

ONE HUNDRED SEVENTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

March 16, 2022

Mr. Mike Duffey
Assistant Special Agent in Charge
Florida Department of Law Enforcement
2331 Phillips Road
Tallahassee, FL 32308

Dear Mr. Duffey:

Thank you for appearing before the Subcommittee on Consumer Protection and Commerce on Tuesday, March 1, 2022, at the hearing entitled “Holding Big Tech Accountable: Legislation to Protect Online Users.” I appreciate the time and effort you gave as a witness before the Committee on Energy and Commerce.

Pursuant to Rule 3 of the Committee on Energy and Commerce, members are permitted to submit additional questions to the witnesses for their responses, which will be included in the hearing record. Attached are questions directed to you from certain members of the Committee. In preparing your answers to these questions, please address your response to the member who has submitted the questions in the space provided.

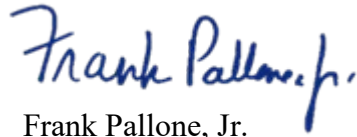
To facilitate the printing of the hearing record, please submit your responses to these questions no later than the close of business on Wednesday, March 30, 2022. As previously noted, this transmittal letter and your responses, as well as the responses from the other witnesses appearing at the hearing, will all be included in the hearing record. Your written responses should be transmitted by e-mail in the Word document provided to Ed Kaczmariski, Policy Analyst, at ed.kaczmariski@mail.house.gov. To help in maintaining the proper format for hearing records, please use the document provided to complete your responses.

Mr. Mike Duffey

Page 2

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Ed Kaczmariski with the Committee staff at (202) 225-2927.

Sincerely,

A handwritten signature in blue ink that reads "Frank Pallone, Jr." in a cursive style.

Frank Pallone, Jr.
Chairman

Attachment

cc: The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy and Commerce

The Honorable Jan Schakowsky
Chair
Subcommittee on Consumer Protection and Commerce

The Honorable Gus Bilirakis
Ranking Member
Subcommittee on Consumer Protection and Commerce

Attachment—Additional Questions for the Record

**Subcommittee on Consumer Protection and Commerce
Hearing on
“Holding Big Tech Accountable: Legislation to Protect Online Users”
March 1, 2022**

Mr. Mike Duffey, Special Agent Supervisor, Florida Department of Law Enforcement

The Honorable Anna Eshoo (D-CA)

1. Your testimony identified tech companies’ data retention practices as an inhibitor of investigations into cases involving child sex abuse materials (CSAM).
 - a. Federal law requires companies reporting to NCMEC’s CyberTipline to retain data for 90 days after a submission (18 U.S.C. §2258A(h)(1)). Would you support an extended retention requirement of 180 days?

RESPONSE: Representative Eshoo- I would support the extension to 180 days. In some instances, information or leads are reported to law enforcement beyond the 90 day period, which leaves law enforcement with no way to obtain additional information to initiate or further an investigation.

- b. The *Invest in Child Safety Act* is my bipartisan and bicameral legislation that extends the CyberTipline data retention requirement to 180 days and also directs \$5 billion in mandatory funding to investigate and target individuals who create and share CSAM, including funding for additional personnel in federal, state, and local law enforcement agencies, along with NCMEC, dedicated to combating CSAM. Would this bill aid your efforts to combat CSAM and do you think Congress should pass this legislation?

RESPONSE: Representative Eshoo- I fully support the “Invest in Child Safety Act”. This Act will allow for all entities involved to expand their growing efforts to protect children and allow law enforcement to add expertise to combat CSAM. This would help as we continue to struggle to keep up with today’s technology and how its used to produce, self-produce and distribute CSAM on these platforms.

Improvements to data retention and additional funding are not a complete solution, however. There are companies who by the nature of their network architecture won’t be able report CSAM as it won’t be visible to them. The latest publicly reported numbers from NCMEC reveal a significant disparity in reporting based on the design decisions made by individual companies. For

example, Apple reported only 160 instances while Facebook reported 22,118,952 instances. If companies are permitted to intentionally blind themselves to CSAM on their networks, increased retention periods and more funding will do law enforcement only limited good.

2. You testified that encrypted messaging inhibits investigations. Please answer the following questions regarding your agency's investigations in the last 12 months (or for another similar time period for which your agency collects such data) that were inhibited due to encrypted messaging:

a. How often did your agency access or request metadata associated with encrypted messaging related to crimes from technology companies, wireless providers, or other companies?

RESPONSE: Representative Eshoo- We request this information as the specific case dictates. We are aware of the various platforms that are already engaging in end-to-end encryption and as such we try to determine if the potential metadata retained is of value to the case. In some cases, suspects use virtual private networks (VPNs) to further hide their internet protocol address which often results in another roadblock in an investigation. The reality is that metadata, while useful in many cases, is not a substitute for content for several reasons. First, it is not always available; for example, if investigators are seeking evidentiary conversations on an encrypted chat platform, even where metadata is available from the provider in some cases, if the evidence is in transit on the data side of the device off the carrier's network (i.e. on public or private wifi) it may not be reflected in what companies provide in response to our legal demands. Second, metadata itself is not an evidentiary substitute for content. Criminal prosecutions require proof of a subject's mental state, for example, and metadata by itself cannot easily be used to prove motive or malice. Finally, metadata isn't an effective substitute for content even if prosecution is a secondary consideration to mitigation of violence. If a group of individuals is plotting to carry out some kind of violent behavior, a pattern of communication that we might glean from metadata won't reveal their targets, methods, or indeed the planned time and date of their intended attack, which makes it less useful from a violence prevention standpoint.

b. What portion of these requests are informal and what portion involve formal legal processes (e.g., subpoenas)?

RESPONSE: Representative Eshoo- All of our requests to Electronic Service Providers (ESP) and Internet Service Providers (ISP) are formal processes that often start with data preservation requests, which then lead to additional formal legal process for content and other data possessed by the platforms. Our requests for this information are often time-intensive. To obtain content we must get a court order and search warrants as required by Federal law.

- c. How often did companies comply with these (i) informal requests and (ii) formal requests?

RESPONSE: Representative Eshoo- Generally all formal legal requests are responded to by the various companies. The issue is what data they retain as a matter of business practice; some types of data that would be helpful in an investigation is not retained, and this varies from platform to platform. With no regulatory framework mandating the retention of specific types of data, there are inconsistencies in what our legal demands will produce. There are also instances where data exists, but some platforms don't have the ability to extract this data in a timely manner because the companies have not built tools to extract the data requested during a specific time period.

- d. How many cases was your agency ultimately unable to solve because of encrypted messaging?

RESPONSE: Representative Eshoo- This varies depending on the crime type and platform type, as the most popular messaging apps and platforms have only talked about implementing end-to-end encryption for messaging. If and when they implement encrypted messaging, it will turn successful cases into unsuccessful ones and will allow those preying upon our children to operate with the full protection of encryption. We see encrypted messaging platforms being used routinely in illegal narcotics cases since traffickers believe their activities are more effectively protected.

In some instances, law enforcement has decided to not issue legal process in the first place because they know the platform deploys end-to-end encryption, which would likely result in no information being provided. As a practical matter, law enforcement does not generate legal demands that we know are futile. We are too busy with cases to spend time trying to access evidence that we know companies cannot produce. If a particular platform or technology is known to be inaccessible, investigators will explore other avenues or, if they hit a dead end, other cases. Criminal investigations are often too complex and nuanced to attribute their outcome to one factor like encryption. In many cases where a subject is still identified and prosecuted, the case takes longer to make and requires more effort. Those are law enforcement resources that could be going to something else...working through a cybertip backlog, for example. That might not be a case law enforcement was unable to solve, but it was certainly a significant negative impact on public safety caused by warrant-proof encryption.

3. Please answer the following questions for your agency's investigations in the last 12 months (or for another similar time period for which your agency collects such data) that involved accessing *un*encrypted messages:

- a. How often does your agency access or attempt to access unencrypted messages?

RESPONSE: Representative Eshoo- We regularly serve legal process to Internet Service Providers and Electronic Service Providers for data they retain. This data is often returned to law enforcement in a format that is determined by each company – responses do not come in a standard format. As a result, law enforcement then must use various analytical tools to review and make sense of the data to determine if it is relevant to the legal process. This often requires a third-party paid service, and these paid services are another cost that our agencies must bear to ensure we can make the most of the evidence we are able to obtain.

- b. What portion of these unencrypted messages does your agency access directly (i.e., from an unlocked phone) and what portion does your agency access by requesting messages from a company?

RESPONSE: Representative Eshoo- It ends up being both – examining information from an unlocked device that was obtained using extraction tools, and also serving legal process on the platform for this data. With today’s users being able to delete messages from a device after messages are sent, and users being able to send messages that disappear after they are read, it is important that law enforcement examine both sets of data as individuals and platforms can choose to remove content. In some instances, this data might have been deleted on the recipient’s device but not deleted from the platform’s cloud or on the platform’s site.

Since February of 2021, FDLE has documented 119 locked mobile devices that have been part of criminal investigations, but the contents of which we were unable to access. These devices were involved in all types of crimes. The 119 devices is only a FDLE snapshot and does not account for all of Florida law enforcement.

- c. What portion of requests to companies are informal and what portion involve formal legal processes (e.g., subpoenas)?

RESPONSE: Representative Eshoo- All of our requests to Electronic Service Providers (ESP) and Internet Service Providers (ISP) are formal processes that often start with data preservation requests, which then leads to additional formal legal process for content and other data possessed by the platforms. If the subject’s mobile device that is part of the investigation is locked, agencies must purchase costly third party tools to ensure data on the device is available to identify additional details related to the crime.

- d. How often did companies comply with these (i) informal requests and (ii) formal requests?

RESPONSE: Representative Eshoo- Generally all formal legal requests are responded to by the various companies. The issue is what data they retain or as a matter of business practice; some types of data that would be helpful in an investigation are not retained, and that varies by platform. With no regulatory framework mandating the retention of specific types of data, there are inconsistencies in what our legal demands will produce. There are also instances where data exists, but some platforms don't have the ability to extract this data in a timely manner because the companies have not built tools to extract the data requested during a specific time period.



2021 CyberTipline Reports by Electronic Service Providers (ESP)

NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children, including child sexual abuse material, child sex trafficking and online enticement. In 2021, the CyberTipline received more than 29.3 million reports. 29.1 million of these reports were from Electronic Service Providers that report instances of apparent child sexual abuse material that they become aware of on their systems.

Higher numbers of reports can be indicative of a variety of things including larger numbers of users on a platform or how robust an ESP's efforts are to identify and remove abusive content. NCMEC applauds ESPs that make identifying and reporting this content a priority and encourages all companies to increase their reporting to NCMEC. These reports are critical to helping remove children from harmful situations and to stopping further victimization.

The following is a breakdown of reports by electronic service providers.

ESP	Number of Reports
4chan	973
4shared	75
7web	1,908
Absolute Software Corporation	3
Adobe Systems Incorporated	1,066
Affinity Apps	869
Afilias USA	203
Airbnb	62
Airtime Media	95
Alpha Exploration Co (Clubhouse)	620
Amazon	99
Amazon Games	4
Amazon Photos	27,101
Amino Apps	75
animebw	16
Apple	160

ESP	Number of Reports
Apricot Digitals	1
Arctic Wolf Networks, Inc.	3
Ariemgroup Limited	32
Ask.fm	117
Asurion Corporation	2
AT&T WorldNet Service	1
Badoo	475
Bark Technologies Inc	282
BigBang Media	225
Blizzard Entertainment (World of Warcraft)	4
Blue Vision	43
Box	2,599
Bublup	13
Canva	1
Care.com	2
Chatango LLC	2
Checkstep	127
Classmates Online	1
Cloudflare	12,932
Comcast Cable Communications	8
Cyveillance	5
deviantART	6
Digital Ocean	200
Discord	29,606
Dreamstime.com	2
Dropbox	48,371
Easynews/Newshosting/Usenetserver	21
EasyOnlineSolutions/MojoHost/ North Tone/Hosthead	41
Ebay	19
Electronic Arts	7
Ello.co	4
Endurance International Group	103
Enom	56
Etsy	6
Facebook	22,118,952
Fenix International Limited	2,984

ESP	Number of Reports
FotoLoce	9
FreeDNS.Afraid.org	3
Gaggle	4,656
Get Together (IRL)	1
GF Networks	12
Giphy	229
GitHub	4
Globtech	4,078
GLU MOBILE	2
GoDaddy	32
GoFundMe	1
GoGuardian	21
Google	875,783
Grindr	10,671
Gumroad	2
Hacker Factor	386
Hewlett Packard Enterprise	5
Hinge.co	6
Hosting Services Inc/Midphase/ WestHost/Autica/VPS	33
HowlogicKFT	3
Imagebam/Flixya Entertainment/Videobam	54,742
Imgur	47,274
IMVU	10
Indeed	2
InfraWeb Solution Limited	7
INHOPE	130,723
Instagram	3,393,654
Internap Corporation (INAP)	15
Internet Archive	188
Interspace Technologies (Byte)	11
Intrado Interactive Services Corporation	184
JMS Internet	1
JNJ Mobile (MocoSpace)	33
Joyo Technology Pte	1
Kaleton Web S.R.O	1
KnownHost/PrivateSystems Networks	1

ESP	Number of Reports
Lain.la	2
LBRY INC	2
LegitScript	1
LEGO System	37
Life on Air (Houseparty)	8,575
Linden Lab (SecondLife)	30
LinkedIn	110
Linode	28
Luftgescheft	5,270
Marbore Web Solutions Limited	4
Marinus Analytics (Traffic Jam)	9
Match Group	158
Medal.tv	26
MediaFire	3,506
MediaLab (Kik)	33,619
Medium	113
MeetMe	2,930
MeWe	1,444
MG Freesites	16
MG Freesites (Pornhub)	9,029
MG Freesites (Redtube)	21
MG Freesites (Tube8)	6
MG Freesites (Youporn)	31
Microsoft	78,603
Microsoft - Xbox	170
MMGuardian	54
Momentive	3
motherless	3,110
Movie Star Planet	5
Mozilla Corporation	2
Multi Media/Zmedianow/Chaturbate	532
Name.com	1
NameCheap	5
National Center on Sexual Exploitation	14
NEOSOLUT WEB SERVICES	3
Nexeon Technologies	8
NextDoor	2

ESP	Number of Reports
Niteflirt/Phrendly.com/Platphorm	22
NorfexHoldingsLimited	7
Northlock Holdings Limited	2
Notion Labs	1
Novi	1
OfferUp	1
Okcupid	178
Omegle	46,924
Orbiseen s.r.o	2
Outschool	1
OVH US	25
Padlet/Wallwisher/Cloudfront	235
Patook	2
Patreon	37
PayPal	970
People Media	1
Photobucket	10
PicsArt	316
Pinger	2
Pinterest	2,283
PocketStars	1
Pokemon	2
Porkbun	1
PORTICATO MEDIA	13
ProBoards	5
Public Interest Registry	183
Quora	25
RealNetworks	4
Redbubble	41
Reddit	10,059
Redgifs	87
Reflected Networks	124
RingCentral	1
Roblox	4,684
Scratch Foundation	20
Scruff App (Perry Street Software)	19
sendvid	703

ESP	Number of Reports
SimilarWorlds	94
Skout	1,203
Slack Technologies	1,263
SmugMug-Flickr	1,169
Smule	2
Snapchat	512,522
Sniffies	9
Softlayer	1
Sohosolutions	2
Sony Interactive Entertainment	2,071
Spotify USA	258
Squarespace	1
StackPath/Highwinds	4
Stanford Internet Observatory	1
StarNow	1
Stelivo	2,034
Stolichnaq	29
Streamable	90
Streamate	16
Stripe	1
Sykes	2
SynaptiCAD	31
Synchronoss Technologies	3,472
Tagged	5,504
Take-Two Interactive Software	3
TECH MEDIALAND KFT	1
The Walt Disney Company	1
Thorn	114
ThumbSnap	308
Thumbtack	1
TikTok	154,618
Tinder	3,642
Toontown Rewritten	12
Tropical Sun (Clips4Sale)	2
Tsu	18
Tumblr	4,511
Twitch	6,629

ESP	Number of Reports
Twitter	86,666
Uncharted Software	18
Various/FriendFinder/Tangotime	26
Veoh Networks	1
VeriSign	341
Verizon Online	50
Verizon Wireless	5
Vero Labs	177
Vimeo	360
Vistaprint	2
Visual Supply Company	34
Voice	1
Vokal (First Media)	130
Web.com/Network Solutions/ Register/NameBargain	3
Weebly	4
WhatsApp	1,372,696
Whisper	1
Wickr	15
Wikimedia Foundation	8
Wildlife Studios	84
WildWorks (AnimalJam)	8
Wink	108
Wixpress (Wix)	1
WordPress.com (Automattic)	310
x-up.ws	636
Yahoo!	5,485
Younow	1,001
Yubo	885
ZeroFox	1
Zoom Video Communications	548
Zvelo	1
Total:	29,157,083