Barr says the US needs encryption backdoors to prevent “going dark.” Um, what?

Enlarge / US Attorney General William Barr speaks at the International Conference on Cyber Security at Fordham University School of Law on July 23, 2019 in New York City. In his remarks, Barr stated that increased encryption of data on phones and encrypted messaging apps puts American security at risk. Barr encouraged technology companies to provide law enforcement with access to encrypted data during certain criminal investigations.
Drew Angerer/Getty Images

reader comments

151 with 121 posters participating, including story author

Share this story

On July 23, in a keynote address at the International Conference on Cyber Security at Fordham University, US Attorney General William Barr took up a banner that the Justice Department and Federal Bureau of Investigation have been waving for over a decade: the call for what former FBI director James Comey had referred to as a “golden key.”

Citing the threat posed by violent criminals using encryption to hide their activities from law enforcement, Barr said that information security “should not come at the expense of making us more vulnerable in the real world.” He claimed that this is what is happening today.

“Service providers, device manufacturers, and application developers are developing and deploying encryption that can only be decrypted by the end user or customer, and they are refusing to provide technology that allows for lawful access by law enforcement agencies in appropriate circumstances,” Barr proclaimed.

And this, he said, was making it increasingly difficult for law enforcement to surveil criminal activity. This blindspot what also allowing criminals to make their information and communications “warrant proof… extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes,” and allowing “criminals to operate with impunity, hiding their activities under an impenetrable cloak of secrecy.”

In other words, the lawful surveillance capabilities of the government are “going dark,” according to AG Barr.

“The net effect is to reduce the overall security of society,” he continued. “I am here today to tell you that, as we use encryption to improve cybersecurity, we must ensure that we retain society’s ability to gain lawful access to data and communications when needed to respond to criminal activity.” AG Barr closed by saying that US citizens should accept encryption backdoors because backdoors are essential to our security.

In response, Gen. Michael Hayden, former director of the National Security Agency, said, “Not really.”

> *Not really. And I was the director of national security agency*
>
> *— Gen Michael Hayden (@GenMhayden) July 23, 2019*

Regardless of the accuracy of Barr’s claims, encryption is certainly far more prevalent than it was even five years

ago—back when freshly minted memoirist Edward Snowden gave the world a look at the workings of US intelligence agencies' digital surveillance capabilities. For better or worse, Snowden's data dump continues to shake up not just the world's view of communication privacy—it upended the world's view of information security in general.

Snowden's impact on the *de jure* of mass surveillance was perhaps less than he would have hoped for. But his revelations had wide-ranging effects on the tech industry and on the development of Internet and security standards. While Snowden opened up a dialogue about intelligence policy, "some of the most significant reforms were technical, not legal."

That's according to Ben Wizner of the American Civil Liberties Union, who has acted as Snowden's attorney. "The proliferation of encryption was rapidly accelerated," he says. "And the Internet is more secure today than it was in 2013. Technology companies realized that they had been operating under the wrong threat model."

After Snowden, Internet and technology firms could no longer ignore the threat posed by state-funded actors to their customers, said Mark Rumold, senior staff attorney at the Electronic Frontier Foundation (EFF). He went on:

> *Companies recognized guarding against state surveillance is a bottom line issue for them… It is a question of financial interest to these companies to be able to convince their users that their data is secure with them, so we saw a lot of companies take steps to roll out encryption in various ways and I think that there's no question that this enhances security and privacy.*

Just how much those steps have hindered legal surveillance and investigation—attempts by law enforcement and intelligence agencies operating under the authority of a court-approved warrant—is in dispute. As information security professional

Robert Graham pointed out in a recent blog post, there is no evidence of a surge in crime corresponding to the use of encryption. Such claims, he says, are “based on emotional anecdotes rather than statistics.”

Even allegedly hard data presented by the government has been routinely inflated. In December 2017, FBI Director Christopher Wray claimed in Congressional testimony that, in the 2017 fiscal year, the bureau “was unable to access the content of approximately 7,800 mobile devices” using available tools. Wray made this proclamation a year after the government’s highly public battle over encryption with Apple in the wake of the tragedy in San Bernardino, California. But that figure was vastly larger than the 880 devices the FBI had cited a year before, and a Washington Post investigation found that the number of inaccessible devices in 2017 was actually about 1,200 according to an FBI internal estimate.

So, is surveillance really “going dark”? Or is this, as Graham suggested, “a Golden Age of Surveillance” where even more privacy is required? Joseph Lorenzo Hall, Chief Technologist at the Center for Democracy and Technology (CDT), leans toward the latter.

“The FBI says they’re ‘going dark’,” Hall told Ars. “Well yeah, because they’ve been staring at the sun.”

Fixing overexposure

Like this prison in Cuba, the NSA has turned the Internet into a place where the watchmen can see all and exploit the shoddy privacy of Internet services prior to Snowden.

Much of the Internet has become more secure over the past five years. The Snowden revelations may not have directly caused the rise of secure Web protocols, but they sure helped motivate protocol development. While the threat of a “global observer” on the Internet had been theorized before Snowden, his evidence of that sort of capability immediately triggered a response from the technical community.

“The engineering community took the succession of Snowden revelations really seriously,” Hall told Ars. Just 11 months after the first of the leaks, the Internet Engineering Task Force put out RFC 7258, “stating that pervasive monitoring is an attack,” Hall noted.

To be fair, the Internet in 2014 had practically nowhere to go but up in terms of protecting privacy. Almost all of the fundamental building blocks of the Internet were, at the time, “almost completely insecure” since their creation, Hall

explained. That's "because we were experimenting with them. And now we're retroactively having to go back and put security back on."

That shift in perception of the threat of mass surveillance was followed by significant improvements in securing Web traffic. That included much more security-focused operations at major Internet service providers. Two particular changes were accelerated by the Snowden revelations: adoption of secure HTTP (HTTPS) and TLS encryption by major Internet services, and the development of Transport Layer Security (TLS) 1.3.

HTTPS has had the biggest effect so far, and the changes in TLS will further close the door on surveillance. In 2013, less than 30% of Web traffic was encrypted, and less than 10% of websites supported secure connections. By 2017, more than half of the Web supported HTTPS, and today over 70% of Web traffic is encrypted, based on data from Google and Let's Encrypt. As of April 2019, 91% of webpages visited by US users were secured. Internationally, about 85% of webpages visited were encrypted.

Adoption of encryption for email traffic—both between client and server and from provider to provider—also grew dramatically as a direct result of the Snowden revelations. In early 2014, only about a quarter of the email traffic between Google and other providers was encrypted. Now, it's over 75%.

The adoption of encryption has had major implications for both the intelligence community and law enforcement, at least in terms of "traditional" Internet traffic. Much of the metadata we examined in our 2014 project with NPR that was usable for surveillance by the NSA's XKeyscore system has become much less accessible. We re-staged the tests recently, using ourselves as the victim. Many of the identifiers and other content we were able to pick out of passive traffic collection in 2014 have been dramatically reduced. That isn't to say that

they’re gone—they’re just concealed within encrypted HTTPS and TLS traffic now, at least for standard Web and email traffic.

This practical consideration may be directly responsible for NSA dropping “about” collection (searching the contents of traffic for communications that mentions specific keywords or identifiers for persons of interest). But there are still other ways to gather surveillance data from Internet traffic that won’t be going dark anytime soon.

Listing image by Markus Gann / EyeEm via Getty Images

https://arstechnica.com/?p=1400515