INDYPENDENT READER
toward building a new society on the vacant lots of the old . . .
Published on *Indypendent Reader* (https://indyreader.org)

Privacy Will Survive as Long as We Work to Trust Each Other

Contributed by:
Brian Duggan[1]
Monday, May 13, 2013 - 00:00

A recent article in the Washington Post [2] details the first measures of potential legislation known as CALEA 2. The FBI and Department of Justice want to fine companies for noncompliance with surveillance orders.

The death of privacy has been a popular trope in establishment media lately. Unfortunately, pitiful displays by establishment journalists like Tom Brokaw [3] encourage Americans to comply with expanded state surveillance measures. But the facts of the reporting are usually true: our privacy is under attack from almost all authorities we are trained to trust.

Activists intuitively understand the importance of privacy. Even while many of us are forced to utilize a range of online services to communicate with each other, most of us are constantly aware that both machines and humans are sleeplessly reading and processing the information we share with, and send to, each other. We understand that the online spaces that we're forced to inhabit are both our own and the property of corporations and the state. And we use these spaces as the primary platform for expressing dissent, criticizing authority, and organizing resistance against the very authorities that control them. The contradiction is plain, and most of us feel powerless to address it.

Meanwhile, the United States is seeking to expand its already near-limitless access to these

spaces. Authorities enjoy a nearly bit-for-bit copy [4] of almost all electronic communications that light up US telecom infrastructure.

So why are law enforcement agencies threatening companies like Facebook, Google, and Twitter with fines as a punitive measure to ensure access to our communication data? While they may have access to the digital equivalents of post offices, much of the data we send and receive is encrypted by the services we use. Instead of sending letters without envelopes that the postal worker or lurking agents could read companies like Google cooperate with other software vendors to provide us with encryption technologies, the digital equivalent of stuffing a letter in to an opaque envelope. During the FBI's nefarious COINTELPRO efforts that spied on civil rights activists in the 50s through 70s, the FBI opened and read almost a quarter million pieces of mail [5] correspondence [5] between US citizens. Thanks to some sound engineering design, the same agency has a much more difficult time reading our Gmail and Facebook chat messages. Instead, remaining privacy laws and the 4th ammendment force the FBI to ask Google and Facebook for access to our data.

And much of the time, the companies comply. Some have policies that require warrants [6] before responding to requests for data. Some produce yearly transparency reports [7] about the number of requests they respond to. Eventually, though, the government often succeeds in invading our privacy. But that doesn't mean law enforcement are satisfied with this level of access. On the contrary, the DOJ and FBI intend to bully companies that don't agree with their intepretation [8] of wiretapping laws. Ultimately, the feds want direct, unfettered access to the data firehose: they want a software "backdoor" [9] in Gmail and many other similar services.

"Backdoors" are holes in otherwise secure software. Imagine that you want to send a letter to a friend through the United States Postal Service. Given historical precedent, you are reasonably concerned that a postal worker or FBI agent might read your messages. So your friend gives you a lockbox that you can put your letter in. When you need to send your friend a message, you send the whole locked box through the USPS. Your friend tells you that you and he are the only two people who have the keys to lockbox. But what your friend meant was that you, he, and the FBI agent in the local post office hold keys to the lockbox, because your friend was compelled by law to make a third copy and give it to the government. This is what the DOJ and FBI are trying to force online service providers to do with our digital communications.

This communication system is not what any honest person would consider secure. You, as a rational person, have made an informed decision that you can trust your friend. You trust your friend to keep the contents of your communication private. That means your friend neither divulges the contents of the message to other parties without your consent, nor does your friend give access to the container of that content to any other person. Your friend even wants to honor that trust. But in the real world, your friend is a corporation whose property is threatened by the US government so long as it refuses to comply with government orders to make copies of all keys for law enforcement. And breaking this trust model is the precise, explicit agenda of the FBI.

For believers in democracy, state access to the private realm of intra-citizen communication is a power so perverse and intrusive that it fails to pass the giggle test. But the dangers for subjects to this corporate and state fiefdom don't end at the destruction of privacy from the government. Imagine that hackers in the employ of a rival state gained access to an FBI agent's office and stole (or worse, made a copy of) the key that the agent uses to read your mail. Imagine that the process of creating a third key meant modifying the lock and that made it easier for a hacker to pick the

lock. Imagine that the FBI agent hands the key over to a terrorist group in return for relieving the agent's credit card debt. All of these are real dangers as a result of electronic surveillance provisions that the FBI is seeking as part of a yet-to-surface law known as CALEA 2.

The patchwork of regulations allowing law enforcement agencies to violate our privacy is extensive and complex. The most widely understood technical surveillance mechanism, the wiretap, was permitted by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 [10]. A wiretap, while technically unsophisticated by today's standards, is a powerful tool that allows targeted collection of telephone data including the content of telephone calls, recipients of calls, and time and date of calls. Wiretaps allow authorities to collect data related to a single telephone number.

In contrast, the more recent Communications Assistance for Law Enforcement Act (CALEA), passed in 1994, mandated surveillance mechanisms at the core of United States telecommunication infrastructure. This meant that instead of targeting individuals and every party that individual communicates with, law enforcement now has the technical capability to wiretap anyone who utilizes telecommunication infrastructure. During the 2000s, the majority of electronic communication shifted to the Internet. And it was a happy coincidence for law enforcement agencies that telcos also provided Internet infrastructure. It was not difficult to expand the reach of CALEA [11] from traditional telephone services to Internet communications. But this is where surveillance powers reached what the FBI called the "Going Dark" problem. As users of services like Gmail and Facebook demanded better security, CALEA only allowed the FBI to collect encrypted communications between users and these companies, communications the FBI couldn't read without the cooperation of online service providers. Hence their need for CALEA 2 and backdoors.

But even the morass of US surveillance laws has not neutralized every opportunity for privacy. Citizens may be encouraged through schools, workplaces, advertising, and privilege or lack thereof to use these services. But few of us are truly coerced. Nor do any existing surveillance laws prohibit the creation of non-corporate email and chat services or the use of non-US-based services that would not be subject to US surveillance requirements. In a country where privacy rights are being deliberately dismantled by those who were supposed to defend them, a struggle for the freedom to choose whom we trust may supplant the struggle for privacy.

Links:
[1] https://indyreader.org/contributor/brian-duggan
[2] http://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html
[3] http://www.nbcnews.com/video/nbc-news/51552278/#51552278
[4] http://www.guardian.co.uk/commentisfree/2013/may/04/telephone-calls-recorded-fbi-boston
[5] https://en.wikipedia.org/wiki/Church_Committee
[6] http://www.wired.com/threatlevel/2013/01/google-says-get-a-warrant/
[7] https://www.google.com/transparencyreport/
[8] http://news.cnet.com/8301-13578_3-57583395-38/doj-we-dont-need-warrants-for-e-mail-facebook-chats/
[9] http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-

technologies
[10] https://en.wikipedia.org/wiki/Wiretap_Act#Wiretaps
[11] http://arstechnica.com/uncategorized/2006/07/7372/