Criminal Law & Procedure

The Evolution of Wiretapping

*By Paul Rosenzweig**

In 2010, the government of India approached Research In Motion (RIM), the manufacturer of Blackberry devices, with a demand. India wanted to monitor the encrypted e-mails and Blackberry Messages (a form of internet chat) that passed across RIM's servers between corporate clients. And it wanted help in decrypting the encrypted messages. This was, the Indian government argued, essential to allow it to combat terrorism. And, they added, if you don't give us this access, then we'll pull your wireless license and close down Blackberry in India. Faced with the loss of more than one million Indian corporate customers, RIM compromised—it found a way to share with the Indian government where to find the encrypted messages the government wanted—in effect identifying the servers where the information originated—without actually decrypting the messages itself.[1]

In making this arrangement (and, by all reports, placating the Indian government), RIM nicely illustrated two distinct, yet linked, issues that relate to the security of cyber communications, and are deeply imbedded in all aspects of the conflict in cyberspace. One is the issue of encryption—when and how communications and information can be encoded and decoded so that only the people you want to read the information can have access to it. The other is wiretapping—that is, whether and under what rules someone can intercept messages in transit and divert or copy them to their own purposes. The linkage between the two seems apparent—wiretapping a message you cannot decrypt still conceals the content of the message, and even unencrypted information is safe if the transmission channels are absolutely secure. Those engaged in a conflict in cyberspace want both capabilities—to intercept/divert information and to decode it so that they can read its contents.

And therein hangs a tale. India is not alone in its interest in being able to read people's encrypted mail. Other governments from Dubai and China to the United States have the same interests—for good or for ill. Indeed, late in 2010 the United States government disclosed plans to expand its wiretapping laws to apply to encrypted e-mail transmitters like BlackBerry, social networking websites like Facebook and software that allows direct "peer to peer" messaging like Skype.[2] How well (or poorly) a nation achieves this objective bears directly on its ability to successfully win conflicts of espionage, crime, and war in cyberspace—and also on how great or little intrusion the government makes into the communications of its private citizens.

* * * * *

The Internet is a means, essentially, of transmitting information across large distances at a ridiculously rapid pace. All of the various types of attacks and intrusions that have become commonplace on the Internet today are, fundamentally, based upon the ability to corrupt the flow of accurate information—whether by stealing a portion of it for misuse, disrupting the flow so that accurate information does not arrive in a timely manner, or inserting false information into an otherwise secure stream of data. If the confidentiality and integrity of the information being transmitted cannot be relied upon, then the system or network that acts based upon that data is vulnerable. That, in a nutshell, is the core of much of cyber warfare, cyber crime, and cyber espionage—the ability to destroy or corrupt the flow of information from your enemies through intrusion or attack—and the collateral real-world effects of that destruction.

What if you could make your data incorruptible (or, slightly less useful but almost as good, if you could make your data tamper-evident, so that any corruption or interception was known to you)? If your goal is to protect your own information from attack, there are a number of ways you might achieve that objective. One of the earliest defensive measures taken in cyberspace was a method as old as human history—data and information were protected by encryption.

But this expansion of cryptographic capabilities to protect cyber networks comes with an uncertain cost to order and governance. Advances in cryptographic technology have made it increasingly difficult for individuals to "crack" a code. Code breaking is as old as code making, naturally. But as the run of technology has played out encryption increasingly has an advantage over decryption, and recent advances have brought us to the point where decryption can, in some cases, be effectively impossible. This has the positive benefit of allowing legitimate users to protect their lawful secrets—but it has the inevitable effect of distributing a technology that can protect malevolent uses of the Internet. If the United States government can encrypt its data, so can China, or the Russian mob, or a Mexican drug cartel.

An alternative strategy that works in concert with encryption is to make your information transmission immune to interception. Here, too, the changes wrought by Internet technology have made interception more difficult and enhanced the security of communications. In the world of telephone communications, for example, intercepting a communication was as simple as attaching two alligator clips to the right wire—hence the word "wiretapping." Communications through the Internet are wholly different: the information being transmitted is broken up into small "packets" that are separately transmitted along different routes and then reassembled when they arrive at their destination. This disassembly of the data makes effective interception appreciably more difficult.

These two technological developments have led to controversy over critical policy issues that bear on cyber conflicts today. In the wiretapping realm, can the government require communications transmission companies to assure the

---

* © *Paul Rosenzweig. Carnegie Fellow, Medill School of Journalism, Northwestern and Professorial Lecturer in Law, George Washington University.* *Portions of this article will appear as a chapter in Paul Rosenzweig, Cyberwarfare: How Conflicts In Cyberspace Are Challenging America and Changing The World (Praeger 2012) (forthcoming).*

government access to communications? In other words, can they require internet service providers (ISPs) to provide them access to the data as it transits the net?

And if they can, under what rules would these communications be accessed? At the whim of a government? Or only with an appropriate court order? Under what sorts of standards?

I. Wiretapping—Yesterday and Today

Pre-Internet, wiretapping was an easy physical task. Early telephony worked by connecting two people who wished to communicate through a single, continuous wire (typically made of copper). The image that captures this concept most readily is of a telephone operator moving plugs around on a board and, by that effort, physically establishing an end-to-end wire connection between the two speakers.

That made wiretapping easy. All that was required was attaching a wire to a terminal post and then hooking the connection up to a tape recorder. The interception didn't even need to be made at the central Publicly Switched Telephone Network (PSTN) switching station. Any place on the line would do. And, there was only one telephone company, AT&T, and only one system, so coordination with the PSTN was easy if it was authorized.

Things became a little more complicated when AT&T broke up into the "Baby Bells," but the real challenge came with the development of new communications technologies. As microwave, FM, and fiber optic technologies were introduced, the technical challenges of intercepting communications increased as well.[3] The technological difficulty in intercepting communications grew exponentially in a relatively short period of time.

Today the problem is even more complex—in addition to cellular telephones, we now have instant messaging and email and text messaging for written communications. If you want to communicate by voice, you can use Skype (a web-based video conferencing system), or Google Chat (an embedded browser-based chat program). Businesses use web-teleconference tools for teleconferences, and many people (particularly in the younger generation) communicate while present in virtual worlds through their "avatars." Twitter and Facebook allow instant communication between large groups of people.

In short, we have created a massive number of ways in which one can communicate.[4] When combined with the packet-switching nature of Internet web transmissions, and the development of peer-to-peer networks (that completely do away with centralized servers), the centralized PSTN network has become a dodo. And the Internet Engineering Task Force (the organization that sets standards for operation of the Internet) has rejected requests to mandate an interception capability within the architecture of the Internet communications protocols.[5] With these changes, the laws and policies for authorized wiretapping have, effectively, become obsolete.

Contemporary Communications Systems

Skype
X-fire
Google Chat
Google Apps
Go-To-Meeting
Quick Connect
Reddit
Tumblr
Facebook
My Space
Second Life
EVE Online
Chat Anywhere
Napster
Grokster

II. Wiretapping and Changing Technology

The law enforcement and intelligence communities face two challenges in administering wiretap laws in the age of the Internet—one of law and one of technology. The legal issue is relatively benign and, in some ways, unencumbered by technical complexity, though highly controversial nonetheless. We need a series of laws that define when and under what circumstances the government may lawfully intercept a communication. For the most part the authorization issues are ones involving the updating of existing authorities to apply explicitly to new technologies. The technical issue is far harder to solve—precisely how can the desired wiretap be achieved?

Legal Authorization—In *Katz v. United States*,[6] the Supreme Court held that the Fourth Amendment applied to electronic communications, and that a warrant was required for law enforcement-related electronic surveillance conducted in the United States. *Katz* was codified in the Omnibus Crime Control and Safe Streets Act of 1968, with particular requirements for such interceptions laid down in Title III.[7] In general, Title III prohibits the interception of "wire, oral, or electronic communications" by government agencies without a warrant and regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers.

Reflecting its pre-Internet origins, Title III originally covered only "wire" and "oral" communication. It has since been modified to take account of technological changes and now covers all forms of electronic communication (including, for example, e-mails).[8] The law also regulates the use of "pen register" and "trap and trace" devices (that is, devices designed to capture the "addressing information" of a call, such as the dialing information of incoming and outgoing phone calls). In general, this "non-content" information may be collected without a warrant or showing of probable cause, unlike the "content" portions of a message.

As a core part of its structure, Title III also incorporates certain privacy and civil liberties protections. It permits issuance of an interception warrant only upon a judicial finding of probable cause to believe that the interception will reveal evidence that "an individual is committing, has committed, or is about to commit" certain particular criminal offenses.[9] Title III also has minimization requirements—that is, it requires the adoption of procedures to minimize the acquisition and retention of non-publicly available information concerning

non-consenting U.S. persons who are not the targets of surveillance, unless such person's identity is necessary to understand the law enforcement information or assess its importance. In other words, if while investigating a terrorist case, the wiretap intercepts a conversation with a doctor, or a lover, or a pizza salesman that is not relevant to the investigation, that conversation must be "minimized," and information not meeting that standard may not be disseminated.

Beyond this, the use of Title III warrants is subject to periodic congressional review and oversight. Most significantly, electronic evidence collected in violation of Title III may not be used as evidence in a criminal case.

As Title III applies in the law enforcement context, the Foreign Intelligence Surveillance Act (FISA) authorizes the collection of communications for certain intelligence purposes. Passed in 1978, the Act creates the mechanism by which such orders permitting the conduct of electronic surveillance could be obtained from a specialized court—the Foreign Intelligence Surveillance Court (FISC). This court was, initially, authorized to issue orders for targeting electronic communications in the U.S. of both U.S. and non-U.S. persons based on a showing of probable cause of clandestine intelligence activities, sabotage, or terrorist activities, on behalf of a foreign power. The law was subsequently expanded to authorize the court to issue warrants for physical searches (1994), the use of pen registers/trap and traces (1999), and the collection of business records (1999).

To obtain a FISC order authorizing surveillance, the government must meet the same "probable cause" standard as in a criminal case: it must make a showing of probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power. And, as with Title III, the law imposes minimization obligations on the agency intercepting the communications.[10]

Technical Capacity—While amending the laws authorizing wiretaps to accommodate changes in technology has been, for the most part, a ministerial exercise of amending legislation, the same cannot be said of maintaining the technical capacity to tap into the ever-changing stream of communications.

Congress first attempted to address this problem through the Communications Assistance for Law Enforcement Act, known as CALEA.[11] CALEA's purpose was to insure that law enforcement and the intelligence agencies would not be left behind the technology curve, by requiring telecommunications providers to build the ability to intercept communications into their evolving communications systems.

CALEA dealt with a technically feasible requirement. Initially, many digital telephone systems did not have interception capabilities built in.[12] CALEA required providers to change how they built their telecommunications systems so that they had that capacity—an effort that could be achieved, generally, without interfering with subscriber services. (As an aside, CALEA also provided for a federal monetary subsidy to the telecommunications providers to pay for the changeover.)

As drafted in 1994, CALEA's requirements were applicable only to facilities-based telecommunications providers—that is, companies who actually owned the lines and equipment used for the PSTN and Internet. "Information services providers" (in other words, those who provide e-mail, instant messaging, chat, and other communications platforms that are not dependent on traditional telecommunications) were excluded, at least in part because those forms of communication were still in their infancy and of relatively little importance.[13]

Finally, and perhaps most importantly, CALEA did not say that telecommunications providers had to give government a way of decrypting encrypted messages that were put on its network for transmission. A telecommunications provider only had to decrypt messages if it provided the encryption services itself. So if an individual independently used encryption at the origin of the message, all that CALEA required is that the telecommunications provider should have a means of intercepting the encrypted message when authorized to do so.

III. The Wiretapping Problem Today

The problem today is two-fold: Cyber criminals, cyber spies, and cyber warriors are increasingly migrating to alternative communications systems—ones like Skype and virtual worlds that are completely disconnected from the traditional PTSN networks covered by CALEA. And they are increasingly using encryption technology that prevents law enforcement, counter-espionage, and counter-terrorism experts from having the ability to listen in on communications.[14] On the wiretapping front the problems are, again, both technical and legal.

Technologically, the distributed nature makes true interception capabilities extremely difficult. In a peer-to-peer network there is no centralized switching point. And in a packet switching system where the message is broken in many parts, there is no place on the network where the whole message is compiled, save at the two end points. While peer-to peer systems can be used for illegal activity (e.g. illegal file sharing),[15] they are also an integral part of legitimate file-sharing activities.[16]

The government must use sampling techniques to intercept portions of a message and then, when a problematic message is encountered, use sophisticated techniques to reassemble the entire message (often by arranging for the whole message to be redirected to a government endpoint). The FBI developed such a system in the late 1990s, called Carnivore.[17] It was designed to "sniff" packets of information for targeted messages. When the program became public, the uproar over this sort of interception technique forced the FBI to end the program.

It is said that the National Security Agency (NSA) uses a packet sniffing system, called Echelon, for intercepting foreign communications traffic that is significantly more effective than Carnivore ever was when deployed domestically.[18] Indeed, according to the *New York Times*, the Echelon system was at the core of the NSA's post-9/11 domestic surveillance system. [19] While little is publicly known about the capacity of the Echelon system, one observer (an EU Parliamentary investigation) has estimated that the system could intercept three million faxes, telephone calls, or e-mails per minute.[20]

In order for a system like Carnivore or Echelon to work, however, the routing system must insure either that traffic is routed to the sniffer along the way or that the sniffer is physically located between the two endpoints of the communication.

Therein lies the problem—many of the peer-to-peer systems are not configured to route traffic to law enforcement sniffers.

IV. Changing Law—Addressing New Challenges

To address these problems, the U.S. government has announced its intent to seek an amendment to CALEA. According to public reports, the government would seek to extend CALEA's wiretapping requirements for traditional telecommunications providers to digital communications technologies. Doing so would, according to the government, close a growing gap in existing surveillance capabilities that increasingly places criminal or espionage activity behind a veil that the government cannot pierce.

The proposed changes would have three components: 1) expansion of CALEA's decryption requirement to all communications service providers who give their users an ability to encrypt their messages;[21] 2) a requirement that foreign-based service providers doing business in the United States have a domestic office to which the government may go where interceptions can take place; and 3) apparently, a requirement that providers of peer-to-peer communications systems (like Skype) alter their software to allow interception of distributed communications. The government, speaking through Valerie Caproni, the General Counsel for the FBI, has argued that these proposed changes (which are expected to be the subject of legislative consideration in the coming year) would not give additional wiretapping authority to law enforcement officials, but simply extend existing authority "in order to protect the public safety and national security."[22]

The government's proposal poses any number of challenging legal and policy issues that will need to be addressed when (or if) Congress gets around to considering the question (some of these are issues unique to American consideration, others will be repeated globally).

The principal legal issues will, as before, involve authorization rules and standards for operation. Presumably, if the government is to be taken at its word, it will be seeking no greater interception authority than exists today for wire communications—routinized access to non-content "header information" joined with a probable cause standard for access to "content."

In some conceptions, the CALEA expansion might also implicate the Fifth Amendment protection against self-incrimination. Imagine an individual who encrypts messages he sends across the Internet. The courts have yet to determine whether or not an effort to compel that individual to disclose the decryption key constitutes a violation of his Fifth Amendment privilege. In general, the answer to the question will turn on whether disclosing the decryption key is thought of more like the production of a physical object (such as the physical key to a lock box), which may be compelled, or like the production of a person's mental conceptions (such as the memorized combination to a safe), which may not be.[23]

These Fifth Amendment considerations are likely to be of limited applicability. Even in many peer-to-peer applications (like Skype), the encryption keys are held by a centralized provider who uses the user-generated keys to enable encrypted communications from a variety of different platforms where the user might log in. In effect, to make the system more convenient, the user allows a third-party coordinator (here, Skype) to have access to the key. In doing so, Fifth Amendment protections are likely waived.

At bottom, however, the issues raised by the nascent proposal are more policy questions than legal questions. Consider a short list of these sorts of questions:

Is implementation of an expanded CALEA even technically feasible in all cases? How will software developers who are providing peer-to-peer services provide access to communications when there is no centralized point in the network through which the data will need to pass? Presumably this will require developers to reconfigure their software products in ways that permit the interception and decryption.

Think, for example, of an open-platform encryption program like TrueCrypt, where users retain sole possession of their own generated encryption keys. Here, the users might retain Fifth Amendment rights against self-incrimination that would protect them against the compelled disclosure of their keys—but could CALEA be amended to require that software commercial vendors who manufacture such programs include decryption back-doors? The answer is unclear.

And if they could, what then? Depending on how broad the modified CALEA requirements are, the economic costs of modifying existing platforms could run into the hundreds of millions, if not billions, of dollars. When CALEA was first implemented, the federal government made funds available to offset the costs of the upgrades.[24] Would it do so again, and to what degree?

More significantly, what would be the security implications of requiring interception capabilities in new technologies? Building in these capabilities would necessarily introduce potential vulnerabilities that could be exploited, not only by those who would have authorized access, but by hackers who found a way to crack the capabilities of the protection itself.[25]

And, finally, there are issues to be considered in connection with international perceptions of American conduct. In recent months, there has been a spate of efforts by various foreign governments to secure access to Internet communications.[26] It is difficult, if not impossible, for the United States to oppose such efforts in international fora when its own policy favors expansions of interception capabilities domestically. Indeed, our stated public policy favors Internet freedom, in large part as a way of energizing democracy movements around the world[27]—a policy that is difficult to square with a domestic move toward greater governmental interception capabilities.

Conclusion

Technology has evolved far faster than the law. Existing wiretapping laws will, at a minimum, need to be updated to reflect the changing architecture of distributed communications. More fundamentally, we will need to consider whether (or not) to mandate the development of technology in a particular direction for the purposes of enabling governmental activities. Doing so will surely have positive investigative benefits for the government, but there will undoubtedly be collateral legal, economic, and political ramifications of such a requirement.

Endnotes

1 Vikas Bajaj, *India May Be Near Resolution of BlackBerry Dispute*, N.Y. Times, Aug. 17, 2010, *available at* http://www.nytimes.com/2010/08/18/business/global/18rim.html.

2 Charlie Savage, *U.S. Wants to Make It Easier to Wiretap the Internet*, N.Y. Times, Sept. 27, 2010, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=2&hp.

3 Jeffrey Yeates, *CALEA and the RIPA: the U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 Alb. L.J. Sci. & Tech. 125, 135-36 (2001).

4 In the film He's Just Not That Into You (New Line Cinema 2009), one of the characters, Mary (played by Drew Barrymore), bemoans the proliferation of communications methods: "I had this guy leave me a voicemail at work, so I called him at home, and then he e-mailed me to my BlackBerry, and so I texted to his cell, and now you just have to go around checking all these different portals just to get rejected by seven different technologies."

5 IETF Policy on Wiretapping, May 2000, http://www.ietf.org/rfc/rfc2804.txt.

6 389 U.S. 347 (1967).

7 Title III is now codified in the United States Code at 18 U.S.C. §§ 2510-22.

8 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2510).

9 The list of offenses can be found at 18 U.S.C. § 2516.

10 The law makes clear that U.S. persons cannot be targeted solely on the basis of their lawful business or political relationships with foreign governments or organizations, or on the basis of other activities protected by the First Amendment.

11 Communications Assistance for Law Enforcement Act, Pub. L. No. 102-414, 108 Stat. 4279 (1994) (now codified at 47 U.S.C. § 1001-1021).

12 Dan Eggen & Jonathan Krim, *Easier Internet Wiretaps Sought; Justice Dept., FBI Want Consumers to Pay the Cost*, Wash. Post, Mar. 13, 2004, at A01; Marcia Coyle, *Wiretaps Coming to Internet; Critics Considering Legal Challenges*, Nat'l L.J., Aug. 15, 2005, at P1.

13 Initially, Voice over IP (VoIP) services (that is, telephone-type connections using the web instead of phone lines for the connection) were excluded from CALEA. In 2006 interconnected VoIP services (i.e. any service where a portion of the call was connected to a PTSN, like the service provided by Vonage) were included under CALEA. *See In re* Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs,, 20 F.C.C.R. 14989, ¶¶ 9-37 (2005).

14 Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. Times, Sept. 27, 2010, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=2&pagewanted=1.

15 Napster, for example was the first peer-to-peer network used for large-scale music sharing. Since then, there have been dozens of similar file sharing programs, many used for seemingly illicit purposes.

16 For example, Ubuntu Linux and World of Warcraft patches are distributed using the BitTorrent protocol.

17 John C. K. Daly, *Echelon—the Ultimate Spy Network?*, United P. Int'l, Mar. 1, 2004, http://slickmisc.spunge.org/list/200403/msg00006.html.

18 Duncan Campbell, *Inside Echelon: The History, Structure and Function of the Global Surveillance System Known as Echelon*, Echelon On Line, July 25, 2000, http://echelononline.free.fr/dc/insideechelon.htm.

19 James Risen & Eric Lichtblau, *Bush Lets US Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

20 Daly, *supra* note 17.

21 Google, for example, now encrypts all e-mail in its system, while in transit, unless a user opts out of the encryption policy and chooses to send his e-mail unencrypted. Presumably, under the government's proposal Google would need to re-engineer its system to allow decryption upon receipt of an authorized government request.

22 Savage, *supra* note 14.

23 The contrasting formulations were posited as useful analogies in *Doe v. United States*, 487 U.S. 201 (1988). In *Doe*, the signing of a blank bank consent form was considered more like the production of a physical object. By contrast in *Hubbell v. United States*, 530 U.S. 27 (2000), the documents produced by the defendant in response to a subpoena were organized and selected through his own mental analysis and thus protected from disclosure. Few court cases have addressed the encryption question directly: Two, *United States v. Rogozin*, 2010 WL 4628520 (W.D.N.Y. Nov. 16. 2010) and *United States v. Kirschner*, 2010 WL 1257355 (E.D. Mich. March 30, 2010) thought that the password could not be compelled, while another, *In re Boucher*, 2009 WL 424718, *1 (D. Vt. 2009), *available at* http://federalevidence.com/pdf/2009/03-March/InreBoucherII.pdf, was decided on the technicality that Boucher had already given the government access to his computer once, so he could not object to doing so a second time and disclosing his encryption key.

24 *See* FBI & Dept. of Justice, Communications Assistance for Law Enforcement Act (CALEA) Implementation Plan, Part V, Mar. 3, 1997, *available at* http://www.cdt.org/digi_tele/CALEA_plan.html#five.

25 When the Clipper chip (a chip to allow decryption of encrypted phone traffic) was first introduced, flaws in it were quickly found. *See* Matt Blaze, Protocol Failure in the Escrowed Encryption Standard (Aug. 20, 1994), *available at* http://www.crypto.com/papers/eesproto.pdf. More recently, Greek official communications were intercepted illegally through a security flaw created by the inclusion of built-in interception feature. *See Vodafone Greece Rogue Phone Taps: Details at Last*, H Security, *available at* http://www.h-online.com/security/news/item/Vodafone-Greece-rogue-phone-taps-details-at-last-733244.html.

26 In addition to the Indian example mentioned at the outset, see *UAE Crackdown on BlackBerry Services to Extend to Foreign Visitors*, Wash. Post, Aug. 3, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080204752.html.

27 Hillary Clinton, Remarks on Internet Freedom, Jan. 21, 2010, *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.