From real-time intercepts to stored records: why encryption drives the government to seek access to the cloud

Peter Swire*

The changing technology of wiretaps and government access

This section of the paper provides a brief history of wiretap technology. The history reveals two themes: (1) a shift in the place of interception from the local to the remote; and (2) a shift from ‘voice’ wiretaps in real time to ‘data’ access to stored Internet records. Taken together, this history shows a shift in how government accesses records, with a far greater emphasis today on access to records stored remotely.

Figure 1 shows the traditional wiretap of a copper phone line. In the figure, Alice is calling Bob. For a copper wire, the technology of a wiretap is quite simple—touch another copper wire to the phone line, and the sound flows to a person wearing headsets or recording the call. This wiretap might take place near Alice’s (or Bob’s) house, such as if a police officer tapped the phone line near the house. It could also take place at the telephone company’s central office, where the officer could similarly implement a wiretap.

By the early 1990s, however, many phone lines were shifting from copper to fibre optics. Copper touching a copper wire is satisfying for the wiretapper—the police officer can listen to the call. Glass touching glass is distinctly unsatisfying—no current passes from glass to glass, and no sound emerges. Other changes in technology included the emergence of call forwarding and other advanced services, so that a wiretap at Alice’s house might not capture relevant communications. Technology changes provided important justification for the passage in the United States in 1994 of the Communications Assistance to Law Enforcement Act (‘CALEA’). A core requirement of CALEA was that telecommunications carriers and manufacturers of

Abstract

- Encryption. Adoption of strong encryption is becoming much more common for data and voice communications, via virtual private networks, encrypted webmail, SSL web sessions, and encrypted Voice over IP voice communications.
- Declining effectiveness of traditional wiretaps. Traditional wiretap techniques at the ISP or local telephone network increasingly encounter these encrypted communications, blocking the effectiveness of the traditional techniques.
- New importance of the cloud. Government access to communications thus increasingly relies on a new and limited set of methods, notably featuring access to stored records in the cloud.
- The ‘haves’ and ‘have-nots’. The first three changes create a new division between the ‘haves’ and ‘have-nots’ when it comes to government access to communications. The ‘have-nots’ become increasingly dependent, for access to communications, on cooperation from the ‘have’ jurisdictions.

* Peter Swire, C. William O’Neill Professor of Law, Ohio State University; Senior Fellow, Future of Privacy Forum. Email: peter@peterswire.net.

Thanks for research assistance from Kenesa Ahmad and Steven Beale, and for comments on earlier drafts from Steve Bellovin, Caspar Bowden, and Susan Landau. This paper was funded as part of The Privacy Project’s Initiative on Systematic Government Access to Private-Sector Data.

telecommunications equipment design their products and services to ensure that they could carry out a lawful order to provide government access to communications. The Department of Justice and Federal Communications Commissioner were given important powers to assess whether products and services complied with the CALEA requirements.

In Figure 2, Alice once again calls Bob. Even if Alice has fibre optic services to the home, the telephone company is required to design its system so that lawful access is available at the switch. For mobile telephone calls, there may be encryption between Alice and the cell tower, but the telephone company has to be able to carry out a lawful access order at the cell tower or elsewhere in its network. The emphasis on access at the switch or cell tower is a step from the local to the remote. The wiretap no longer occurs next to Alice’s house; instead, the wiretap typically occurs at a switch in a digital network. This change puts the fruits of the wiretap closer to the center of the network—an interception at the central switch likely can be sent easily to a centralized location for the law enforcement or national intelligence agency.

CALEA as enacted in 1994 made an important distinction between ‘telecommunication services’, which are covered by the law, and other ‘information services’, which are not. CALEA clearly applied to the traditional voice calls made over a public switched telephone network. By contrast, CALEA did not apply to the nascent use of data sent over the Internet. The first commercial activity over the Internet was permitted only in late 1992. Thus, the meteoric rise of the Internet occurred after CALEA was drafted, and the Internet was left unregulated by the CALEA requirements to design products and services as wiretap ready. In a 2005 order by the Federal Communications Commission, CALEA was interpreted to apply to Voice over Internet Protocol (VoIP) providers who connect calls to the public switched telephone network.

As shown in Figure 2, CALEA applied to the traditional phone network, which had one or a few dominant telephone companies in most countries. The rise of the Internet, however, placed an enormous number of different entities in the communication path from Alice to Bob. Figure 3 shows that, as Alice’s packets go from Alice to Bob, a large and unknown number of actors are potentially in the position to store those packets and read them. Some of these actors are actually or potentially malicious, from amateur hackers through organized crime groups to hostile nation states. The operators of numerous other nodes have weak cybersecurity, so that malicious parties can create ‘bots’ under their remote control, or can gain root access to servers and thus send data back to the intruding party.

---

The fundamental insecurity of the intervening nodes was well known in the 1990s, and was a key technical reason in favour of strong encryption for Internet communications. The ‘crypto wars’ of the 1990s resulted from the tension between (1) this technical need for strong communications security and (2) the opposing concern of law enforcement and national security agencies that strong encryption would block access to data, a problem that has since become known as ‘going dark’.\(^5\) In 1999, the US government shifted its position, and permitted the exporting of strong encryption to most countries and for most purposes.\(^6\)

The growing adoption of strong encryption

Although the exporting of strong encryption from the USA became generally legal in 1999, actual adoption was lower than expected for email and other Internet actions.\(^7\) After all, few of us make a conscious decision to use an encryption program as part of sending and receiving email. Despite this previously low adoption, a major point of this paper is that effective encryption is in the midst of becoming the default way that many communications occur on the Internet.

Figure 4 illustrates the effect of strong encryption on lawful access at an Internet Service Provider or in the other nodes of the Internet between Alice and Bob. In the diagram, Alice wraps her message in Bob’s ‘public key’. This public key is a long set of numbers that Bob posts publicly, to enable anyone to send a message to him. The message is thus encrypted all the way between Alice and Bob. At Bob’s end, he deploys his ‘private key’, known only to him, to return the encrypted communication to plain text.

This encryption by Alice and Bob limits the usefulness of a lawful access order implemented at Alice or Bob’s Internet Service Provider (ISP), or at any node in the Internet between Alice and Bob. The reason is simple—the order may capture the bits of Alice’s message, but those bits are strongly encrypted. The lawful order does not give the government agency access to the content of the communication, unless special circumstances exist (eg use of weak encryption or government knowledge of Bob’s private key).

For today’s Internet, one variation is worth noting. Major webmail providers, including Gmail and Hotmail, now automatically encrypt emails from their customers to their own servers. A lawful order at the ISP level thus sees only encrypted, unreadable ones and zeros. However, and central to the emerging strategies for lawful access, emails saved by Alice or Bob on the webmail’s servers are not strongly encrypted. Instead, by default the server owner retains the technical ability to read the plain text of the emails. A lawful access order to the server owner (often referred to as a ‘cloud provider’) can successfully compel disclosure of the email content.

The shift to encryption for major webmail providers, all by itself, substantially reduces the effectiveness of a lawful access order to an ISP. This shift occurs in the context of the widespread adoption of other effective encryption:

- Corporate and government users have widely adopted Virtual Private Networks (VPNs) for remote users. VPNs are strongly encrypted, thus protecting the organization’s emails and other communications.
- Electronic commerce, including credit card numbers, is overwhelmingly conducted today using SSL (Secure Sockets Layer).
- Facebook now supports SSL. If it enables SSL by default, then its social networking communications would not be readable at the ISP level.
- Research in Motion’s Blackberry products use strong encryption, and RIM itself does not have the keys for corporations who manage keys themselves.


\(^6\) The White House announcement of this policy is at <http://intellit.muskingum.edu/cryptography_folder/encryption2.htm>.

\(^7\) For a panel discussion of ‘Why Traditional Encryption Products Have Low Adoption’, see <https://www.voltage.com/PKC/index.htm>. 
Major web locker services, such as Dropbox, use SSL by default.

Skype, the leading VoIP provider, encrypts end-to-end. Many international calls are made using Skype. VoIP enables voice communications to be encrypted at scale.

Many Internet games and other services use encryption, often with accompanying voice and chat channels.

Taken together, these changes indicate that widespread encryption adoption is well under way for email and voice communications. This shift brings greater cybersecurity, greatly reducing the risk that the millions of nodes of the Internet can be used to read the content of communications. The shift also means that government agencies will be far less likely in the future to be able to intercept the content of communications at the local ISP or telephone company.

Why these technology trends result in greater focus on cloud providers

The widespread adoption of encryption for communications affects the choices for government agencies seeking lawful access. Logically, there are four ways for agencies to access communications:

1. break encryption in transit;
2. intercept before or after encryption;
3. assure access in unencrypted form;
4. access after the fact, in stored form, often in the cloud.

A major descriptive conclusion of this paper is that a wide range of law enforcement and national security agencies will face large or insuperable obstacles to the first three methods. These agencies will thus increasingly depend on access to stored records, notably those stored in the cloud.

Break encryption in transit

By definition, ‘strong’ encryption means that it is extremely difficult for government agencies or others to get the plain text of encrypted communications. For an unbroken encryption algorithm, attackers must use a brute force attack, trying each possible key until the plain text is revealed. A higher key length exponentially increases the average number of calculations needed on average to decrypt a communication. Today, users of encryption can simply increase the key length to make brute force attacks ever more difficult.

After the USA permitted the exporting of strong encryption in 1999, routine commercial deployment of encryption became unbreakable, as a practical matter, for most law enforcement and national security agencies. Academic cryptographers constantly test for flaws in widely-used cryptosystems, and publish known attacks. This constant and public testing of cryptosystems means that flaws become widely known.

As with other methods of access, it is possible that there are ‘haves’ when it comes to breaking encrypted messages. One recent publication claimed that the US National Security Agency has made a significant breakthrough against the globally used Advanced Encryption Standard. Without access to classified information, it is not possible to assess this claim, or the extent of any such breakthrough. This sort of breakthrough, however, is at most available to a tiny subset of all law enforcement and national security agencies that may wish to gain lawful access to communications. For the rest, breaking modern encryption is not feasible.

Intercept before or after encryption

If it is too difficult to break an encrypted message, then government agencies may try to get access to real-time communications before or after they are encrypted. One way to do this is by physically entering a person’s home or business, and installing a bug or

---


9 My thanks to Chris Soghoian for his insights on the effects on the ‘haves’ and ‘have nots’.

other surveillance device. Such a physical entry may be used in high-priority cases, but it is risky and costly for government agencies to insert such devices often.

An approach with less risk of an agent being caught would be for the government agency to hack into the target’s computer remotely. The large size and number of ‘bot farms’ and other compromised computers suggests that an appreciable fraction of computers may be open to such attacks. According to one estimate, at least 6 per cent of the world’s four billion IP addresses are part of a zombie network, and another expert estimates that the top four botnets alone control over 20 million computers.

The adoption of strong encryption creates a motive for government agencies to break into a target’s computer before or after encryption. The large number of vulnerable computers creates an opportunity for such entry. Press reports of an FBI ‘computer and internet protocol address verifier’, placed remotely on a user’s computer, provide evidence that these sorts of software break-ins have occurred in at least some instances. Sophisticated government agencies may thus employ this strategy in high-priority cases.

There are nonetheless important reasons to believe that hacking into targets’ computers is not and will not be a major strategy for lawful access. First, this sort of secret and routine access, into users’ actual computers, is unlikely to remain secret over time. Second, the legal infrastructure for this sort of government hacking is uncertain or non-existent in many jurisdictions. Third, the growing recognition of the importance of cybersecurity creates strong policy reasons to improve computer security, rather than rely on weak security for lawful access.

Assure access in unencrypted form

Another route for lawful access is for the law to mandate a communications infrastructure that assists lawful interception. As discussed above, CALEA is a prominent example, requiring that telecommunications products and services in the USA be wiretap-ready. Similar rules exist under the Regulation of Investigatory Powers Act of 2000 in the United Kingdom, and Canada is now considering similar legislation. The analysis here suggests that such laws may remain an important source of lawful access in some settings, but are unlikely to succeed for many types of communications of interest to government agencies.

For landline telephone calls, CALEA means that telephone calls can be accessed ‘in the clear’ (unencrypted) at the switch. For wireless calls, there typically is encryption from the handset to the tower, and the telephone company decrypts the call at the tower or elsewhere so that the wiretap can operate. The handsets themselves must comply with CALEA as well. CALEA is thus an example of an architectural rule—the telecommunications architecture is created in a manner that enables lawful access to the telephone call.

Going forward, a key question is the scope of this architectural rule as communications shift from the traditional telephone network to the Internet. Telephony has historically covered a small number of large, regulated companies, and a tiny fraction of telephone equipment has used strong encryption that would frustrate a wiretap. Implementation of CALEA even in this environment took a number of years and included contentious court suits. Yet it is relatively easy to enforce CALEA in this setting of a few companies, experienced with regulators, and with little encryption.

The Internet, by contrast, features a large and shifting array of (often unregulated) information services providers, not just for VoIP but for a burgeoning array of text, audio, and video services. And the computers, games consoles, and other products that use these services are also incredibly diverse. Requiring ‘wiretap readiness’ for all of these products and services would be considerably more difficult than for traditional telephony, given the diversity of products and services, the lack of regulatory experience among many of the actors, and the widespread use of encryption in many Internet activities.

A popular online video game such as World of Warcraft (WoW) illustrates the different perspectives of government agencies and Internet users. To players of WoW (such as my sons), WOW is a fun game. They

15 CALEA itself preserves the ability of a telecommunications carrier to provide a service where users perform the encryption themselves: ‘A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication’ 47 U.S.C. § 1002(b)(3).
often wear headsets to talk with teammates while playing, and keep a chat window scrolling as well. To law enforcement, WoW (or any other similar game) can seem instead to be a global terrorist communications network. Players can talk and send chat messages, internationally, outside of the traditional telephone network and outside of the scope of CALEA. The architecture is based on what works for the game, and not what facilitates lawful access.

To summarize on this architectural approach, government agencies will face a number of practical obstacles in attempts to require ‘in the clear’ communications over the Internet. The fundamentally insecure nature of the Internet (as shown in Figure 3) means that effective encryption is vastly more common and more important for Internet services than for traditional telephone services. Even when government agencies temporarily learn how to gain access to a particular product or service, the rate of innovation on the Internet remains high—when a new game or a new version of a game is issued, the access that worked previously may no longer succeed. At a minimum, the complexity and innovation on the Internet will likely cause further separation between ‘have’ and ‘have not’ agencies, with a far greater ability to adapt for leading national agencies than for local police departments or agencies in poorer countries.

Access after the fact, in stored form, often in the cloud

The discussion thus far has highlighted new obstacles in the path of access to communications at the local ISP or telephone company. Where strong encryption is used, then attempts at such access will produce random ones and zeros rather than the contents of the communication. The widespread use of encryption is spreading from VPNs to standard webmail, social networks, and VoIP such as Skype.

When local attempts to access fail, then government agencies have a strong incentive to find content in unencrypted form, either from a party to the communication or the owner of a system between the parties. The widespread use of encryption for E-Commerce, banking, and other Internet activities means that data are often available from one of the parties to the communication (such as the E-Commerce site), but not from wiretaps in transit. Even if an entity such as the E-Commerce site encrypts its own databases, it will have the keys, so lawful access will typically not be blocked due to that encryption. In other words, the stored records of a corporate party to a communication will often be available to government agencies.

Stored records will also often be available when held by the owner of a system between the parties to the communication. For instance, most emails using Gmail or Hotmail are currently unencrypted at the server level, so government agencies around the world have reason to seek access from Google and Microsoft. In such cases, lawful access shifts from access from a local ISP to access from the cloud provider, which has stored the emails.

Here is where ‘few users deploy encryption’ shifts to its next generation. In the 1990s, e-mail encryption programs such as Pretty Good Privacy became available, but few users chose to take advantage of those programs. Thus, lawful access to e-mails remained generally available through the local ISP. Today, default use of encryption for webmail and E-Commerce means that access to content is often not available at the local ISP. Access seems likely to remain available from the cloud provider, however, for a large portion of the communications and other data held in the cloud, for a number of reasons:

1. **Key management.** It is extremely risky for users to store data in the cloud without having a backup of the keys—loss of the keys irretrievably loses access to the data. Sophisticated business customers can manage their own keys. Cloud providers, however, have a strong business reason to provide key backup, so that individuals and other less sophisticated users don’t lose all of their data if the key is lost. To understand the problem, consider how often websites have a ‘lost your password’ function—without that function, a service is much riskier for the user.

2. **Cost and loss of function of encrypted storage.** Users of webmail and other cloud services often wish to search through their data, to sort and find the information they need. More generally, individuals and organizations store data in the cloud specifically so that the data can be used more intensively, often from multiple locations. Computer scientists are actively researching the topic of search of encrypted databases. Current research indicates that using encrypted databases raises the cost of cloud services, search of such databases is considerably more difficult than standard search, and the increased difficulty is likely to continue. These functional

---

obstacles to the use of encrypted databases will reduce the demand for such encryption even from sophisticated users.

3. Incentives of cloud providers. Cloud providers may well have additional incentives to retain access to the databases stored by their customers. For instance, at least some cloud providers have business models that gain revenue based on access to unencrypted data, such as Gmail’s automatic scanning of the content of email in order to serve targeted advertisements.

In short, important incentives exist for users and cloud providers to select architectures where the cloud provider retains the ability to access content. Where such an architecture exists, lawful access remains available through the cloud provider.

This technical possibility to respond to process leads to an important, specific split between the ‘haves’ and ‘have nots’. Some jurisdictions will have the cloud server in their jurisdiction, with relatively straightforward access to the stored records under local law. Other jurisdictions will not have such access. They will have to use a Mutual Legal Assistance Treaty (MLAT) or other mechanism to gain access to the holder of the records. These ‘have not’ jurisdictions may well face added expense and delay in gaining access to the records. In some (or perhaps many) cases they will not be able to access records that they consider important for law enforcement or national security purposes. Conversely, cloud providers and other holders of records are likely to face an increasing number of lawful access requests, from a potentially bewildering array of jurisdictions.

Conclusion

The focus of this paper is to describe the effect of technical changes on likely paths for lawful access to communications information. This paper does not propose how best to resolve legal issues, including the complex multi-jurisdictional issues that will occur increasingly often. An improved understanding of the technology, however, can help clarify what legal and practical options may exist going forward.