LATHAM & WATKINS LLP

Case Study on Lawful Intercept

Presented to:
Harvard Law School
Cyber Law And The Global Economy

Thursday, November 11, 2004

Presented by:
Tim Ehrlich
Latham & Watkins LLP
Email: tim.ehrlich@lw.com

CASE STUDY ON LAWFUL INTERCEPT

You are an in-house attorney for a large IP networking equipment manufacturer which is headquartered in the United States and has subsidiaries all over the world. In June of 2001, the general counsel asks you to take responsibility for the company's legal strategy on the topic of "lawfully authorized electronic surveillance" (commonly referred to as "lawful intercept" or "LI"). He mentions to you that some of your service provider customers, the vast majority of whom provide IP-based communications services (e.g., high speed and dial-up internet access, web and IP-based telephony services, etc.), have started to ask pointed questions about your company's technological approach to lawful intercept. Some have even made mention of deadlines for compliance with their country's laws. He has asked you to monitor this situation and to serve on a worldwide team tasked with developing the company's global technical strategy for LI and to provide legal and regulatory guidance to that group. After accepting the general counsel's offer, you conduct some initial research on the topic of LI. You discover that some of the countries in which the greatest number of your customers do business, including the United States and Germany, have indeed set firm compliance deadlines for their lawful intercept laws, but that none of those deadlines is imminent. Consequently, you spend the next few months bringing yourself up to speed on the LI laws around the world and monitoring the progress of your company's technical development efforts.

Less than three months after accepting this position, the tragic events of September 11th take place, after which both your company and your customers find themselves in a dramatically different legal and technological environment. Shocked and frightened by the unprecedented scope and impact of the terrorist acts, the United States, along with many other countries around the world, are left to question how the terrorists could have planned and executed such coordinated acts of violence largely without detection by law enforcement. Particularly relevant for your company's work on lawful intercept is the discovery that Al Qaeda may have used the Internet and other advanced communications technologies to plan the attacks on the United States.[1] At least in part due to this discovery, the amount of interest shown by the governments around the world in the area of wiretapping and interception of all forms of IP-based communications increased dramatically in the months following 9/11.

Despite this interest, however, many countries found their access to the technologies capable of permitting them to intercept and spy on these new criminal methods was

[1] See, e.g. Kevin Maney, Osama's Messages Could be Hiding in Plain Sight, USA Today, December 19, 2001 at B6 (noting Al Qaeda's use of advanced technologies such as encrypted Internet communications and steganography); Greg Wright, "Terrorists Leave Their Footprints Across Internet," Denver Post, October 8, 2001 at E2 (noting the likely use of encrypted e-mail, chat rooms and even Internet audio and digital images by Osama bin Laden to communicate with his 'cells' around the world); Ariana Eunjung Cha and Jonathan Krim, "Terrorists' Online Methods Elusive," Washington Post, September 19, 2001 at A14 (citing the federal government's difficulty in tracking down and deciphering secret messages embedded in mundane e-mails and on Web sites used by Al Qaeda.

blocked by a myriad of legal and technical hurdles. While a few governments had updated their legal systems in the late 1990s to account for criminals' increasing use of new technologies such as email, cell phones and the Internet to commit crimes, many others still had laws which were either outdated or which failed to address the unique challenges which IP-based technologies, such as high-speed DSL services, presented to law enforcement's interception efforts. In the interest of protecting national security and of closing these increasingly apparent technical and legal gaps, a number of governments pushed up the deadlines for compliance with existing laws relating to lawful intercept. Others enacted new laws giving law enforcement agencies enhanced intercept powers, often at the explicit behest of those agencies.

In the United States, for example, the Federal Communications Commission dramatically pushed up the deadlines for compliance with the Communications Assistance for Law Enforcement Act (discussed in greater detail below) after 9/11. Particularly relevant for your customers was the FCC's decision in late September 2001 (amid obvious pressure from the FBI)[2] to end its longstanding tradition of granting industry requests for repeated, annual extensions of the compliance deadline for all packet-based (including IP-based) communications. Instead, the FCC agreed to extend the deadline by only two months, until November 19, 2001. While recognizing the technical challenges associated with compliance in his Order announcing the limited extension, FCC Commissioner Michael Copps acknowledged that these technical and financial concerns had been outweighed by the recent tragic events of 9/11: "[w]e view this brief extension as extraordinary relief necessary in the interests of fairness and reasonableness and do not expect to grant any further extensions on an industry-wide basis with respect to packet-mode communications."[3] The U.S. Congress also created a new law to deal with these enhanced threats to national security, namely the USA Patriot Act[4] which was enacted on October 26, 2001. The Patriot Act introduced immediate and significant changes to the country's existing electronic surveillance laws. These changes included an expansion of law enforcement's powers to intercept new forms of IP-based communications and a broadening of the scope of the existing surveillance laws to cover non-traditional communications providers.

---

[2] In his testimony before Congress on September 25, 2001, Attorney General John Ashcroft stated: "Terrorist organizations have increasingly used technology to facilitate their criminal acts and hide their communications from law enforcement. Intelligence gathering laws that were written for the era of land-line telephone communications are ill-adapted for use in communications over multiple cell phones and computer networks. . . .Our proposal [for the USA Patriot Act] . . . ensur[es] law enforcement's ability to trace the communications of terrorists over cell phones, computer networks and new technologies that may be developed in the coming years." See http://216.239.57.100/search?q=cache:0vAG72qq4loC:www.techlawjournal.com/alert/2001/09/26.asp+Ashcroft+FCC+surveillance+authority+FBI++2001&hl=en&ie=UTF-8

[3] FCC 01-265 Order by Commissioner Copps http://216.239.39.100/search?q=cache:01Vq7Icl0I8C:www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01265.pdf+FCC+commissioner+copps+packet+compliance+%22september+21%22++%22november+19%22+2001&hl=en&ie=UTF-8

[4] Pub. L. 107-56, 115 Stat. 272. The formal title is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."

Taking a similarly proactive response to the events of 9/11, the German government passed the Telecommunications Interception Ordinance (TKUV) on January 29, 2002. This Ordinance explicitly authorized German security services to conduct surveillance of emerging technologies (including IP) and imposed strict compliance deadlines on the companies providing those services. Similarly, on August 1, 2002 the British Parliament passed Order number 1931, pursuant to the Regulation of Investigatory Powers Act, in which it imposed specific technical obligations on certain types of service providers to maintain a permanent intercept capability. Finally, the Council of Europe's Convention on Cybercrime, which was signed shortly after 9/11 on November 26, 2001, provided for mutual assistance among the signatory countries in the fight against cybercrime. Specifically, the Convention required the signing countries to adopt legislative measures necessary to compel Internet Service Providers ("ISPs") to maintain an ability to conduct real-time interception of their communication services and to provide that information to a signatory country upon request.[5]

This increase in attention and activity in the area of surveillance and wiretapping did not go unnoticed by the press or by privacy advocates. For example, a search of Westlaw in the spring of 2003 for articles written within one year of 9/11 and containing the words "surveillance" and "September 11" returned three hundred and forty four articles. Adding the word "wiretap" to the same search returned ninety-two articles. A search of the word "surveillance" for the period from September 11, 2001 to March 26, 2003, almost two and a half years later, returned over three thousand two hundred articles. Similarly, one need only glance at a few of the titles gracing US and foreign news publications following 9/11 to witness the increase in concern for the loss of personal privacy rights that emerged in the wake of government demands for increased authority to intercept communications. The title of a September 16, 2001 Agence France Press article, for example, read "US to seek expanded surveillance powers after terror strikes." Similarly, the UK's "Daily Mail" ran a headline on June 12, 2002 that read "March of Big Brother; Your Phone Calls, Emails, Medical Records: the Government and its Spies Want Access to Them All," while the Wall Street Journal Europe ran an article on September 27, 2001 entitled "Bush is Seeking More Surveillance, But Will it Work? FBI May Collect More Data Than it Can Actually Track –A Fight over Civil Liberties."

As a direct result of all of this activity on LI, many of your customers have found themselves under substantial pressure from their local governments and law enforcement agencies to take affirmative steps to assist in the interception of their customer's communications, including through the purchase of new equipment and possibly even reconfiguration of their existing networks.[6] Not surprisingly, they have turned to your

[5] A number of other countries also established laws after 9/11 to address what was seen as a widening gap between the powers of law enforcement to intercept new forms of communications and the ability of terrorists and criminals to leverage those technologies to their advantage. Austria, for example, published a decree on the lawful interception of telecommunications in February 2002 and set a compliance deadline of June 1, 2002. Similarly, Canada issued a draft proposal in August of 2002 which would force ISPs to rewire their networks to ensure easier surveillance by Canadian law enforcement and to build a database of every Canadian with an Internet account.

[6] While a number of different types of service providers, including traditional local voice service providers, such as Verizon and SBC, and cellular phone service providers, felt the impact of this increased interest in

company as the primary provider of their networking equipment to help them meet their legal obligations. Some have simply asked to learn more about your company's general approach to LI and how they might leverage it to meet their obligations. Others have gone so far as to demand that your company give legal guarantees that your products will enable them to meet their LI obligations and to pay any penalties in the event of non-compliance. As a company with a very strong customer focus, you are eager to meet your customers' requests. At the same time, you are also concerned about balancing those requests with any laws that impose affirmative obligations on your own company, including substantial financial penalties for non-compliance. More generally, in a tough telecom market it is especially important for you to be sensitive to any factors, including unhappy customers and stiff legal penalties, that could hinder your company's ability to do business on a world-wide basis.

Given these facts, your company has asked you to assess its current strategy for LI in order to make sure that (1) it is sufficient to shield it from financial and legal risk, and (2) it is flexible enough to meet the evolving technical requirements of governments and customers around the world. As part of this assessment, you have been asked to analyze the laws on lawful interception of IP-based communications in three of your company's biggest markets, the United States, the United Kingdom and Germany. The objective of this analysis is to try to discern where the laws in these three countries appear to converge or diverge, and if so, then why. The expectation is that your company will be able to leverage this information to develop an effective global strategy for LI that allows it to take advantage of all possible economies of scale and to carve a careful middle ground through the legal and technical idiosyncrasies of the different countries.

I. BACKGROUND

Both the idea and the technology for intercepting personal communications have been around since the beginning of the 20th century. Almost since the advent of the telephone in the late 1800s law enforcement and others have devised ways to "tap" or listen in to people's conversations.

From the early 1900s up to the 1970s, interception of communications was affected by law enforcement in a fairly consistent and easy manner. In order to find out who an individual suspect was calling (i.e. the phone numbers they were dialing out), police would simply attach a device called a "chart recorder," which later became known as a "pen register," to the phone lines coming directly from the individual's house. The pen register device would draw a spike on a chart of paper for each electrical impulse that was generated by the dialing of the phone in the individual's house. For example, when the number 1 was dialed, one spike was drawn on the chart, and when the number 2 was

---

lawful intercept and the passage of new laws, the vast majority of your company's products are sold to providers of IP-based communications. Therefore the focus of your company's concern will be on how the various laws impact those types of communications.

dialed, two spikes were drawn on the chart, etc.[7] In order to find out who called a suspected target ("trap and trace"), law enforcement would simply ask the phone company delivering the call to trace it back mechanically (i.e., by hand) to each local central office that had carried the call from the sender, all of which were owned by the same company (i.e., Ma Bell).

Intercepting the content of telephone calls prior to the 1970s was equally straightforward. All that was required for law enforcement to listen in to a person's conversations was to put a second phone line in parallel with that person's phone line. The phone company would facilitate this by using a "punch down block" to splice an additional telephone wire onto the target's phone line. This second line would pick up all of the electrical signals passing over it, including the contents of the call. Phone companies would then run that second line directly to the police station where it would be hooked up to a phone without a receiver so as to not pick up any breathing from the investigators listening in. Every time the suspect's phone rang, the phone at the police station would also ring and the police would be able to listen in.[8]

Starting in the 1970s interception techniques were forced to change, albeit for the better, in order to accommodate the telephone companies' adoption of computerized phone switches for routing and setting up their calls instead of manual switches. With this new technology, pen registers and trap and trace interceptions now could be implemented simply by programming the software in the telephone company's central office switch to pick up the numbers that were being dialed to or from a target and then to send them to an electronic teletype to be printed. The need to do mechanical "punch-downs" on individual telephone wires, which was done prior to the 1970s, was eliminated as the traffic on telephone wires coming from a home could now be monitored and controlled by software contained in the central office switch. Similarly, interception of the content of phone conversations could now be performed by typing an additional command into the central office switch (i.e. separate from the command used to implement a pen/trap intercept) that instructed the switch to automatically send a duplicate signal of the phone call to law enforcement any time the target either dialed or received a call.

Along with the nature of the technologies used to carry and deliver traditional telephone calls, the make-up and structure of the telecommunications market for the better part of the 20th century also contributed to the ease with which law enforcement could intercept telephone calls. With respect to the technology, most telephone calls are still carried over what is called "circuit-switches" (as distinguished from "packet-based" technologies). A circuit switch maintains a dedicated connection between two parties for the entire duration of the call. This ensures that all of the information of interest to law enforcement, whether it is a voice call or fax, follows the same transmission path and

[7] These devices allowed law enforcement agents to record how long each call lasted, simply by measuring the length of time that the phone was off the hook and the paper in the machine continued to run out.

[8] This process was described by the U.S. Supreme Court in one of the seminal cases on the issue of lawful interception, *Olmstead v. U.S.,* 277 U.S. 438, 457 (1928): "Small wires were inserted along the ordinary telephone wires from the residences of . . . the petitioners and those leading from the chief office. . . . They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses."

comes over a single line through the telephone company's central office where it can be intercepted. The fact that traditional phone companies assigned a fixed telephone number to each individual or location, and associated that number with a fixed geographic location, also meant that law enforcement could locate their targets fairly easily. It also meant that law enforcement agents could be confident that the communications they were intercepting actually belonged to that target. Finally, prior to the Telecommunications Act of 1996, the vast majority of all telephone calls ran over the networks of only a handful of telecommunications companies (i.e. the descendants of AT+T). In order to intercept communications passing over those networks, law enforcement agents would have to make requests to a few large companies and could rely on those few companies to implement the order consistently throughout their networks.

With the emergence of new, packet-based forms of communications such as email and the Internet, law enforcement agencies' ability and desire to maintain the upper-hand in the fight against crime were presented with serious new challenges. These challenges are not surprising given the fundamental nature of packet-based networks, in which the contents of any communication (e.g. email or web page) are sliced up into millions of individual "packets" before being sent along to their final destination or recipient. Along the way, each packet can take a different route over the Internet and is not re-assembled until the final destination is reached. In addition, most ISPs do not tend to keep track of the sites that their customers visit or have any easy way of correlating particular communication traffic with an individual. In order to intercept communications of this nature as they are taking place, therefore, law enforcement is forced to install permanent surveillance equipment on one of the individual networks carrying the communications. Alternatively, they must be empowered to require the service provider carrying the communications to configure the equipment in their network to route the entire communication to their recording devices before it is ever passed to the final destination.

II. THE LEGAL STATUS OF LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE OF IP COMMUNICATIONS

A. United States

The primary basis for U.S. law enforcement's authority to conduct the real-time interception of IP-based communications derives from two statutory sources: (1) Sections 2510-2522 of the Omnibus Crime and Control Bill of 1968 ("Title III"); and (2) Sections 3121-3127 of the Electronic Communications Privacy Act ("ECPA") of 1985 (called the "Pen/Trap Statute"), as amended by the USA Patriot Act of 2001. The former statute authorizes the interception of the "content" of communications and the latter allows for the interception of the "addressing information" (e.g., to/from of emails, or phone numbers dialed) associated with a communication.

Section 2511(1) of Title III states that federal and state law enforcement agencies are permitted to intercept the contents of any "wire" and "electronic communication"[9]

[9] Section 2511 of Title III also permits the interception of "oral communications" as well, which are defined as "any oral communication uttered by a person exhibiting an expectation that such communication

provided that one of several statutory exceptions applies, such as the prior issuance of a court order (typically referred to as a "Title III order").[10] The key to the application of "wire communications" to IP-based communications lies in the fact that its definition includes any "aural transfer made . . . by aid of wire, cable or other like connection."[11] This definition has consistently been interpreted to include any form of communication that has a human voice component to it.[12] Therefore, any IP-based communications that meet this basic requirement, such as voice over IP telephony services (VoIP), would seem to fall within law enforcement's ability to intercept that communication. It is similarly easy to draw a connection from "electronic communications," which are defined as "[a]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature" to all non-voice forms of IP communications, such as Internet traffic and email.[13] As for the power to intercept "addressing" (a.k.a. non-content) information associated with IP communications, Section 216 of the USA Patriot Act makes it very clear that the Pen/Trap statute authorizes law enforcement to intercept all "dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted . . . ."[14] These "facilities" might include an Internet user account or e-mail address, as well as an IP address or to/from of emails.[15]

In terms of the thresholds that must be met in order for the interception of an IP-based communication to be lawful, the laws in the US impose substantially more rigorous requirements upon an application for a Title III content order than for a Pen/Trap order. In order to receive authorization to intercept the content of an IP communication, a law enforcement agent must, at a minimum, prove to a court that: (1) there is "probable cause" to believe that the interception will reveal evidence of one of the predicate offenses listed in 18 U.S.C §2516,[16] (2) that normal investigative procedures have been

---

is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." As almost all IP communications fall outside of this definition, you should not be concerned with the government's authority to intercept these types of communications.

[10] Title III contains dozens of exceptions, which may or may not apply in countless different situations. Of these, the primary exception used by law enforcement to conduct the interception of IP-based communications is a court order pursuant to 18 U.S.C. §2518 Both Title III and the Pen/Trap statute also provide law enforcement with the authority to conduct an interception of IP communications without a court order, but only in the event of emergencies and then only for a limited period of time if a normal court order is not otherwise obtained. 18 U.S.C.§§ 3125(a)-(b), 50 U.S.C. §1843(b)-(c).

[11] §2510(1)

[12] See United States Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations at 74 (July 2002)(hereinafter "CCIPS manual") (available at www.cybercrime.gov/s&smanual2002.htm).

[13] §2510(12).

[14] 18. U.S.C. §3127(3). These days, given that IP headers contain both "to" and "from" information, a device that reads the header (and excludes the content) is commonly referred to as a "pen/trap" device.

[15] Prior to 9/11, the Pen/Trap statute defined pen registers and trap and trace devices in terms of telephone communications (e.g. "numbers dialed" and "transmitted on the telephone"). 18 U.S.C. § 3127(1). As a result, the application of the law to the interception of IP communications was never definitively made in the statute. Despite this uncertainty, it was common practice for the Justice Department and the courts to apply the law to those types of communications, presumably in the interest of erring on the side of crime detection and prevention. See e.g., CCIPS manual at 71; Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 Northwestern Univ. Law Rev (forthcoming 2003) at 34.

[16] See 18 U.S.C. § 2518(3)(a)-(b). For federal agents, the predicate offense must be one of the *felony* crimes specifically enumerated in § 2516(1)(a)-(r) to intercept wire communications, or *any federal felony*

tried and have failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous;[17] (3) there is probable cause for believing that the communications facilities to be tapped are either being used in the commission of the crime or are commonly used by the suspect; and (4) the surveillance will be conducted in a way that minimizes the interception of communications that do not provide evidence of a crime.[18] In addition to the courts, law enforcement agents are required to also seek approval from the Justice Department, by statute in the case of "wire communications" (e.g. local phone calls) and pursuant to Justice Department policy in the case of "electronic communications," (e.g. emails) before applying for a Title III order.[19] Once a Title III order has received the blessing of the Justice Department and has been signed by a U.S. District Court or Court of Appeals judge, it can authorize interception for up to thirty days.[20]

In sharp contrast to these elaborate requirements, law enforcement must only show that the information to be obtained is "relevant" to an ongoing investigation before a court is required to issue a Pen/Trap authorization for up to sixty days.[21] Following the passage of the Patriot Act, this authorization can be extended to interceptions conducted anywhere in the United States[22] and even outside the district of the issuing court.[23]

With respect to the relative obligations of law enforcement agencies and the providers of IP-based communications relating to the implementation of a Title III or Pen/Tap order, the U.S. laws draw a distinction between services classified as "information services," which are governed by the ECPA, and services that are provided by a "telecommunications carrier" which are governed by the Communications Assistance for Law Enforcement Act (CALEA).[24] On the surface, the impact of these legal definitions and the relative obligations imposed by the two statutes on you and your customers appear to be relatively straightforward.

By its terms, the ECPA imposes interception obligations on the provider of an "electronic communication service" which is defined as "any service which provides to users the ability to send or receive wire or electronic communications," including electronic mail services. This definition must also be read in conjunction with the definition of "electronic communication" contained in Title III as well as the definition of "information services" contained in Section 1002(b) of CALEA, however.[25] Taken

---

to intercept electronic communications, § 2516(3). The predicate crimes for state investigations are listed in 18 U.S.C. § 2516(2).

[17] 18 U.S.C. §2518(1)(c)

[18] Id. At §2518(5)

[19] CCIPS manual at 77

[20] 18 U.S.C. §2518

[21] 18 USC §3122(b)(1)-(2). The issuing court must also have jurisdiction over the offense being investigated. Id at § 3127(2)(a)

[22] Id. At §3123(a)(1)

[23] Id. At §3123(c)

[24] 47 U.S.C. §§1001, *et seq.*

[25] Section 1001 of CALEA defines "information services" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." See also FCC NPRM FCC 97-356 (expanding upon the definition of "information services" provided in CALEA to include any service that permits a customer to retrieve stored information

together, it becomes relatively clear that the ECPA regulates the interception of "information services" of the type that are typically provided by Internet Service Providers (e.g. AOL and Comcast), including high speed internet access services, email and web hosting services.[26] In terms of the specific technical obligations which the ECPA imposes on these providers, Section 2518(4) of 18 U.S.C. requires them simply to:

> "furnish the application forthwith **all information, facilities and technical assistance necessary to accomplish the interception** unobtrusively and with a minimum of interference with the services that such service provider . . . is according the person whose communications are to be intercepted." [27]

Despite this language, the ECPA does not provide any further explanation as to what the obligation to "assist" actually means from a practical perspective. Instead, it leaves it to the affected service providers to make that determination on their own. Nor does the ECPA set any specific timelines for compliance or provide a clear basis for reimbursement of costs associated with meeting these vague obligations.[28] One possible explanation for this continued ambiguity in the law may be that, in those cases where a service provider claims an inability to intercept emails or is unwilling to comply with an intercept order, the US government has shown little hesitation in using its own surveillance technologies, such as Carnivore, to carry out the interception.[29]

By contrast, CALEA imposes significantly more rigorous and costly obligations on providers of IP-based services that fall under the definition of a "telecommunications carrier" contained in the Act. The FCC has defined "telecommunications carriers" to include any provider of a packet-mode (including IP) communication switching or transmission service[30] that provides the equivalent of a local telephone exchange service, for a fee to the general public.[31] While this definition has been interpreted by law enforcement to include any IP telephony or similar service that resembles those traditionally provided by phone companies such as Verizon and AT+T, the FCC has only recently taken the first steps towards clarifying and cementing the application of CALEA to those services. Specifically, in February 2004 the FCC issued a Memorandum and Order in which it hinted that it would go to great lengths to read CALEA as broadly as possible in order to apply it to all types of IP-enabled services.[32] In response, the United States Department of Justice, the FBI and the Drug Enforcement Administration

---

from, or file information for storage in, information storage facilities, electronic publishing and electronic messaging services, and citing email providers and online service providers as examples).

[26] Section 211 of the USA Patriot Act amends title 47 §551(c)(2)(D) to clarify that the ECPA and the wiretap statute governs disclosures by cable companies that relate to the provision of communications services such as telephone and internet services.

[27] Section 2518(4)

[28] 18 U.S.C. §2518(4): A government entity must reimburse a provider for its "reasonable expenses" in providing interception assistance.

[29] 18 U.S.C. §3121(c) also permits law enforcement to "use technology reasonably available to it" to conduct an authorized pen register. For a description of how Carnivore actually works, see Kerr, pp. 54-58.

[30] FCC FNPRM, November 1998

[31] 47 U.S.C. 1001(8). In its Second report and Order, the FCC included within this definition any service that allows a customer to access the publicly switched telephone network (PSTN).

[32] FCC Memorandum Opinion and Order, FCC 04-27.

petitioned the FCC together in order to, among other things, convince the FCC to subject VoIP to CALEA.[33] The FCC has yet to make a final decision on this matter. However, in August, 2004 the agency issued a "Notice of Proposed Rulemaking and Declaratory Ruling"[34] in which it tentatively concluded that VoIP services offered to the general public as a means of communicating with any telephone subscriber, including those reachable only through the public switched telephone network, are subject to CALEA. The FCC reasoned that (a) VoIP companies provide services that are functionally equivalent to traditional phone services, and (b) there was an "overriding public interest in maintaining law enforcement's ability to conduct wiretaps" in networks that are rapidly replacing the "traditional circuit-switched network."[35] Although the FCC has indicated what its decision will be, it is still seeking comments before the final rulemaking.

From a technical standpoint, CALEA imposes explicit capability, capacity and security requirements on the affected service providers, all of which requirements are theoretically designed to ensure that their networks are capable of implementing law enforcement's intercept orders.

The "capability" requirements imposed by CALEA include the ability of a service provider to: (a) isolate and enable law enforcement to intercept the content of a communication; (b) isolate and enable law enforcement to access pen/trap information (collectively labeled as "call-identifying information") that is associated with the communication and that is 'reasonably available" to the carrier; (c) deliver the call content or call-identifying information to law enforcement in a format such that it can be transmitted by government equipment to a location outside the carrier's premises; and (d) perform these tasks without alerting the target to the interception or interfering with their services, and without delivering any information (i.e. call-identifying information or content) other than that which law enforcement has been authorized to intercept.[36] The FCC has made it clear that an IP telecommunications carrier must also be able to isolate and deliver data that goes beyond basic dialing and routing information such as party hold, join, and drop on conference calls, timing information and dialed digit extraction.[37] IP telecommunications carriers must also make sure that their networks are capable of accommodating up to the maximum number of simultaneous Title III orders and pen/trap orders set out by the Attorney General in a notice published in the Federal Register.[38] Finally, a telecommunications carrier's network must be configured in such a way as to ensure that all of these requirements can be met solely by means of an affirmative act by the provider (i.e. by flipping a switch, as opposed to an interception device that is on until it is turned off).[39]

---

[33] "Joint Petition for Expedited Rulemaking," *available at* http://www.askcalea.net/jper.html/.
[34] 69 Fed. Reg. 56976 (2004)
[35] *Id*. At para. 56.
[36] 47 U.S.C. § 1002
[37] FCC Order on Remand, CC Docket No. 97-213, April 5, 2002.
[38] 47 U.S.C. § 1003.
[39] Id at §1004.

While CALEA does not require that telecommunications carriers adopt "any specific design of features or system configurations" in order to meet these capability requirements,[40] it does explicitly recommend that law enforcement and your IP telecommunications carrier customers collaborate in the development of industry-wide technical standards detailing specific ways of implementing them. It also provides a safe harbor to any telecommunications carrier complying with any of those standards.[41] As a result, there continues to be a substantial amount of uncertainty as to the proper technical standards for you and your customers to follow and whether compliance with any one in particular will shield your company from any legal and financial risk. You should also keep in mind that law enforcement's ability to participate in these standard-setting activities means that at least some standards will likely contain their desired configurations and technical requirements. Development to those standards could, in turn, lead privacy advocates to conclude that you favor the law enforcement interests of the government over the privacy interests of U.S. residents. Finally, it is also important to remember that CALEA does not require telecommunications carriers to seek confirmation of their compliance with the capability requirements from either the FCC or law enforcement prior to deploying any service to the public. Therefore, a decision not to implement a safe harbor or industry standard does not preclude a telecommunications carrier from meeting their obligations under the law. Rather, a carrier's compliance would instead be determined upon the issuance of a court order authorizing an interception of IP communications, and then only upon a further finding that the telecommunications carrier was unable to meet the capability, capacity and security requirements contained in CALEA.[42]

Perhaps the most important element of CALEA for your company is its imposition of substantial obligations on all "manufacturers of telecommunications transmission and switching equipment" and its establishment of penalties for non-compliance. While it is debatable whether the drafters of CALEA envisioned companies like yours being subject to this definition, your company has decided to take a conservative approach and assumes that it is covered by this definition. Consequently, CALEA requires that you consult "in a timely fashion" with your customers to make sure that your product roadmaps are in synch with their plans for delivering CALEA-compliant services by the statutory deadlines.[43] Your company is also required to "make available" to all of your IP "telecommunications carrier" customers "such features or modifications as are necessary to permit" them to comply with their capability and capacity requirements.[44] Moreover, you must provide these features "on a reasonably timely basis and at a reasonable charge."[45] The law also contemplates that your company will participate in the standard-setting activities mentioned earlier and extends the safe-harbor exemption to your company in the event that you comply with one of those standards. Just as with your customers, however, your company is not required to build its products according to

[40] Id. At §1002(b)(1).
[41] 47 U.S.C § 1006.
[42] Id. At §1007.
[43] Id. At §1005(a).
[44] Id. At §1005(b).
[45] Id.

any particular standard or to seek prior approval from the FCC in order to be in compliance with its legal obligations.

From a financial perspective, CALEA theoretically allows for the possibility that your customers could recoup some of their costs directly associated with achieving compliance.[46] However, the Attorney General has officially interpreted the relevant sections of the Act so as to make it is unlikely that any products purchased or deployed by service providers after January 1, 1995 will be eligible to receive that compensation.[47] Given that the vast majority of your products fall into this category, your company's CALEA strategy needs to account for the potentially negative financial impact it could have on your customers.

By contrast, the possibility of fines for non-compliance under CALEA is quite real. Subsequent to the FCC's September 2001 Order, any new IP-based communication services deployed after November 19, 2001 must be in compliance with CALEA. All services in existence prior to that date must either be in compliance or be under consideration by the FCC for an individual extension.[48] In the event that any court issuing an intercept order on one of those service providers after that date finds them unable to meet the capability and capacity requirements of CALEA, it may impose a civil penalty of up to $10,000 per day on both the telecommunications carrier and the manufacturer of telecommunications equipment. This fine may be levied for each day that the court determines them to be in non-compliance. In addition, the court may direct that the manufacturer of the carrier's transmission or switching equipment immediately make available those modifications to its products that are necessary for the customer to comply with the law. To date, these fines have already been levied against one service provider in the United States in the fall of 2002.

Despite the apparent clarity of the definitions and corresponding technical obligations for both your company and your customers under the ECPA and CALEA, it is important to realize that there are some significant grey areas in these laws that could impact your company's overall strategy. For example, "private networks" are explicitly exempt from CALEA.[49] In public announcements, the FCC has stated that it conceives of a private network as a telephone network that is served by traditional phone equipment (e.g. PBX) which sits at the customer's site and which provides voice and information services solely to that company's internal employees (i.e. internal network). In the case of a company that provides what are called "managed voice services," however, a service provider might offer these same voice services, but instead of locating the telephone equipment at the customer's site, they may locate it on their own premises. The service provider may also sell this service to several different companies using the same PBX instead of just one. Is this still a "private network" or does it become a telecommunications service subject to CALEA? In this situation, there are multiple customers and the relevant equipment is owned and operated by the service provider,

[46] 47 U.S.C. §1008.
[47] See FBI's final Cost Recovery Regulation at 28 CFR Part 100.
[48] 47 U.S.C. §1006(c).
[49] Id. At § 1002(b)(2).

thereby making it look a lot like regular local phone services. Similarly, while email services and hi-speed internet access providers (e.g. DSL and cable) are clearly classified as "information services" under CALEA, and thus exempt from its requirements, the FCC has questioned whether that exemption should still apply where those same services are provided by a telecommunications carrier or where the carrier uses the same equipment to provide both telecommunications and information services (i.e. "joint use facilities). What is the appropriate line for your company to draw between these two views? Conversely, what about when an ISP like AOL provides VoIP services? While you are not expected to provide definitive answers to your company on all of these questions, you are responsible for making sure that your company's overall strategy for LI accounts for these grey areas.

B. Germany

The legal basis under German law for the real-time interception and recording of IP-based communications comes from three different statutes: the G-10 Law,[50] the Criminal Code, and the Foreign Trade and Payments Act. The G-10 law authorizes federal and state authorities to "intercept and record telecommunications . . .[and] to open and inspect mail covered by the privacy of correspondence and posts."[51] Similarly, the Foreign Trade and Payments Act (FTPA) allows for the Customs Criminological Office to "monitor and record telecommunications," and the Criminal Code permits the "[i]nterception and recording of telecommunications."[52] The key to the application of all three laws to IP communications is found in the broad definition of "telecommunications" contained in the German Telecommunications Act (TKG). The term is defined as "the technical process of sending, transmitting and receiving any kind of message in the form of signs, voice, images or sounds by means of telecommunications systems."[53] When read in conjunction with the definition of "telecommunications systems" under the TKG,[54] it is fairly clear that "telecommunications" can be applied to all forms of IP communications including VoIP, data services such as web hosting, email and Internet services. This application of the laws to IP-based communications is further supported by the Technical Directive TR TKÜ 3.1 (discussed below), which implements the technical details of interception under the TKG for IP-based communications.

In order to be legally authorized to intercept "telecommunications," the federal agencies endorsed under the G-10 law and the FTPA must meet the requirements set forth in Section 100a and 100b of the Criminal Code. Under section 100a, an official order authorizing the interception and recording of telecommunications may be granted by a judge[55] simply upon a showing of "suspicion"[56] that a person was "the perpetrator or

[50] The full title of the law is "The Act on the Restriction of the Privacy of Correspondence, Posts, and Telecommunications."
[51] G-10 Law, §1(2).
[52] Criminal Code § 100(a).
[53] TKG § 3(16).
[54] TKG §3(17).
[55] While the order to intercept can typically only be given by a judge, the law does also allow for one to be issued by the public prosecution office in the case of emergency circumstances. Criminal Code §100(b)(1).

inciter of, or accessory to" a broad list of crimes including violations of the FPTA and the Criminal Code. The predicate crimes under the Criminal Code include threatening national defense and manslaughter.[57] The order must set out in writing the details of the interception, such as the "type, extent and time" of the intercept measures to be carried out, and can permit the interception for anywhere from 3 to 6 months.[58] In the event that the interception order is requested by the Federal Authorities, the activities to be carried out under that order are subject to the supervision by the Parliamentary Supervisory Board and a special G-10 Commission.[59]

Somewhat differently from the laws in the United States, the obligation to implement orders to intercept all types of IP communications under German law sits squarely and completely on the affected service providers. Nor does German law draw a distinction between the obligations pertaining to the interception of "addressing information" and the "content" of the communication. Rather, Section 2 of the G-10 law and section 88(4) of the Telecommunications Act impose an obligation on every operator of "a telecommunications system commercially providing third parties with network access to his telecommunications system"[60] to: (a) supply law enforcement with "information on the particular circumstances of telecommunications;" (b) "turn over mail" transmitted over their network; (c) "enable the interception and recording of telecommunications;"[61] and (d) provide "network access for transmission of the information obtained" under the intercept order.[62] This effectively means that the affected telecom operators are required to deliver a copy of the entire stream of information passing over their networks to law enforcement, as opposed to filtering out content and addressing information before delivery.

The German government has gone to great lengths to try to spell out exactly which entities are impacted by these interception obligations. The Telecommunications Interception Ordinance (TKUV), which was passed in January 2002 and later amended in August 2002, makes it clear that only those service providers offering fee-based "telecommunications services" to the general public, as opposed to members of "closed user groups,"[63] and then only those portions of the network actually used to provide those services, [64] must meet the technical requirements set out in the TKG and the TKUV. In terms of your customers, this definition includes, among others, providers of high-speed and dial-up internet access services, web hosting and Internet services. Explicitly

---

[56] Criminal Code §100(a).
[57] Id at §§100a (1a)-(5)
[58] Criminal Code §100b(2)
[59] G-10 Law, §1(2)
[60] TKG, §88(4)
[61] G-10 Law, §2
[62] TKG §88(4). Section 100b(3) of the Criminal Code simply requires that "all persons providing, or collaborating in the provision of, telecommunications services on a commercial basis shall enable [law enforcement] to intercept and record telephone calls."
[63] TKG §3(19). Section 3(1) of the TKUV makes reference to and incorporates the definition of "telecommunications services to the public" from the TKG.
[64] TKUV §3(1). The exclusion with respect to portions of the network not in use presumably applies to those cases where a telecommunications system was used to provide both telecommunications and non-telecommunications services (i.e. "joint-use facilities").

excluded from this group are entities operating simple interconnection services, German operators of terminal equipment that is located outside of Germany and operators serving less than 1,000 subscribers. With respect to providers with less than 1,000 subscribers, their obligation is limited simply to "enable[ing]" law enforcement to intercept and record calls.[65] This is similar to the obligation on information service providers under the U.S.'s ECPA to "assist" law enforcement with interception. Notwithstanding these attempts at clarity, it is important to recognize that the law does not give any definitive guidance as to what constitutes a "closed user group" or whether a single large chain of hotels providing Internet services to their guests should be considered to be "connected with more than 1,000 subscribers."[66] Consequently, your company should carefully consider whether these types of customers can be safely excluded from your overall strategy for LI.

In order to be eligible to deliver services to the public, your customers qualifying as operators of "telecommunications systems" must comply with the detailed technical and organizational requirements pertaining to the interception of IP communications that are set out in the Telecommunication Interception Ordinance (TKUV), and must do so solely at their own expense.[67] It is only after they have received an explicit acknowledgment from the Regulatory Authority for Telecommunications and Post (RegTP)[68] that they have met those requirements that they will be legally permitted to deploy those services. With respect to the specific technical obligations imposed on service providers, the TKUV is similar to CALEA in many respects in that it sets out capability and capacity requirements for the impacted service providers.[69]

The TKUV also accounts for the financial challenges smaller telecom service providers face with these capability and capacity requirements by granting them certain exemptions from the general technical obligations. Specifically, telecommunications operators serving less than 10,000 subscribers are still able to receive regulatory approval to deliver services as long as these providers are able to implement an interception within 24 hours after receipt of judicial notice, and are capable of meeting several other reduced capacity benchmarks. [70] This is applicable only to those facilities that are not a part of a larger telecommunications facility of the same operator, however. Presumably this would mean that if Deutsche Telekom provided Internet access services to a small neighborhood of less than 10,000 people by means of the same facilities it otherwise used to provide its

[65] TKUV §3(2)(5), citing G-10 law, §2(1); FPTA, §39(5); Criminal. Code §100b(3).
[66] Id.
[67] TKG, §88(1)
[68] Id. TKUV § 18.
[69] These capabilities include as the ability to intercept only those communications specified in a judicial order (§5(1)) and to do so without being detected by the target (§5(3)). In addition, the TKUV requires service providers to deliver details relating to the call-identifying information to law enforcement similar to those set out in the FBI's "punch list." TKUV §7. E.g. the call number dialed(2)(a), call-forwarding information (2)(b), the call number received (3), and call-drop information. The TKUV goes further than CALEA, however, to the extent that it codifies additional technical requirements into the law, such as the configuration of the handover point between the service provider and law enforcement (§8), the automatic and proper protocolling of the equipment used in the interception (§§16 and 17), and the organizational and procedural rules relating to the implementation of an intercept order (§27).
[70] Id. At §21.

nationwide local telephone services, then Deutsche Telekom would still be legally required to bring that smaller service into compliance with the TKUV's requirements.

Even more significant for you and your customers from a financial perspective, however, is the fact that the German laws stipulate the specific technical standards which all affected telecommunications companies must meet in order to comply with their legal obligations under the TKUV. These details are set out in the TR TKÜ 3.1, which was issued by the RegTP in May, 2002. While this technical directive was the result of a collaborative effort between service providers, law enforcement agencies, and telecommunications equipment manufacturers and regulatory authorities,[71] compliance with it is now mandatory. Deviations from the specific technical requirements set out in the TR TKÜ, if any, are permitted only on a case-by-case basis in "technically justified exceptional cases,"[72] provided, however, that the deviation does not fundamentally alter or impair law enforcement's ability to conduct interceptions.[73] Failure by your customers to be in compliance with their obligations under the German LI laws could result in the revocation of their license to do business,[74] and the imposition of fines of up to one million deutschmarks.[75] Despite all of these obligations on service providers, the LI laws in Germany do not provide for any compensation to be paid to the service providers for the costs incurred to build these capabilities into their networks.[76]

With respect to your company's obligations under Germany's LI laws, the TKUV sets an expectation that equipment manufacturers will work with their affected customers, as well as law enforcement and the RegTP, to help develop and implement the Technical Directive (TR TKÜ). The TKUV also sets a deadline of January 1, 2005 by which either new equipment or modifications to existing equipment needed to implement the Ordinance's interception measures must be made available.[77] The responsibility to meet these legal deadlines rests solely with the affected service providers, however. Therefore, from a purely legal perspective there is very little risk that your company could be subject to any fines or penalties for non-compliance with any existing laws. From a practical business perspective, many of your customers are now faced with a requirement that they maintain permanent LI capabilities in their networks or lose their right to do business in Germany altogether. Given this reality, it is incumbent upon your company to provide these customers with a technical solution which helps them meet these obligations or risk losing substantial amounts of business from them going forward.

C. United Kingdom

The primary statutory basis authorizing law enforcement agencies in the United Kingdom to conduct real-time interception of IP communications is the Regulation of Investigatory

[71] Id. At §11.
[72] TKG §88(2).
[73] TKUV §22.
[74] TKG §15.
[75] TKG §96.
[76] TKG §88(1)
[77] TKUV §30.

Powers Act of 2000 (RIPA).[78] RIPA is the result of the UK government's publicly expressed desire to update the pre-existing law governing the real-time interception of communications (the Interception of Communications Act of 1985) by extending its reach from the traditional, incumbent telecommunications providers, such as British Telecom (BT), to all Communication Service Providers (CSPs). This broader category includes ISPs and other types of IP communication service providers (e.g. ASPs, VoIP and DSL service providers). As with other countries, this extension of the law was considered necessary in light of both the rapid development of new communications technologies and a substantial increase in the number and types of companies providing those services. Together these elements made law enforcement's job of detecting and preventing crimes much more challenging.

RIPA provides law enforcement with expanded intercept powers by making it lawful for them to intercept the content of "any communication in the course of its transmission by means of a public telecommunications service," where that interception takes place in accordance with a warrant.[79] The law defines "communication" very broadly to include "anything comprising speech, music, sounds, visual images or data of any description; and . . . signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus."[80] When read in conjunction with the definitions for "public telecommunications service," "telecommunications service" and "telecommunications system" contained in Section 2 of RIPA, it is clear that the law permits the interception of the content of almost any IP-based communications service that is provided to "a substantial section" of the UK populace, including voice services, email, web hosting and the Internet access.[81]

In addition to the power to intercept and record the content of communications, law enforcement is also entitled to intercept the "communications data" associated with any "communication," such as the dialing, routing, or signaling information associated with a phone call or email.[82] Section 5(d) of RIPA authorizes law enforcement to require CSPs to disclose all related communications data that "is obtained by, or in connection with"

---

[78] Similar to the situation in Germany and all other European countries who were signatories to the same laws, the interception of personal communications in the UK is also permitted by the European Convention on Human Rights as well as the Data Protection Act of 1998. The former asserts both the right of individuals to preserve their privacy and the right of authorities to "interfere" with that right in certain lawful and clearly demonstrated circumstances. See Article 8.2, European Convention on Human Rights. The latter applies to the processing of personal information that has been lawfully obtained and allows its disclosure to law enforcement only if there is a legal basis to do so (e.g. RIPA). That said, RIPA is still the primary statutory source authorizing lawful interception of IP communications in the UK.

[79] RIPA §§1(5) and 2(2).

[80] Id at §81(1).

[81] Unlike the United States, however, RIPA also includes within the reach of "real time" interception any time when the communication is "stored" prior to a recipient collecting it or having access to it, such as when email is made available for download on a server. (§2(7))

[82] The clearest definitions of "communications data" under RIPA are in Section 2(9) of Chapter I and in Section 21(6) of Chapter II. Communications data can be understood to include traffic data (i.e. to/from, when, where), which is effectively the "addressing information" specified under the United States laws. It also includes service data (i.e. which services used and for how long) and subscriber data (i.e. name and address of user).

the "communication" being intercepted.[83] This effectively means that law enforcement is able to receive both the content and the addressing information of any IP-based communication simply upon the issuance of a warrant to intercept content only. In the event that law enforcement desires to acquire only the "communications data," Section 22 of Part I, Chapter II of RIPA authorizes it to intercept that information by means of its own device or by requiring a telecommunications provider to intercept it on his behalf.

While RIPA provides for several different grounds under which the interception of the "content" of IP communications may be authorized,[84] the vast majority of these intercepts are conducted under a warrant signed by the Secretary of State.[85] The law allows a number of different government officials and law enforcement agencies to apply for a warrant, including any "person who, for the purpose of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom."[86] Before they can receive a warrant, these officials must be able to prove to the Secretary of State that the interception is both "proportionate to what is sought to be achieved by the interception"[87] and "necessary" (a) in the interests of national security, (b) for the purpose of preventing or detecting serious crimes, (c) for safeguarding the economic well-being of the UK or (d) for complying with the provisions of any international mutual assistance agreement.[88] Interestingly, all of these terms go largely undefined in the law itself and in the official explanatory comments issued by the UK Home Office. The majority of warrants are issued for a period of three months, but the law also provides for renewals and even extensions in some cases for up to six months.[89]

By contrast, the legal thresholds applicable to a request to intercept communications data under RIPA are far more lenient. As long as one of a large number of individuals and organizations specified in Section 25 believe that the data is "necessary" and "proportionate"[90] on one of eight different grounds, including the detection of *any* crime,[91] then they may issue an order to any person within their same organization authorizing them to intercept and require the disclosure of that information for an initial period of a month.[92] As a counterbalance to the seemingly broad and sweeping authorization to intercept IP communications, RIPA prohibits any information (including both the content and traffic data associated with telephone calls, emails, and internet web

[83] RIPA § 20(a). Each warrant to intercept the content of communications automatically authorizes any conduct which is necessary to achieve the overall objective of law enforcement, including the interception of both communications not specifically identified by the warrant and also communications data, such as IP headers and to/from of emails, that is simply "related" to the communication being intercepted. § 6(6).
[84] Id. At § 3
[85] Similar to the laws in Germany and the United States, RIPA allows warrants to be issued without the signature of the Secretary of State in the case of emergencies and where it is necessary to comply with a request for mutual assistance from a country outside the UK. Id. At §7(2)
[86] Id. At § 6(2)
[87] Id. At §5(2)(b)
[88] Id. At §5(3)
[89] Id at §9(6)
[90] Id. At §22(5)
[91] Id. At §22(2)(b)
[92] Id. At §22(3)

pages) that is intercepted pursuant to a warrant from being introduced as evidence in court, limiting their application only to intelligence gathering instead.[93] In addition, RIPA provides for the establishment of an Interception of Communications Commissioner[94] who is responsible for ensuring that the intercept activities of the Secretary of State and all other authorized agencies are carried out in compliance with the law.

In terms of which entity is responsible for implementing a lawfully authorized interception order, RIPA requires all "public telecommunications service" providers in the UK to "take all such steps for giving effect to" a warrant authorizing the interception of "communications" and related "communications data" that are "reasonably practicable."[95] A very similar obligation is imposed on providers with respect to the interception and disclosure of "communications data."[96] What these general obligations actually mean for your customers only becomes clear, however, when one reads them in conjunction with Section 12 of RIPA and the associated Order No. 1931. These two pieces of law draw a significant distinction between the obligations imposed on providers of IP-based communications services who serve more than 10,000 persons, which is the vast majority of your customers, and those who serve less than that number. The latter group of providers, for example, is subject to very minimal regulation and is neither subject to any specific technical requirements nor responsible for maintaining any permanent interception capabilities. Indeed, small IP-based communications providers can meet their obligations under section 11 of RIPA simply by permitting law enforcement to install their own equipment, such as an IP packet-sniffer, into their network.[97]

By contrast, Section 12 of RIPA and Order no. 1931 effectively impose affirmative and specific obligations on all large IP communications providers to configure their networks so as to ensure that they maintain the permanent interception capabilities and capacities set out in that Order.[98] In terms of the specific configuration changes and other accommodations which a service provider must make to its network in order to comply with these obligations, the law contemplates that the Secretary of State will work collaboratively with CSPs, on a case-by-case basis,[99] to create a solution that is tailored to each individual service provider's network.[100] It is only after this consultation has taken

[93] Id at §17
[94] Id at §57
[95] §11(4)-(5)
[96] §22(7)
[97] §11)(1)
[98] These required features include: (1) the ability to intercept both communications and any related communications data in real-time; (2) the ability to transmit that information simultaneously with its interception to a designated hand-over point within their network; (3) to ensure the simultaneous interception of up to 1 in 10,000 persons; and (4) to ensure that the reliability of the interception capability is equivalent to that of the service being intercepted. Therefore, any communications provider subject to these obligations would be unlikely to claim an inability to comply with a Chapter II order to intercept only communications data on the grounds that it was not "reasonably practicable" for them to do so.
[99] §12(9)
[100] This means that you could have two similar services meeting their compliance obligations in two different ways. For example, two ISPs providing web-based email services could utilize two completely different means of authenticating their users for purposes of LI. One could allow a packet-sniffer to be

place that the Secretary of State will issue a notice under section 12(2) laying out the precise steps that must be taken by the service provider, including the purchase of additional networking equipment.[101] In effect, this close, collaborative effort makes it highly unlikely that the technical requirements contained in any notice would ever come as a surprise to the CSP. It also reduces the likelihood that law enforcement would be unable to intercept the precise IP-based communications of a particular criminal target passing over that network and thus that a CSP would ever be found to be non-compliant.

If for some reason a public IP communications service provider subject to the Section 12 order was unable to agree with law enforcement as to the appropriate changes to be made to their network, or had determined that the financial costs of compliance with a particular notice were too burdensome, RIPA provides a means for appeal and possible redress to a Technical Advisory Board (TAB).[102] The TAB is comprised of seven total representatives, including three each from the law enforcement and CSP communities and a single independent chairman.[103] While in principle the TAB is empowered to make recommendations to the Secretary of State as to whether it thinks any notices referred to it by a CSP are reasonable, the law grants the Secretary of State the final authority to determine whether to withdraw the notice to the CSP or to enforce it without modification. Therefore, despite its appeal, a CSP could still be required to implement the specific capabilities into their networks in order to meet the demands of law enforcement. Fortunately, Section 14 does allow for an affected CSP to receive a "fair contribution towards the costs incurred" in meeting their intercept obligations under RIPA. While this language would tend to suggest that the UK government would be willing to meet the costs associated with the purchase and installation of new equipment needed to permit interception of the CSP's service, the details of this compensation have not been worked out yet and remain somewhat vague.

Given this structure of the UK law, there is minimal risk that one of your customers either will be found in violation of their technical obligations under RIPA or will be subject to the substantial criminal and civil penalties, including imprisonment and fines, which are set out in the law.[104] In light of publications from the UK government suggesting that the state of the law relating to interception of communications data is largely in flux,[105] the risk faced by the smaller providers of IP-based communications services (i.e. less than 10,000 subscribers) is similarly minimal. Equally important for your company is the fact that RIPA does not impose any explicit or implied obligations on manufacturers of telecommunications equipment. Therefore, there is almost no risk that your company could be cited for non-compliance with the law or be subjected to any

---

installed in their network and the other could re-write the software code on its networking equipment to deliver that information to law enforcement.

[101] §12(2)

[102] This was established by Section 12 of RIPA and Order number 3734 (11/22/01)

[103] Per the terms of Order number 3734, the membership of the TAB is not required to include any representatives from telecommunications equipment manufacturers

[104] See RIPA §11(7) and §12(7).

[105] See Consultation Paper from the UK Home Office, "Access to Communications Data: Respective Privacy and Protecting the Public from Crime," (proposing a number of modifications to the existing rules on the interception of communications data under RIPA).

penalties, financial or otherwise. That said, a failure by your company to provide new products or to modify your existing ones in order to help your customers meet their legal obligations could not only create a serious impediment to doing business in the UK with large IP-based service providers, but could also shut off a potentially large source of new revenue. You should also consider whether to take any steps to address the fact that the legislation forming the TAB did not require the participation of companies like yours in the consultative process taking place between your customers and law enforcement. Thus there is a risk that decisions about the future technical direction of LI in the UK could be made without your involvement. This, in turn, could negatively impact your company's current development efforts and inhibit your company's ability to do business in this area.

III. WORLDWIDE STANDARDS ACTIVITIES ON LI

There is currently a lot of development activity around the world in the area of standards for LI. That said, there is no uniform standard either within the United States or among the European countries generally, or between the US and Europe at this time. There are however some discernible trends in the various standards body activities that you should be aware of and incorporate into your guidance to the company regarding its LI strategy.

In the United States there are at least six different standards bodies working on the development of a safe harbor specification for CALEA. From a resource perspective, this is too many groups for your company to participate in all of them. At the same time, it is hard to find clear uniformity among the safe harbors being developed by each group. It is also important to consider the fact that the FBI participates in the activities of some of these groups and not in others. Given the FBI's power under CALEA to seek fines for telecommunications carriers and equipment manufacturers that are unable to provide them with the information they desire, there would seem to be more than ample incentive to participate in these groups with the FBI. Balanced against this benefit, however, is the risk that law enforcement agencies could use their position in the standards bodies to advocate for the development of technical requirements and definitions, such as the one for "call-identifying information," that could effectively expand their authority to intercept IP communications beyond what has been provided to them in the statute. Participation in these activities therefore could be seen by privacy advocates as favoritism towards law enforcement over the privacy interests of Americans.

Similarly to the United States, there are at least six European standards bodies that are working on the topic of lawful intercept of IP-based communications. Also worthy of consideration is an international partnership which includes standards bodies from Europe, Japan, the United States, China and Korea. The goal of this partnership is to develop a global framework standard for the interception of IP data which can be modified as necessary by each country to meet their own specific legal and technical requirements.

IV. QUESTIONS

General:

1. Do we see more similarities or differences among the three country's approaches to lawful intercept? What might be some reasons for these differences or similarities? What are some of the ways that these differences and/or similarities might impact your company's legal and technical approach?
2. What are some of the risks for your company under these laws (e.g. fines, lawsuits)? What steps can and should you take to protect your company from them?
3. How should your company engage with relevant government agencies? Actively and openly? Equally across all countries or just the most strident? Should you let your customers do it instead of you? What factors you should consider in making this determination?
4. Do you need a computer science background to answer these questions and to guide your company? Are there ways to answer these questions using basic legal principles and theories?
5. If you were to do more research into this issue in order to advise your company, where would you look, who/what entities would you try to speak with, and what types of resources would you consult?

Specific:

1. Your company has one product that can be used both by private enterprises to create their own internal corporate voice network and by public service providers to provide the same voice services to enterprise customers in the form of a "managed voice service" for a fee. In the latter case, the product can either sit on the customer's premise or the on the service provider's site in their central office. The team developing this product within your company want to know whether they are "legally required" to build LI functionality into this product, and if not, whether there are some other (non-legal) reasons that they should. What advice do you give them and why? (NOTE: Be sure to point to specific factors and/or laws upon which you based your advice). What steps, if any, would you advise the engineering team to take if they choose to go ahead with selling the product into both markets?
2. During negotiations on a sales contract with one of your global service provider customers they demand that you include a guarantee that <u>all</u> of your products are "LI-compliant" on a world-wide basis. They suggest that breach of this guarantee would result in liquidated damages. They also ask you to indemnify them for any penalties they might suffer for non-compliance with a particular country's LI laws. How do you handle this?