FILED UNDER SEAL

EXHIBIT 16

Message

From: Naomi Gleit [/O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 6/24/2019 5:25:54 PM
To: [redacted] [[redacted]@fb.com]
Subject: FW: Prereads for 6/24 NCMEC Meeting and Ashton Kutcher/Thorn Call
Attachments: Briefing E2E Meeting w_Co-Founder of Thorn Ashton Kutcher (External).pdf; MZ Briefing NCMEC (External).pdf; On encryption_ Law Enforcement _ Child Safety messaging.pdf

Can u print all

From: Antigone Davis <[redacted]@fb.com>
Date: Sunday, June 23, 2019 at 4:21 PM
To: Mark Zuckerberg <[redacted]@fb.com>
Cc: Naomi Gleit <[redacted]@fb.com>, Guy Rosen <[redacted]@fb.com>, Kevin Martin <[redacted]@fb.com>, Joel Kaplan <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: Prereads for 6/24 NCMEC Meeting and Ashton Kutcher/Thorn Call

Hi Mark,

I have attached pre-reads for you meeting tomorrow afternoon with NCMEC and your call with Ashton Kutcher. I also have attached a doc laying out our current public messaging on encryption.

NCMEC Preread: "MZ Briefing NCMEC (External)"
Kutcher/Thorn Preread: "Briefing E2E Meeting w/Co-Founder of Thorn Ashton Kutcher (External)"
E2E Messaging Doc: "On Encryption: Law Enforcement / Child Safety Messaging"

We have a 3:30 pm prep meeting tomorrow. If you have any questions ahead of that, I am available until 9:45 pm ET at which point I board a plane.

Thank you very much for doing this meeting,
Antigone

On Encryption: Law Enforcement / Child Safety Messaging

Proactive *(supporting points that provide added value to the discussion)*

- **Our vision on messaging privacy is driven by:**
  - **our commitment to give users the ability to control the security and privacy of their own communications;**
  - **market forces** that emphasize users' demand for secure, private services.
    - This is where technology is headed.
    - Facebook continues to face pressure from many governments, including in the US, to increase users' control of their data and ensure the security and privacy of their data.
- **We're using this moment in time to evaluate how we approach safety:**
  - We are re-examining our understanding of different harms that exist on our platforms - from high volume activity, low impact activity (like spam), to medium volume, (child sexual abuse meme imagery distribution) to low volume, high impact (like child sex abuse) looking at all the signals we have around these harms;
  - **Our teams will be working to understand alternative methods to stop these harms and keep users safe.**
- **We are exploring what more we can do,** building on our existing strong work on Facebook and Instagram, and our learnings from WhatsAp.
- **The town square vs living room dynamic is one we're using, to help formulate our thinking;**
  - Facebook and Instagram help people connect with friends, communities, and interests in the digital equivalent of a town square. Increasingly people also want to connect privately in the digital equivalent of the living room.
    - this dynamic is helping us think about what users expect us to do on safety in the different digital environments;
- **We are looking at digital-spaces-specific harms - town square or living room.**
  - we know there is a specific risk to minors of being identified in the 'town square', then taken into a 'living room' by individuals wishing to harm them;
- **We want to work with you on:**
  - **Prevention**
    - reducing the ability of bad actors to discover victims / other bad actors
    - reducing the ability for bad actors to contact victims / other bad actors
    - Up-selling education to bad actors and victims at the point of contact or discovery
  - **Behavioral detection and enforcement**
    - Detecting and enforcing against inauthentic and malicious distribution
    - Detecting and enforcing against victim targeting
    - Detecting and enforcing against bad actors coordinating / building networks
  - **User reports**
    - Promoting reporting and improving actioning of user reports
- **We would like to have follow up meetings** focused on specific harm areas (such as regional behaviours on distribution of images of child sexual exploitation, different predator and victim profiles), and what specific measures for prevention and detection looks like, on and off our platform.
  - **I know you have already started these conversations with our team**

- **I would like us to set up a regular exchange of expertise and views.**

- **We know prevention and detection is easier for some harms than others;**
  - *We will never find all of the potential harm we do today on Messenger when our security systems can see the messages themselves;*
    - *We will invest in and work to improve our ability to identify and stop bad actors on Messaging by detecting patterns of activity or through other means, even when we can't see the content of the messages.*
    - *We know we can also do more to prevent and detect harm on [the town square] Facebook and Instagram, where content will still be available.*
- We'd like your thinking on our framing: are we starting from the right points?
  - Town hall and living room (and movement between the two);
  - Prevention, detection and seeking assistance
- **We are developing a safety engagement plan so we can seek global safety advocates views and input.**
  - We would appreciate your input in this.
  - Who else should we be talking to?
- Our door is always open for further conversation.

Reactive — what does this person or group care about or what do we expect them to ask *(set responses for questions / comments (as needed))*

You already committed to e2e without knowing what safety you can build

- I believe a privacy-focused communications platform will become even more important than today's open platforms.
- Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks.
- End-to-end encryption is the next stage of this.
- We continue to be committed to preventing abuse of our platform, particularly sexual abuse of children.
- Now is a time to re-examine how we prevent and detect harms, using the best innovations in technology.

We all know the extent of the problem - you must hold onto the content based work for CSE; you must have a carve out for CSE. Facebook accounts for the vast majority of cybertips send to NCMEC.

- We don't think it is technically possible to do any carve outs within a privacy focused model.
- We continue to be committed to preventing abuse of our platform, particularly sexual abuse of children.
- We are re-examining our understanding of different CSE harms that exist on our platforms - from child sexual abuse meme imagery distribution and child sexual abuse and grooming. We want to look at all of these in detail to understand all the signals we have around these harms;
- Our teams will be working to understand alternative methods to stop these harms and keep users safe (e.g., upstream prevention, behavioral detection, user reporting/remediation) in the future..
  - <u>We want to work with you on these;</u>

- Now is a time to re-examine how we prevent and detect these harms, using the best innovations in technology.

You are locking kids in an unsafe place (even if you build protections) and locking us out.

- We are re-examining our understanding of child sexual abuse and grooming.
    - We want to look at this in detail to understand all the signals we have;
- Our teams will be working to understand alternative methods to keep children safe (e.g., upstream prevention, behavioral detection, user reporting/remediation) in the future..
    - We want to work with you on these;
- Now is a time to re-examine how we prevent and detect these harms, using the best innovations in technology.

How will you measure the effectiveness of the safety measures you develop?

- We believe there are signals that we can use, including user reporting, closed and blocked accounts, user surveys etc.
- We have been exploring this within WhatsApp, but still have much work to do. It is important.
    - We want to work with you on these;

Users want privacy, but not at the expense of child safety from sexual exploitation. What proof do you have users want end-to-end encryption?

- We know people can be confident what they say to each other stays secure and their messages and content won't stick around forever. They also want to feel safe in the way they do in the real world.
    - This is what we are working towards.

After we collaborate, if we don't think you can build true safety into this platform will you abandon e2e messaging?

- We will do everything we can to keep them safe on our services within the limits of what's possible in an encrypted service

Industry is not moving toward more encrypted services: Facebook is moving industry not the other way around.

- I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever.

You understand that you will degrade or interfere with law enforcement and safety capabilities?

- That is certainly not our intent
- We feel the change is necessary for the people who use our services.
- We're committed to continuing to work with law enforcement and providing the assistance we can consistent with this important change.

Are you doing this to stop us getting data?

- No, we're doing this to increase the privacy and security of our messaging services. It's what we as a company believe in and what our users want.
- We want to be clear that it is not the intent of our product and service changes to diminish or adversely affect our ability to work with law enforcement and national security authorities

- We will, of course, continue to comply with all applicable laws, data protection laws and compelled assistance laws, to the best of our ability

Will you do client side scanning?

- In order to accomplish our privacy-focused vision, the company will standardize on being best-in-class for privacy, not looking at content and minimizing what we log (similar to where WhatsApp is today), and explore how to do our integrity work within this strict privacy model
- For our Integrity teams, this means doing everything we can to keep users safe, within the limits of what's possible in a private, encrypted messaging surface

Will you be building exceptional access provisions:

- No. An exceptional access capability would be fundamentally at odds with the customer privacy and security e-2-e encryption is intended to achieve.
- [*If asked only*] We understand current laws to protect technology companies' freedom to create, design and build products based on their principles and consumers' desires. We do not understand there to be any legal obstacle to building a secure, e-2-e encrypted service. In fact, several already exist.

Will you work with other companies?

- We'll also need to work together with other platforms to make sure that as an industry we get this right. The more we can create a common approach, the better.

Can you delay product implementation?

- I understand the request. This change is driven by principled and business considerations and is assessed as essential to Facebook. I will certainly make Mark and our leadership aware of the request, but a great deal of thought preceded Mark's announcement and — just to be frank with you — I don't expect that they will be receptive to a request for delay.

Can we have a technical meeting to help you build our system in a way that allows exceptional access?

- We need the freedom to design and build our product to reflect these values and meet these business objectives.
- While we welcome the opportunity to continue open, constructive discussions with you and hope to continue to work cooperatively with you to combat criminal abuse of our services, I'm sure you understand that we cannot include the USG in the design and build of our service.
- We value and need to protect our independence and freedom.
- We don't understand there to be any US law that requires providers to involve government in designing and building their online services. To the contrary, we understand US law to recognize providers' prerogative to design and build their own services. [**Note –** even in the far more heavily regulated traditional telephony space, CALEA, the statute that imposes obligations on telephone companies expressly recognizes the right of those companies to design and build their own services. See below.]
    - We don't understand there to be any precedent for government involvement in the design and build of online services.
- Any suggestion that the US had been involved in designing and building our system would destroy our business.
- Any suggestion that was an appropriate role for a government to play would give license to repressive regimes we have so far held successfully at bay to demand the same to the detriment of our users privacy and personal safety.

What are your privacy focused principles?

- **Private interactions**. People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.
- **Encryption.** People's private communications should be secure. End-to-end encryption prevents anyone -- including us -- from seeing what people share on our services.
- **Reducing Permanence**. People should be comfortable being themselves, and should not have to worry about what they share coming back to hurt them later. So we won't keep messages or stories around for longer than necessary to deliver the service or longer than people want them.
- **Safety.** People should expect that we will do everything we can to keep them safe on our services within the limits of what's possible in an encrypted service.
- **Interoperability.** People should be able to use any of our apps to reach their friends, and they should be able to communicate across networks easily and securely.
- **Secure data storage.** People should expect that we won't store sensitive data in countries with weak records on human rights like privacy and freedom of expression in order to protect data from being improperly accessed.

APPENDIX I: Facebook child sexual exploitation stats and background

- Service Providers such as Facebook are legally obligated to make reports to the National Center for Missing and Exploited Children (NCMEC) when they become aware of child exploitation imagery (CEI) and related offenses[1]. Those reports are called CyberTips. One CyberTip could have many individual pieces of content in it.

- In 2018, NCMEC had a total **18.4M** CyberTip reports. Facebook & Instagram made up **17,366,320** of those reports. (Or **94.3%** of NCMEC's total volume). WhatsApp submitted approximately 13.8K reports.

    - Feedback is hard to come by. Out of our 17M reports, we received feedback from law enforcement through NCMEC for about 27,000 reports. Most have limited feedback such as "on-going investigation" or "closed" without more. In limited cases we hear about child rescues and arrests.

- Year to date 2019, we have submitted 4.17M cybertips. These are made up by FB Msgr 2.87M **(69%)**, FB Blue 971 K (23%), IG 316 K (7.5%), WA 19.6 K (0.5%).

    - Of the 2.87M Messenger cybertips, 531k (18.5%) hit the egregious industry standards (A1 - B2) on child sexual exploitation (compared to 82k on FB Blue).

[1] The type of offenses that we report per the statute include contact offenses, possession, distribution, production, solicitation or advertisement of CEI and planned or imminent violations, including Inappropriate Interactions with Children ("IIC" or formerly, grooming).

- 1.87M (65%) was severe memes (content that is depicting child sexual abuse but is shared without predatory intent because it is communicating some type of poor humor (majority of reports), or shared in outrage to raise awareness of the issue.)

- **High Priority cases** - where we believe a child is in immediate danger (e.g., abuse at the hands of someone in a position of trust, apparent contact offense, imminent meeting, sextortion), we submit manual report providing additional information following an investigation and escalate to NCMEC
  - Total: 2017 - 607; 2018 - 946; 2019 YTD - 849
- **Arrests/Victims Rescued**:
  - Total Arrests (that we are aware of*): 2017 - 106; 2018 - 86; 2019 YTD - 56
  - Total Victims Rescued (that we are aware of): Jan - Apr 2019 - 110
- 2019 (YTD) we have disabled 831,825 accounts for sharing Child Exploitation Imagery and 1,804,565 accounts for inappropriate interactions with children. We have checkpointed 4,372,699 accounts for sharing Child Exploitation Imagery (meme/ minor self generated).
- **Country-specific information**: Due to a variety of factors, we are unable to reliably trace back exactly which countries correspond to the users in each CyberTip sent to NCMEC. However, by approximating based on hits in our CEI banks, for 2018:
  - Top 5 countries for NCMEC reports: India, Indonesia, Iraq, Pakistan, Bangladesh, representing ~40% of reports
  - Top 5 countries for A1-B2 content: Iraq, Vietnam, India, Algeria, Pakistan, representing ~50% of hits
  - Top 5 countries for potential meme content:
    - India, Indonesia, Pakistan, Bangladesh, Philippines → ~44% of hits
    - Next 5: Vietnam, Mexico, USA, Egypt, Iraq
- **Why are we 94.3%?** We scan more content and for a broader range of images. For example we understand that Google only scan gmail for A1 level images (pre-pubescent minors involved in sexual activity). Apple only scan the photoreel.
- Existing NCMEC FB Special Projects Collaboration:
  - We're funding a rebuild of the CyberTip downloader tool — which will enable law enforcement to more easily review and action the reports sent to them. (Multi-million dollar effort)
  - Project Nix: NCMEC provided us with 1.5M images to help train a child exploitation image classifier.

APPENDIX II: Public NCMEC case examples

Sample case in Denmark - Operation Umbrella[1]*:*

- In 2017 Facebook reported to NCMEC the distribution of videos via **Facebook Messenger**[2] depicting a Danish boy and girl who were engaged in sexual activity.
- NCMEC forwarded the case to Denmark via Europol.
- Over 1000 people had distributed the videos to one or more people via Facebook Messenger and were charged for distribution of child pornography.
- This operation, still ongoing, is the single **largest operation ever** against child sexual abuse in Denmark.

Sample case in Romania[3]

- Romanian police received in 2016 a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
- The investigation revealed that a mother had been abusing her **9 year old daughter** for more than a year and sent the material generated in the sexual abuse to her boyfriend (not the father of the girl) in England.
- The mother was arrested and **her daughter was rescued**.

Sample case in the US - Dabbs Postma case[4]*:*

- US law enforcement received in 2017 a report from NCMEC submitted by Facebook alerting of the exchange between two users via **Facebook Messenger** between Aug. 4 and Oct. 25 of **hundreds of photos and videos** containing child sexual abuse.
- The report led to a criminal investigation in which Postma's home was searched. The police found a video showing him performing sex acts on **a young girl**.
- Postma admitted to producing child pornography and having a sexual relationship with the girl, who was safeguarded.

---

[1] This case was also included in the 2018 Internet Organised Crime Threat Assessment, p. 32, Europol.

[2] The case was also reported in the media (in English).

[3] The case was reported in the media, see here and here.

[4] The case was reported in the press, see here.

APPENDIX III: WePROTECT Board Meeting Readout

From: Antigone Davis <[redacted]@fb.com>

Date: Thursday, May 30, 2019 at 12:25 AM

To: Nick Clegg <[redacted]@fb.com>, Joel Kaplan <[redacted]@fb.com>, Monika Bickert <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, Chris Sonderby <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, Guy Rosen <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, Will Cathcart <[redacted]@whatsapp.com>, Stan Chudnovsky <[redacted]@fb.com>
Subject: Readout: WePROTECT Board Meeting

As flagged, the WePROTECT Board did raise our plans to move to e2e during today's Board meeting. For those unaware, WePROTECT is an international multi-stakeholder organization to fight child sexual exploitation (CSE) online, founded by former UK Prime Minister Cameron. 82 countries, 21 companies, and 30 NGOs belong. We sit on the board alongside Google and Microsoft.

As expected, the conversation was exceptionally challenging – in part because the Board includes members of government and law enforcement, in part because they represent the entire ecosystem that has been built around a content based approach to fighting CSE online, and in part because they understand the extraordinary growth of online CSE. Below I have listed attendees, key takeaways, key points they made, their responses to our messaging, the hard questions they asked, and some ideas we might want to consider. ***Of those ideas, I'd suggest we do the first "a pre-emptive letter to WePROTECT Board inviting a meeting with senior leadership" ASAP to avoid a public letter from them.***

Attendees: UK Home Office, CEOS of DoJ, Interpol, UK National Crime Agency, United Arab Emirates LE, UNICEF, ECPAT International, Internet Watch Foundation, INHOPE, Global Partnership to End Violence Against Children, UN Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, European Commission's Principal Policy Officer Against Cybercrime, Virtual Global Taskforce, Google, Microsoft, former President and CEO of NCMEC and ICMEC Ernie Allen and former adviser to Cameron Baroness Shields.

Key takeaways:

- They will work with us (half-heartedly) while 1) raising the alarm bells with consumers and the press, 2) publicly demanding that we voluntarily carve out child sexual exploitation (e.g., client side, Hany Farid's PDNA w/in e2e,..) with behind the scenes encouragement to break us up if we don't, and 3) lobbying policymakers to legislate in such a way that we either carve out CSE or face legal liability for violating a duty of care, negligence,...
- We should expect a letter (perhaps public) from the Board (minus industry reps) asking us to reconsider our plans to move to e2e (or something along those lines) and requesting some sort of formal engagement.
- We should expect Ernie Allen to reach out to his considerable network to begin lobbying the company, policymakers, and world leaders.

Note: *It will take them a little while to get these things going and build momentum but not that long as they think we are moving quickly.*

Key points made by WePROTECT members:

- You must hold onto the content based work for CSE; you must have a carve out for CSE.

- Facebook accounts for the vast majority of cybertips (claimed 99%).
- We know the extent of the problem: you are locking kids in an unsafe place (even if you build protections) and locking us out.
- We won't even be able to measure the effectiveness of the safety measures you develop, but we know the extent of the current problem.
- This will be a PR nightmare for FB (gently making clear they will make it so).
- You effectively are undoing ALL the technological progress that has been made in the fight against CSE online, and the entire ecosystem built alongside it over the last 10 years.
- Users want privacy, but not at the expense of child safety from sexual exploitation. We have seen the studies.

Responses to our messaging:

1. Message that industry moving toward more encrypted services met with total disbelief:
    1. WhatsApp owned by Facebook -> Facebook is moving industry not the other way around
        i. and this will provoke more calls to break you up (implication that they would support this approach)
    1. Google noted that they are NOT implementing DOH on Chrome, email not e2e encrypted
    2. Microsoft pointed to all the new content based work they are doing (grooming tool, internal research they are willing to share with WPGA,...)
    3. Claim made that at last week's NCMEC roundtable Apple rep announced it will be launching PhotoDNA in iMessage *(need to verify as no FB reps at the RT remember this announcement).*
    4. Noted that Skype not e2e and LE can access data on Google's cloud services with valid legal process.
2. Message that users want more privacy, ephemerality,... doubted:
    1. Studies show people want privacy but not at the expense of child safety from sexual exploitation
    2. Show us proof that this is what they want
    3. You are doing this because you have a fiduciary duty to make money and this will make you more money
3. Message that we want to collaborate on best safety measures within e2e met with strong skepticism:
    1. Your CEO already committed to e2e without knowing what safety you can build *(we hear you may test/launch e2e as early as Jan, 2019)*
    2. We will engage but we can and should do all that work together anyway and still not encrypt

NOTE: *I emphasized that we were early to adopt PhotoDNA, embraced it fully, built a CEI classifier, built a grooming classifier... because we fundamentally are committed to safety and we will apply the same rigor and commitment to safety here within the bounds of e2e. Still, I barely escaped a total rebuke. Some came very close to questioning the morality of our decision and our CEO (and me) "knowing what we know."*

Hard questions:

1. After we collaborate, if we don't think you can build true safety into this platform will you abandon e2e messaging?
2. What proof do you have users want end-to-end encryption?

Some ideas to consider/recommendations:

- A pre-emptive letter to WePROTECT Board inviting a meeting with senior leadership (e.g., Nick Clegg – though I think they might push for Mark since they were stuck on his post).
- Providing a detailed public outline of our plans for collaboration with a timeline of sorts.
- Facilitating a series of conversations with privacy and safety stakeholders in the same room sooner rather than later.
- Providing some data and hard proof to back any claims about what users want and direction of industry.
- Providing examples of the safety measures we are evaluating, more than the three buckets, examples within the buckets.
- Doing more homework on where other members of industry will land in the public debate.

Please let me know if you have any questions. I will follow up with Lara et al. on next steps.

Thanks,
Antigone