June 4, 2018

Dear Inspector General Horowitz,

The undersigned civil society organizations dedicated to protecting civil liberties, human rights, government accountability, and innovation and security online, write to urge you to investigate the failures that led to the Federal Bureau of Investigation (FBI) and Justice Department's inaccurate representations of the number of devices that the FBI could not unlock due to encryption, as recently reported in the *Washington Post*.[1] We also ask that you investigate Justice Department officials' repeated use of those flawed statistics *after* the FBI discovered the miscalculation.

In sworn testimony before Congress and in public remarks, top-ranking officials from the Justice Department and the FBI claimed that in 2017, the FBI was unable to gain access to content stored on 7,775 encrypted devices. However, the *Washington Post* article revealed that, due to what the FBI described as a "programming error," the number is closer to 1,200 devices.

For years, the FBI has claimed that it is "going dark," because the increased use of encryption to protect devices places the contents of communications beyond its reach and severely impedes its investigations. During this time, some FBI officials have advocated for a technical mechanism that would guarantee law enforcement exceptional access[2] to encrypted data – what civil society and security experts refer to as an "encryption backdoor." Domestic and international civil society organizations, security researchers, and academics,[3] as well as some high-ranking U.S. national security officials,[4] have all voiced strong

---

[1] Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html?utm_term=.078374fa56bb

[2] Similar to other publications, including the 1996 National Academies CRISIS report and "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," we use the term "exceptional access" to "stress that the situation is not one that was included within the intended bounds of the original transaction." K. W. DAM ET AL., CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY, 80 (1996); Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY, no. 1, at 69 (2015).

[3] Letter from Civil Society Organizations, Companies and Trade Associations, Security and Policy Experts to President Barack Obama (May 19, 2015) (available at https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf; https://securetheinternet.org/).

[4] *See Top Counter Intelligence Official Recommends Govt. Officials Encrypt Classified Calls*, C-SPAN (May 15, 2018), https://www.c-span.org/video/?c4729458/top-counter-intelligence-official-recommends-gov-officials-encrypt-unclassified-calls; Jenna McLaughlin, *NSA Chief Stakes Out Pro-Encryption Position, In Contrast to FBI*, THE INTERCEPT (Jan. 21, 2016), https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/; Ash Carter, Sec. of Defense, Remarks with Ted Schlein in San Francisco, Calif. (Mar. 2, 2016), *available at* https://www.defense.gov/News/Transcripts/Transcript-View/Article/684858/remarks-by-secretary-carter-in-a-fireside-chat-with-ted-schlein-in-san-francisc/; Mike McConnell et al., Op-Ed., *Why the Fear Over Ubiquitous Data Encryption is Overblown*, Wash. Post (Jul 28, 2015), https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?utm_term=.831178a04269; Tom DiChristopher, *U.S. Safer with Fully Encrypted Phones:*

opposition to encryption backdoors. They have noted that any exceptional access mechanism could also be used by malicious hackers, foreign adversaries or other bad actors, and that such a mandate would pose serious threats to cybersecurity, privacy, human rights, and the U.S. economy.

The Justice Department and the FBI acknowledge the grave security implications of their requests, but they have nonetheless suggested that it is imperative that law enforcement officials be able to access encrypted communications and information stored on devices to protect public safety.[5] While Justice Department and FBI officials did not demand a legislative solution during the Obama Administration, Deputy Attorney General Rosenstein and FBI Director Wray have pushed for a policy change to mandate exceptional access to data stored on devices.[6] To prove the extent of the "going dark" problem and substantiate demands for an encryption backdoor, the Justice Department and the FBI relied heavily on their account that the FBI was locked out of almost 7,800 phones. Given the severe negative effects of an encryption backdoor mandate, the FBI's miscalculation is particularly concerning.

We are also troubled by how the Justice Department responded when it learned of the FBI's error. The *Washington Post* story states that the FBI became aware of the miscalculation approximately a month before the story was published, on May 22. Despite the FBI learning in April that the number of devices it claimed it could not unlock had been grossly inflated, Attorney General Jeff Sessions continued using that flawed statistic in public remarks before the Association of State Criminal Investigative Agencies on May 7.[7] The following day, a Justice Department official repeated the inflated number to a Bloomberg

---

Former NSA/CIA. Chief, CNBC (Feb. 23, 2016), https://www.cnbc.com/2016/02/23/us-safer-with-fully-encrypted-phones-former-nsa-cia-chief-michael-hayden.html.

[5] In an October 2017 speech on encryption, Deputy Attorney General Rosenstein said, "Encryption is a foundational element of data security and authentication. It is essential to the growth and flourishing of the digital economy, and we in law enforcement have no desire to undermine it." Rod Rosenstein, Deputy Attorney General, Remarks at the U.S. Naval Academy in Annapolis, Md. (Oct. 10, 2017), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

[6] *See* Joe Mullin, *FBI Chief Comey: "We Have Never Had Absolute Privacy"*, ARS TECHNICA (Aug. 9, 2016), https://arstechnica.com/tech-policy/2016/08/fbi-chiefs-complaints-about-going-dark-arent-going-away-will-be-revived-next-year/; Natasha Lomas, *FBI Director Comey Backs New Feinstein Push for Decrypt Bill*, TECHCRUNCH (May 3, 2017), https://techcrunch.com/2017/05/03/fbi-director-comey-backs-new-feinstein-push-for-decrypt-bill/; Christopher Wray, Director, FBI, Remarks to FBI Int'l Conf. on Cyber Security at Fordham Univ., N.Y. (Jan. 9, 2018), *available at* https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

[7] After those remarks were delivered, the Justice Department edited the published text of the Attorney General's speech to reflect the error. Jeff Sessions, Attorney General, Remarks to the Ass'n of State Crim. Investigative Agencies in Scottsdale, Ariz. (May 7, 2018), *available at* https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-association-state-criminal-investigative; Archived version of those remarks on Archive.org, *available at* https://web.archive.org/web/20180507183119/https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-association-state-criminal-investigative.

Law reporter.[8] It is very problematic that, weeks after learning of the error, the flawed statistics would still be used.

Given the serious concerns raised by the FBI's miscalculation and the Justice Department's conduct after learning of the miscalculation, we urge you to investigate:

1. The causes that led the FBI to make such a significant error, how it was identified, and why it took so long to identify;
2. Why Justice Department officials, including the Attorney General, used the data point when it was known to be false, and whether, after learning of the error, the Attorney General, other Justice Department, or FBI officials continued improperly using it in public remarks, conversations, or meetings (internal and external); and
3. What measures the Justice Department and the FBI have taken to ensure that they inform lawmakers and the public of this significant miscalculation, both prior and subsequent to the publication of the *Washington Post* story, and whether those steps were sufficient.

This investigation would be an appropriate follow-up to your recent report regarding the FBI's conduct in connection with the encrypted phone in the San Bernardino shooting investigation. In that report, your office has already found that some in the FBI did not appear to be interested in vigorously pursuing investigative leads that might undermine its campaign against the "going dark" problem, and the report raises questions about the FBI's credibility in the encryption debate. Specifically, your report concluded that the FBI *chose* "not [to] pursue all possible avenues in the search for a solution" when trying to unlock the San Bernardino shooter's iPhone. It stated that the Chief of the Cryptographic and Electronic Analysis Unit became "frustrated" and "definitely not happy" when he learned that the Remote Operations Unit had engaged a trusted vendor and identified a solution because it interfered with the FBI's litigation strategy.[9] This context shows how important it is to conduct an investigation into the FBI's miscalculation and obtain answers to the above questions.

If you have any questions, please contact Robyn Greene, Policy Counsel and Government Affairs Lead at New America's Open Technology Institute, at greene@opentechinstitute.org.

Sincerely,

Access Now
American Civil Liberties Union
Center for Democracy & Technology

---

[8] Daniel R. Stoller, *FBI Encryption Snafu Highlights Need for Compromise with Tech*, BLOOMBERG LAW (May 24, 2018), https://biglawbusiness.com/fbi-encryption-snafu-highlights-need-for-compromise-with-tech/?utm_source=bloomberg-menu.

[9] Office of the Inspector General, U.S. Dept. of Justice, A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities During the San Bernardino Terror Attack Investigation (2018), *available at* https://oig.justice.gov/reports/2018/o1803.pdf.

Council on American-Islamic Relations (CAIR)
Defending Rights & Dissent
Demand Progress Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Engine
Freedom of the Press Foundation
FreedomWorks
Free Press
Government Accountability Project
Government Information Watch
Human Rights Watch
Liberty Coalition
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Restore the Fourth
R Street Institute
TechFreedom