NAAUSA
National Association of Assistant U.S. Attorneys

February 7, 2024

The Honorable Dick Durbin
Chair
Senate Judiciary Committee
224 Dirksen Senate Office Bldg
Washington D.C. 20510

The Honorable Lindsey Graham
Ranking Member
Senate Judiciary Committee
224 Dirksen Senate Office Bldg
Washington D.C. 201510

RE: NAAUSA Written Testimony for Full Committee Hearing "Big Tech and the Online Child Sexual Exploitation Crisis"

Dear Chair Durbin, Ranking Member Graham, and Members of the Committee:

On behalf of the National Association of Assistant United States Attorneys (NAAUSA)—representing the interests of over 6,000 Assistant U.S. Attorneys (AUSAs) working in the 94 U.S. Attorney Offices—I write to emphasize the severe impact big tech's utilization of end-to-end encryption has had on the success of federal law enforcement operations, particularly operations against crimes involving the exploitation of children, recruitment of terrorists, and proliferation of drugs online.

From 2016 to 2020, nearly every major category of internet crime saw dramatic increases in complaints issued to the Federal Bureau of Investigations (FBI).[1] In 2021, the nonprofit National Center for Missing & Exploited Children received 29.3 million reports of suspected child exploitation with nearly all of the complaints coming from phone and social media companies.[2] That is an increase of 35% from 2020.[3] Finally, in the first quarter of 2022 alone, Meta took actions against 3.3 million pieces of drug related content on Facebook and another 1.8 million on Instagram.[4]

The data is staggering, but the message is clear: illegal activity on social media and through the use of messaging and other digital applications is happening and it is only getting worse.

Despite this, social media companies, internet service providers and other digital communications companies are taking steps to lock law enforcement out of investigations into these crimes by implementing end-to-end encryption across their platforms. This is a dangerous path that will undermine public safety unless Congress acts to ensure law enforcement access to critical evidence.

As a threshold matter, law enforcement sees the value in end-to-end encryption. Not only does it enhance consumer privacy, but it also can be critical to preventing identity theft and fraud. Nonetheless, when companies implement end-to-end encryption without a clear path for law enforcement to access information pursuant to a lawful court order, the technology translates to a complete lock out of law enforcement.

Even Discord CEO Jason Citron acknowledged this risk during the hearing, saying, "End-To-End Encryption… blocks anyone including the platform itself from seeing users' communications. It's a feature on dozens of platforms but not on Discord. That's a choice we've made. We don't believe we can fulfill our safety obligations if the text messages of teens are fully encrypted because encryption would block our ability to investigate a serious situation, and when appropriate report to law enforcement."

[1] 2020_IC3Report.pdf
[2] More than 29 million reports of suspected child sexual exploitation in 2021, nonprofit center says - CBS News
[3] Id.
[4] Drug Sales Through Social Media Are Increasing (scrippsnews.com)

If social media companies cannot access encrypted data themselves, it is impossible to believe law enforcement could gain access to criminal evidence. This is not to say law enforcement should have access to all data all the time, but rather, that law enforcement must have access to evidence necessary for prosecuting a crime when acting upon issuance of a court order.

I. Meta Spotlight

In December, Meta announced its decision to make end-to-end encryption the default setting across its messaging platforms. This decision comes among widespread concern by law enforcement and victim advocacy groups.[5]

The nonprofit National Center for Missing and Exploited Children (NCMEC) called the move a "devasting blow" to child protection.[6]

Similarly, an international alliance of 15 law enforcement agencies, including the Federal Bureau of Investigation and Immigration and Customs Enforcement Homeland Security Investigations, dedicated to addressing global threats from child sexual abuse named the Virtual Global Taskforce described Meta's decision as a "purposeful design choice that degrades safety systems and weakens the ability to keep child users safe."[7]

The Taskforce shared the story of David Wilson, one of the most prolific child sexual abuse offenders the UK's National Crime Agency has ever investigated. Wilson used Facebook to contact and groom thousands of children. He created fake profiles pretending to be a teenage girl to manipulate victims into sending sexually explicit material of themselves to him. Victims were sometimes blackmailed into abusing their friends and siblings and frequently traumatized by the experience.

The UK National Crime Agency was able to successfully prosecute Wilson because law enforcement was able to access the evidence contained within over 250,000 messages through Facebook. End-to-end encryption makes investigations like these all but impossible.

Previously, Meta has been one of the largest reporters of CSAM material online. But like Google and Apple, who previously routinely provided law enforcement access to mobile phones when under a court-ordered search warrant,[8] the move toward encryption has locked out law enforcement.

Meta has made clear it will not provide law enforcement access to encrypted data barring "imminent risk of harm to a child or risk of death or serious physical injury."[9] This extremely narrow standard neglects the vast majority of criminal investigations which look backward to investigate a crime that has already been committed. Further, many online crimes involving explicit material do not pose a risk of physical injury but are no less traumatizing and severe.

[5] Meta makes end-to-end encryption a default on Facebook Messenger | AP News
[6] TechScape: Will Meta's encryption plans be a 'devastating blow' to child safety online? | Meta | The Guardian
[7] Global law enforcement coalition urges tech companies to rethink encryption plans that put children in danger from online abusers - National Crime Agency
[8] Tech companies push back against lawmakers' demands for encryption backdoors (iapp.org)
[9] Metas-approach-to-safer-private-messaging-on-Messenger-and-Instagram-DMs-Sep-23.pdf (fb.com)

Meta's response to this in its safety strategy is that "law enforcement may still be able to obtain this content directly from users or their devices."[10]

Essentially, Meta expects law enforcement to request data on criminal activity from the criminals themselves. This is an impractical and unsustainable path forward that relies on criminals to take responsibility for their actions rather than the social media companies that enable their illicit activity.

II. Privatizing Public Safety

During the hearing, many CEOs noted their efforts to identify and remove criminals from their platforms. For example, Meta's Mark Zuckerberg discussed using AI to identify explicit content. While these are commendable steps, they are no substitute for criminal prosecution.

An online predator who is kicked off Facebook will create another account, use a different platform, or approach children in-person. Law enforcement must have the information necessary to investigate, arrest, and prosecute these individuals to halt their criminal activity and achieve justice for victims.

Ultimately, public safety cannot be placed in the hands of a private company. Law enforcement must have a process for obtaining lawful access to encrypted data.

III. Legislative Solutions

During the hearing, lawmakers raised various legislative proposals, including the Cooper Davis Act, the EARN IT Act, the SHIELD Act, the REPORT Act, and the Project Safe Childhood Act. ***NAAUSA supports each of these bills.*** Still, these bills are just a band aid for a problem that requires a comprehensive solution that requires companies to provide law enforcement access to encrypted data.

The Communications Assistance for Law Enforcement Act (CALEA) may serve as a potential model for this more comprehensive legislation. CALEA requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that they have the necessary capabilities to comply with legal requests for information.

Meta has characterized this proposal as allowing for "backdoors" or "exceptional access" for law enforcement. Meta claims these proposals would "weaken[] the security of [end-to-end encryption] systems, and... inevitably be discovered and sought to be exploited by malicious actors on a much larger scale."

First, Meta is incorrect that the proposal would weaken the security of encrypted systems. To the contrary, end-to-end encrypted systems that lack law enforcement access are the danger.

As Discord CEO Citron remarked, end-to-end encrypted systems undermine both company and law enforcement efforts to identify and remove bad actors. It is therefore no surprise that every big tech company that has pursued end-to-end encryption has dramatically decreased their assistance with law enforcement.[11]

Considering the rapid increase in online crime and exploitation, end-to-end encryption without law enforcement access will only accelerate this pace.

[10] Id.
[11] Tech companies push back against lawmakers' demands for encryption backdoors (iapp.org)

Second, malicious actors will work hard to hack into systems–no matter how well encrypted–regardless of law enforcement access.

Take the example of Apple. In 2014, Apple began encrypting their devices, preventing federal law enforcement from obtaining full access to data on the devices.[12] Following the San Bernardino terror attack, Apple blocked the FBI from accessing data on the terrorist's device.[13] As a result, the FBI contracted with a company to access the device without Apple's assistance, likely by exploiting a vulnerability that Apple had either not yet identified or patched.[14]

The FBI had no legal obligation to disclose this vulnerability to Apple.[15] And since a private company accessed the information, there is no guarantee it would not expose this vulnerability to an entity other than the U.S. government.[16]

Thus, Apple's choice to lock out law enforcement achieved none of the company's goals: law enforcement still gained access (albeit in a much longer and more costly manner) and Apple's systems were still exposed to an unknown vulnerability.

As this example illustrates, when companies refuse to provide law enforcement access to encrypted data, it reduces the company's control over the "backdoor," diminishes consumer privacy in the long run, and costs law enforcement critical time in high-risk situations.

IV. Conclusion

The safety of children, and indeed all Americans, is at critical risk due to the widespread use of online platforms by criminal actors. As big tech companies move toward end-to-end encryption as the new default, it seriously undermines law enforcement efforts to combat this risk. For these reasons, we urge Congress to take immediate action to ensure law enforcement has lawful access to encrypted data.

Thank you for considering NAAUSA's perspective. Please contact NAAUSA's Washington Representative Natalia Castro (ncastro@shawbransford.com) if you have any additional questions.

Sincerely,

Steven Wasserman
NAAUSA President

[12] Opinion | Why Apple's Stand Against the F.B.I. Hurts Its Own Customers - The New York Times (nytimes.com)
[13] Id.
[14] Id.
[15] Id.
[16] Id.