CALEA II: Risks of Wiretap Modifications to Endpoints

Ben Adida
Collin Anderson
Annie I. Anton *(Georgia Institute of Technology)*
Matt Blaze *(University of Pennsylvania)*
Roger Dingledine *(The Tor Project)*
Edward W. Felten *(Princeton University)*
Matthew D. Green *(Johns Hopkins University)*
J. Alex Halderman *(University of Michigan)*
David R. Jefferson *(Lawrence Livermore National Laboratory)*
Cullen Jennings
Susan Landau *(privacyink.org)*
Navroop Mitter
Peter G. Neumann *(SRI International)*
Eric Rescorla *(RTFM, Inc.)*
Fred B. Schneider *(Cornell University)*
Bruce Schneier *(BT)*
Hovav Shacham *(University of California, San Diego)*
Micah Sherr *(Georgetown University)*
David Wagner *(University of California, Berkeley)*
Philip Zimmermann *(Silent Circle, LLC)*[1]

17 May 2013

Abstract: The U.S. government is proposing to expand wiretap design laws broadly to Internet services, including voice over Internet protocol (VoIP) services and other peer-to-peer tools that allow communications in real-time directly between individuals. This report explains how mandating wiretap capabilities in endpoints poses serious security risks. Requiring software vendors to build intercept functionality into their products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security of the United States.

[1] Affiliations are for identification purposes only. The authors thank the Center for Democracy & Technology for coordinating this effort.

1 Introduction: "Going Dark" and CALEA II

The Washington Post and the New York Times have reported that the U.S. government is considering extending wiretap design laws to cover Internet communications services and software.[2] The Federal Bureau of Investigation argues that ongoing changes in the communications environment are making government electronic surveillance harder, so hard, in fact, that government agents are at risk of "going dark."[3] On technical details, the government is not specific; the FBI has described various aspects of the problem and it appears that its concerns include a variety of Internet-based services that allow voice, video, or text communications in real-time or near real-time. It is clear that the FBI would like policymakers to adopt new legislation requiring some products to be born wiretap-ready or to be modified upon government demand to be wiretap-ready.[4]

This could encompass a wide range of products and services, from instant messaging and chat to Skype to Google Hangouts to Xbox Live. It could include services offered through a variety of means, from stand-alone services to features built into web browser software and social networking sites. The most recent media accounts of the still-secret proposal lack information about the scope of services or companies that would be covered.[5] These stories report that the government seeks 1) authority to fine "companies" that do not comply with wiretap orders,[6] and 2) to expand wiretap obligations to peer-to-peer VoIP services.[7] It is this second aspect of the proposal that is the focus of this report: mandated wiretap modifications to endpoint software and services that allow direct, peer-to-peer communication.[8]

In contrast to the view that the government is going dark, there is a contrary view that technological changes have made available to the government vastly more information than ever before.[9] However, in our analysis we have not attempted to assess the merits of the FBI's characterization of the problem. Instead, we have chosen to focus entirely on the technical issues associated with one aspect of the proposed solution: the mandating of wiretap capabilities in endpoint systems. This report examines the properties of wiretapping mandates on endpoint systems and outlines the technical risks and implications of deploying endpoint systems that provide surreptitious access to communications in real-time or near real-time. We conclude that deployment of an intercept capability in endpoint communications services, systems and applications poses serious security risks.

---

[2] Ellen Nakashima, "Panel seeks to fine tech companies for noncompliance with wiretap orders," Washington Post, (April 28, 2013), *available at:* http://articles.washingtonpost.com/2013-04-28/world/38885216_1_wiretap-proposal-companies; Charlie Savage, "U.S. Is Weighing Wide Overhaul of Wiretap Laws," New York Times, (May 8, 2013), *available at:* http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html.

[3] Valerie Caproni, Statement before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, (February 17, 2011), *available at:* https://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies. The FBI testimony and other government materials — see: http://info.publicintelligence.net/FBI-GoingDark.pdf (FBI Situational Information Report on technical mechanisms that frustrate surveillance efforts) and https://www.eff.org/document/ice-documents-released-response-calea-foia (Customs and Border Protection FOIA response detailing instances where surveillance has been frustrated) — make it clear that "going dark" encompasses a variety of issues, including disputes about the wording of government orders, isolated failures of otherwise sufficient interception systems, dissatisfaction with government-developed industry standards, and government claims that some companies already covered by interception design mandates have not complied.

[4] *See:* Declan McCullagh, "FBI: We need wiretap-ready Web sites – now," CNET, (May 4, 2012) *available at:* http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

[5] *See:* Nakashima and Savage, fn. 2.

[6] Under current law, wiretap orders can be issued not only to any provider of wire or electronic communications service but also to any "landlord, custodian, or other person." 18 U.S.C. § 2518(4). The FBI apparently has in mind some subcategory of these entities.

[7] *See:* Savage, fn. 2 ("The 1994 law would be expanded to cover peer-to-peer voice-over-Internet protocol.")

[8] We also expect to have technical objections to the proposal that would enhance penalties for inadequate response to wiretap orders, but the specifics of that part of the proposal remain vague.

[9] *See*, e.g., Peter Swire, Kenesa Ahmad, "'Going Dark' Versus a 'Golden Age for Surveillance'" (Nov. 28, 2011) (arguing that we live in a "golden age of surveillance" as both the overall volume of information available to the government has greatly expanded and entire new categories of electronic data are being generated) https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance.

2 Technical Background: Monitoring Communications

In the United States, the Communications Assistance for Law Enforcement Act (CALEA) currently requires telecommunications service providers to design their networks to ensure that law enforcement and national security officials can perform lawfully authorized electronic surveillance at service provider premises.[10] In 2005 the Federal Communications Commission (FCC) adopted a rule extending CALEA obligations to facilities-based broadband Internet-service providers (such as cable companies) and interconnected VoIP services — that is, VoIP that can send or receive calls into the public switched telephone network (PSTN).

Traditional telecommunications involved a limited number of service providers offering access services through a limited number of switches. On the public telephone network, the customer had a relatively dumb handset that was connected to a "central switch." This switch controlled call setup and all content flowed through the switch to the recipient. In classical analog phone systems as well as in modern mobile systems, tapping can be performed at the switch without any interaction with the endpoint.

Even as the telephone network transitioned to digital carriage, and as companies began offering broadband Internet access that carried a wide range of services, including voice, all the call setup information and all the content from a subscriber using a particular access point (DSL, cable, wireless) was fed through a facility serving a limited geographical area (a switch or, in the case of cable, the headend or CMTS) that allowed access to the full communications stream. The government, when tapping a particular person's data stream, increasingly had to sort through an array of services (real-time voice calls, email, chat, web browsing, attachments to email), but it could still access these at the "last mile" facility (although some may be encrypted).

Now, however, users are increasingly mobile and use services from a variety of service providers at an increasingly large number of access points, making it more challenging to predict how a user will be connected at a given moment. As we understand the government's problem, the geographically-limited routing facilities that had previously been the focal point of interception no longer provide access to all a target's communications.

In response, it seems the government has two options:

- To wiretap at points where communications can be accessed in a centralized manner; or,
- To access communications at the end-points, by controlling the software or hardware of the endpoints.

Sometimes, there is no centralized point where content is accessible. For example, most VoIP systems have centralized call setup but do not centralize carriage of content. For instance, in a typical VoIP system using the protocol known as SIP,[11] while a centralized system controls call setup, the communications content flows directly between the endpoints ("peer-to-peer"). If an individual is using a fixed access point (such as residential broadband), the content can still be captured at the local switch (the "headend" in the case of cable broadband). However, once a person moves, for example using different Wi-Fi hotspots, it becomes harder for government wiretappers to keep up (though it may be possible to gather pen register information — call routing metadata — at the service provider's central facility).

2.1 Monitoring at the Center

With some Internet services, there is a centralized point where communications are aggregated or controlled. For example, in some VoIP services, the service provider operates a central signaling service that provides:

- Access to pen register information (i.e., who is calling whom).
- The ability to redirect or duplicate the content stream to a location where it can be monitored.

[10] Throughout the remainder of this report, we use "CALEA I" to refer to existing CALEA obligations and "CALEA II" for what we believe to be currently proposed changes.

[11] Rosenberg, J., Schulzrinne, H., Camarillo, G., *et al.*, "SIP: Session Initiation Protocol," IETF, RFC 3261, June 2002, *available at:* https://www.ietf.org/rfc/rfc3261.txt.

Of course, if the traffic is end-to-end encrypted, access to the call content is of limited utility. With older VoIP systems,[12] the signaling server generally had access to the keying material, but modern systems[13] are designed to prevent centralization of keying material for security reasons.[14] With such systems, any effort to substitute the keying material of the intercept service in place of the users' keying material would be detectable by the user and, depending on the system results in the call not connecting. This is to say that only in relatively outdated VoIP systems will central monitoring be feasible. Modern peer-to-peer services don't have such central points at which content can be monitored; to mandate that they do so would require substantial re-engineering that would fundamentally change the service and be expensive to implement, maintain and operate.

2.2 Monitoring at the Endpoint

These technical limitations of centralized monitoring have led to suggestions that instead monitoring should be provided at the endpoints. That is, end-user software should be modified to support monitoring. When monitoring is desired, the feature is activated and the software starts delivering copies of its keys, traffic, or both to some monitoring point. This may or may not be achievable in a way that is undetectable to the user. For example, a Chinese-localized version of the Skype software, called TOM-Skype, used by over 90 million Chinese people has clearly been modified such that when a user sends certain terms during chat sessions, those chat messages are censored (i.e., never delivered to the intended recipient) and/or subject to surveillance (i.e., delivered to a TOM-Skype server, and possibly to the Chinese government).[15]

3 A Wiretap Mandate on Endpoints Will Present Serious Security Risks

Security is a fundamental requirement of communications systems. Commerce, government and interpersonal relationships all rely upon secure communications. However, we know that our communications systems today are under attack, with a particular focus on endpoint systems. Government information and communications systems, including law enforcement and national security systems, have been targeted,[16] as have corporate systems, including the systems of communications service providers.[17] It is in this context that we raise our concern: A wiretap design mandate on communications tools is, plainly put, an opportunity for increased exploitation. As we explain below, extending CALEA to endpoint software and devices will make communications systems, products and services even more vulnerable.

3.1 Vulnerabilities That Are Hidden in Design and Operation Pose Serious Security Risks

All networks, software, and communication tools that support "lawful intercept" include features that are designed to breach the confidentiality of communications without detection by any party involved in the communication. When parties communicate using services with such features, there is an increased likelihood that an unauthorized and/or malicious adversary with the right technical knowledge and access to the system

---

[12] For example, those that use SDP Security Descriptions. *See:* Andreasen, F., Baugher, M., Wing, D., "Session Description Protocol (SDP) Security Descriptions for Media Streams," IETF, RFC 4568, July 2006, *available at:* https://tools.ietf.org/rfc/rfc4568.txt.

[13] For example, ZRTP and DTLS-SRTP. *See:* Zimmermann, P., Johnston, A., Callas, J., "ZRTP: Media Path Key Agreement for Unicast Secure RTP," IETF, RFC 6189, April 2011, *available at:* https://tools.ietf.org/rfc/rfc6189.txt; McGrew, D., Rescorla, E., "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)," IETF, RFC 5764, May 2010, *available at:* https://tools.ietf.org/rfc/rfc5764.txt.

[14] The "signaling server" is the directory server that handles call setup between the two endpoints. "Keying material" refers to the encryption keys needed to render the call content.

[15] Vernon Silver, "Cracking China's Skype Surveillance Software," Bloomberg BusinessWeek (March 8, 2013), *available at:* http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it; Jeffrey Knockel, Greg Wiseman, "Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC," Boston Freedom in Online Communications Day (BFOC 2013), Boston, Massachusetts (March 2013), *available at:* http://cs.unm.edu/~jeffk/publications/bfoc2013censorship-slides.pdf.

[16] James Andrew Lewis, "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies (November 20, 2012), *available at:* http://csis.org/publication/cyber-events-2006.

[17] David Drummond, "A new approach to China," Official Google Blog (January 12, 2010), *available at:* http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (describing a sophisticated and targeted attack against Google).

could capture communications contents without detection. The general nature of CALEA-style mandates and the necessarily clandestine nature of intercept mechanisms increase security risks further.

The cleverest and most dangerous cyber-attackers are those who are able to not only compromise a system but also to evade detection. That is also precisely the objective of a government surveillance solution: to compromise communications without detection. We know that communications networks and services are increasingly the subject of exploitation, often because of unintended and not very well-hidden vulnerabilities. Wiretap capabilities can be uniquely dangerous precisely because they are developed to be hidden, both in design and in application. Wiretaps are designed to be kept secret from both the parties involved in the communication and also from anyone else that does not have a "need to know" in order to execute the tap (including employees of the service provider who are on the alert for system compromises).[18] This requirement for obscurity increases the security risks further because it increases the possibility that a malicious communications intercept could be effectuated with low risk of discovery.[19]

3.2 There Is a High Risk That Wiretap-Modified Endpoints Will Be Vulnerable

3.2.1 Building Wiretap Capability in Endpoint Software Is Dangerous

In a traditional CALEA monitoring setting, the *vendor* builds CALEA access into key network components used by a network operator and the *network operator* performs the wiretap. That is, the access only occurs with the operators' cooperation, and the operators are ultimately in control of their own systems. Further, CALEA I mandates focused on a relative handful of telecommunications network operators who have a long history of cooperating with the government to provide access and have substantial experience and capabilities for monitoring and securing their networks. These service providers have procedures in place that allow trusted and carefully supervised employees to initiate wiretaps inside their networks, and they maintain security operations that are constantly monitoring for unauthorized access.

By contrast, in a system where the endpoints facilitate lawful intercept, the software developer builds the wiretap capability into end user software but the network operator does not control access. (Nor, of course, does the end user.)

The government and the developer have two choices:

- The developer designs the software, product or service so that the developer itself controls the access feature and individually responds to each governmental request for access, making a case-by-case decision about the legal validity of each such request.
- The developer provides the government or some intermediary with the requisite capabilities to access user communications without any further cooperation from the developer.

Neither of these solutions is satisfactory. In the first case, the developer not only needs to have a full-time legal department to respond to requests, but it also runs the risk that rogue employees will surreptitiously activate the intercept feature to access user communications.[20] Therefore, the developer, which may be offering its communications tool for free, would have to establish a systemic security program. It would have to adopt new standards for personnel security: to protect all information about development and operation of the intercept feature, to prevent misuse of the feature by employees, and to ensure that employees preserve the confidentiality of each wiretap in order to protect ongoing investigations. It would have to harden its own network with internal monitoring to prevent employee abuse and with outward facing measures to ensure that an outsider does not

[18] For a technical definition of wiretapping, see Section 3 of RFC 2804: Internet Architecture Board, Internet Engineering Steering Group, "IETF Policy on Wiretapping", IETF, RFC 2804, May 2000, *available at:* https://tools.ietf.org/rfc/rfc2804.txt.

[19] *See*, e.g., Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair", IEEE Spectrum, 44:7, July 2007, *available at:* http://spectrum.ieee.org/telecom/security/the-athens-affair/.

[20] Rogue insider employees may abuse their privileges and gain unauthorized access to sensitive data. *See*, e.g., Adrian Chen, "Google Engineer Stalked Teens, Spied on Chats," Gawker, (Sep. 14, 2010), *available at:* http://gawker.com/5637234/.

take over the surveillance feature or gain access to it for counter-intelligence purposes.[21] This level of security and control is simply not feasible for any but the largest vendors. Consequently, developer controlled intercept capabilities are likely to be highly insecure.

The alternative approach, providing unmediated access to government agencies, is worse. In the U.S. alone, there are many law enforcement agencies at the federal, state, and local level authorized to carry out electronic surveillance.[22] In the context of CALEA I, it is difficult for the employees of these agencies to effectuate a wiretap without the cooperation of the service provider. In the world of CALEA II, employees at each of these agencies would potentially have access to the functioning of the intercept capability, which they could then execute without the cooperation of the developer or the network operator. There would be no way for the developer or the network operator to audit or log the uses of the feature (and, of course, if the feature were well-designed to prevent compromise of investigations, it would be very difficult to know when it was activated).

This eavesdropping capability will not be limited to services for personal and commercial use. Increasingly, the U.S. government, including law enforcement and national security entities, uses commodity software and hardware. Moreover, because the same software is delivered throughout a global market, once a developer has provided access to one government, it will be under enormous pressure to provide access to many governments. The result will be endpoints that are vulnerable to monitoring by hundreds of governments, many of which have adversarial relationships with the United States and with U.S. companies and some of which suffer from high levels of corruption or close relationships with criminal elements. In short, requiring that developers build monitoring capability into end-user software and equipment poses a threat to the economic well-being and national security of the United States.

3.2.2 It Will Not Be Possible to Block Non-Compliant Implementations

The foregoing presumes that the intercept feature must be kept secret.[23] However, many modern communication software systems are built on open standards, open source implementations, or both. For instance, two of the most popular web browsers — Google's Chrome and Mozilla's Firefox — are open source programs that are developing secure communication systems based on the IETF/W3C suite of standards known as WebRTC.[24] Many open instant messaging systems support the popular Off-the-Record (OTR)[25] open source secure communications system. In such systems, it will not be possible to hide the introduction and functioning of intercept capabilities. This could compromise the effectiveness of the surveillance function, its security or both.

Furthermore, for the many products that are open source, it will be trivial for someone to build and redistribute software without the monitoring capability. This sort of "fork" is not exceptional, but rather common. The nature of Open Source software is that people take it, make small modifications, and redistribute. To provide two especially relevant examples, Iron[26] is a fork of Google Chrome that focuses on improved privacy, and the Tor Project[27] maintains its own version of Firefox that is designed to allow private anonymous communications on the Internet under extremely adversarial conditions, such as dissident users in Iran or China. If U.S. software vendors are forced to introduce wiretap capability, it seems certain that there will be non-U.S. forks of popular

---

[21] Kenneth Corbin, "'Aurora' Cyber Attackers Were Really Running Counter-Intelligence," CIO, (April 22, 2013), *available at:* http://www.cio.com/article/732122/_Aurora_Cyber_Attackers_Were_Really_Running_Counter_Intelligence.

[22] Forty-seven states (including the District of Columbia and the Virgin Islands) have adopted statutes authorizing law enforcement agencies at the state level and in many cases the local level to carry out wiretaps. *See*: "Annual Wiretap Report for 2011," U.S. Administrative Office of the Courts, (2012), Table 1, *available at:* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table1.pdf.

[23] CALEA I favored the use of published standards for wiretap capabilities to help protect against government overreaching or security vulnerabilities in the implementation of the statutory mandates; it did so by granting a safe harbor in using published standards. CALEA I could do this without loss of security because *service providers* executed wiretaps. Under CALEA II, given the diversity of services covered, it may not be possible to have standardized intercept capabilities.

[24] *See:* WebRTC, http://www.webrtc.org/.

[25] *See:* Off-the-Record Messaging, http://www.cypherpunks.ca/otr/.

[26] *See:* SRWare Iron: The Browser of the future, https://www.srware.net/en/software_srware_iron.php.

[27] *See:* The Tor Project, https://www.torproject.org/.

open source communications packages that do not allow such access. Moreover, this likelihood of non-compliant forks being developed is not limited to open source software, but also potentially relevant to proprietary, closed-source products, albeit with more effort by the fork's developers. For instance, just as it is possible to "jailbreak" proprietary phone operating system software by downloading a program that "tweaks" the software, disabling monitoring capability in wiretap-modified software may be as easy as clicking a link and running a small program that can disable intercept functionality.

It is important to understand that because these systems are built on open standards, modified software *without lawful intercept capability* will be able to interoperate with systems with the intercept capability and with unmodified systems. To take an extreme example, say that all U.S.-made Web browsers support CALEA II, thus allowing wiretapping of any WebRTC session. Two users who desire unmonitorable communications need only download secure foreign-made versions of one of the major browsers and they can make secure calls using *exactly the same infrastructure* as those that must use compliant versions. We should expect that any user who is concerned about monitoring — including many potential monitoring targets — would obtain and use an unmonitorable version of a given product or service. Ironically, then, potential terrorists may easily be able to use stronger security than the U.S. government, which is less likely to install non-U.S. forks of these programs.

4 Conclusion

The FBI's desire to expand CALEA mandates amounts to developing for our adversaries capabilities that they may not have the competence, access, or resources to develop on their own. In that sense, the endpoint wiretap mandate of CALEA II may lower the already low barriers to successful cybersecurity attacks. We believe that on balance mandating that endpoint software vendors build intercept functionality into their products will be much more costly to personal, economic and governmental security overall than the risks associated with *not* being able to wiretap all communications.