narrowly defeated in a 50-49 vote. *Id.* at S5785.

317. Press Release, Senator Chuck Grassley, Grassley, Baucus Seek Answers on U.S. Companies' Dealings With Countries Named as Terrorism Supporters (Feb. 19, 2004), *available at* http://grassley.senate.gov/releases/2004/p04r02-19.htm.

VI. INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

The recently passed Intelligence Reform and Terrorism Prevention Act of 2004 ("Intelligence Reform Act")[318] contains provisions that may give rise to new burdens on and opportunities for communications providers.[319] Several sections of the Act require the DHS to consult with communications providers. One requires the Department to coordinate industry efforts to identify private sector resources that could help the government prevent or respond to terrorist attacks.[320] Another encourages the Department to promote adoption of voluntary national preparedness standards for the private sector.[321] A third requires the Department, in consultation with the FCC and communications providers, to study the feasibility and desirability of an emergency alert system designed to issue telephonic warnings in the event of a terrorist attack.[322] These provisions place obligations only on the DHS. But they are likely to give rise to government information requests and new consultations.

The Act contains two other provisions that also should be of interest to communications providers. Both sections address communications interoperability. The first directs the Secretary of Homeland Security, in consultation with the FCC, to "establish a program to enhance public safety interoperable communications at all levels of government."[323] It requires establishment of a comprehensive national approach to achieving interoperable communications for public safety providers,[324] and it directs the Secretary to accelerate development of voluntary national consensus

318. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (codified at scattered sections U.S.C.).

319. In addition to the provisions discussed below, the Intelligence Reform Act contains sections addressing critical infrastructure information and the government's surveillance authority. *See, e.g.*, Intelligence Reform Act § 7306 (requiring the Department of Homeland Security to issue a report on threats to the nation's critical infrastructure). *See id.* § 6001 (providing for FISA surveillance of "lone wolf" terrorists); discussion *supra* Part I and Part III.

320. Intelligence Reform Act, § 7402(3).

321. *Id.* § 7305(b).

322. *Id.* § 7403.

323. *Id*. § 7303(a)(1). The Intelligence Reform Act provides:

> "[I]nteroperable communications" means the ability of emergency response providers and relevant . . . government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another on demand, in real time. . . .

Id. § 7303(g)(1).

324. *Id.* § 7303(a)(1)(A).

standards for such communications.[325] It also encourages the development and implementation of flexible and open architectures aimed at providing solutions to public safety communications interoperability.[326] Finally, it requires the establishment of mechanisms for coordinating communications interoperability in high-risk urban areas[327] and cross-border interoperability between the United States and other countries.[328] The second provision directs the Secretary, in consultation with the FCC, to assess strategies for meeting public safety telecommunications needs.[329] It provides that the Secretary shall consider "the need and efficacy of deploying nationwide interoperable communications networks" and "technical and operational standards and protocols for nationwide interoperable broadband mobile communications networks. . . ."[330]

The development of standards—particularly if the standards are used to guide grant-making and other spending—will cause migration to fewer systems, particularly in the communications equipment used by public safety personnel. Suppliers of such systems will need to engage with the DHS on this process. Though the contemplated standards are voluntary, the studies mandated by these provisions could lead to required technological or equipment standards. The Act also provides a source of funding for state and local governments seeking to upgrade their existing communications systems, raising the specter of those entities reducing their purchases from private communications providers and competing with those providers.[331]

Of course, these sections also present an opportunity for some communications companies. The Act directs that interoperable emergency communications systems be deployed as soon as possible for use by first responders.[332] Communications providers that win contracts to design, install, and offer service over these systems may benefit from business relationships with a wide range of government entities. And, as the 9/11 Commission noted, the nation's security is enhanced if first responders can

325. *Id.* § 7303(a)(1)(D).

326. *Id.* § 7303(a)(1)(E).

327. *Id.* § 7303(d) (requiring the Department of Homeland Security, in consultation with the FCC, to support the rapid establishment of effective interoperable communications capabilities in the event of an emergency in urban areas where the risk of a terrorist attack is high).

328. *Id.* § 7303(c) (requiring the President to establish a mechanism to coordinate cross-border interoperability issues between the United States and Canada and between the United States and Mexico).

329. *Id.* § 7502(b).

330. *Id.* § 7502(b)(1).

331. *Id.* § 7303(e).

332. *Id.* § 7303(i)(2).

better communicate with one another.[333]

VII. CONCLUSION

If one theme connects these areas of heightened governmental interest and strengthened governmental power, it is that the communications infrastructure in the hands of the private sector is critically important to the public safety of the people of the United States. In the aftermath of 9/11, the government sought to ensure that its investigators would get the information that they need and that our communications pathways would remain available to us and free from malicious interference. These efforts have presented new and very difficult challenges to the companies that control this infrastructure. By identifying and remaining conscious of those challenges—both to the interests of the shareholders and to the privacy rights of consumers and citizens—industry participants can better acquit their multiple responsibilities and, where necessary, help the government adjust its own approach to these difficult and important efforts.

333. *See 9/11 Commission Report*, *supra* note 183, at 396–97.