





Facebook, Inc. (FB) Vote Yes: Item #10-Child Sexual Exploitation Online

Annual Meeting May 27, 2020
Contact: Michael Passoff, CEO, Proxy Impact <u>michael@proxyimpact.com</u>

THE PROPOSAL

ITEM 10 RESOLVED CLAUSE: Shareholders request that the Board of Directors issue a report by February 2021 assessing the risk of increased sexual exploitation of children as the Company develops and offers additional privacy tools such as end-to-end encryption. The report should address potential adverse impacts to children (18 years and younger) and to the company's reputation or social license, assess the impact of limits to detection technologies and strategies, and be prepared at reasonable expense and excluding proprietary/confidential information.

SUMMARY

In 2019 there were nearly 17 million reported cases of online child sexual abuse material (CSAM), 94% of which stemmed from Facebook. The growth of CSAM is directly tied to the growth of the internet. Facebook and its platforms, including Messenger, Instagram and WhatsApp account for over six billion monthly internet users. Facebook's plan to apply end-to-end encryption to all its platforms, without first stopping CSAM, could effectively make invisible 70% of CSAM cases—an estimated 12 million instances—that are currently being detected and reported. Governments, law enforcement agencies and child protection organizations have harshly criticized Facebook's planned encryption claiming that it will cloak the actions of child predators and make children more vulnerable to sexual abuse. Pending legislation in Congress could make Facebook legally liable for CSAM. The company is facing increasing regulatory, reputational and legal risk due to this issue. Shareholders believe that the company needs to report on its assessment of the risk of increased sexual exploitation of children as it develops and offers additional privacy tools such as end-to-end encryption.

THE LINK BETWEEN SOCIAL MEDIA AND CHILD SEXUAL ABUSE

In 2019, there were more than 16.8 million reports of online child sexual abuse material (CSAM) which contained 69.1 million CSAM related images and videos. More than 15.8 million reports—or 94%—stem from Facebook and its platforms, including Messenger and Instagram.¹

Reported incidents of child sexual exploitation have increased dramatically from year to year over the past decade from 100,000 CSAM incidents ten years ago to nearly 70 million incidents in 2019. ² The exponential growth of CSAM is tied directly to the growth of the internet and social media. ³ The

¹ https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers

² https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

 $[\]frac{3}{\text{https://web.archive.org/web/20190928174029/https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf}$

link between child abuse and the internet is even more evident given the significant uptick in both social media use globally, pornography website visitations, and noticeable increases in child sex abuse searches by child predators on public search engines during the COVID pandemic.^{4 5 6}

With 180 countries and their school systems sending children home to continue their education on Internet-connected devices, many kids are flocking to social media to connect with friends and strangers during social isolation, as parents struggle with juggling work or lack thereof and risks and stress from the pandemic, leaving many children unsupervised online. Many of those children use WhatsApp and Facebook Messenger to connect, likely increasing the chances that Facebook's many platforms are facilitating the connections between child pedophiles and unsuspecting children.

FACEBOOK'S CENTRAL ROLE

Facebook is the world's largest social media company with 2.49 billon active monthly users. Facebook's other platforms include WhatsApp with 2 billion users, Facebook Messenger with 1.3 billion users, and Instagram topping 1 billion users. These four social media platforms alone account for nearly half of the world's monthly social media use.⁷

As the world's largest social media company and the largest facilitator of reported child sex abuse online—Facebook's actions will, for better or worse, have a major impact on global child safety. The company's current plan to apply end-to-end encryption to all its platforms by the end of 2020 has set off a storm of controversy and criticism. Government agencies, law enforcement, and child protection organizations worldwide claim that it will cloak the actions of child predators, make children more vulnerable, and that millions of CSAM incidents will go unreported. In short, law enforcement won't be able to locate the victims appearing online, nor the perpetrators.

THE IMPACT OF END-TO-END ENCRYPTION ON CSAM

To be clear, neither shareholders nor the above entities are necessarily opposed to encryption, but we believe that Facebook should apply these new technologies in a way that will not pose additional threats to children from sexual grooming (the luring or enticement of children for sexual purposes) or exploitation itself. Everyone recognizes that privacy is important but it should not come at the expense of unleashing a torrent of virtually undetectable child sexual abuse materials on Facebook.

The National Center for Missing and Exploited Children (NCMEC) is the national clearinghouse for CSAM materials in the U.S. According to NCMEC, "Over the past 20 years, we've received more than 55 million reports of child sexual abuse to our CyberTipline - in 2018 alone we received over 18 million reports Tech companies use hashing, PhotoDNA, artificial intelligence, and other technology to recognize online child sexual abuse, remove it, and report it to NCMEC. We make these reports available to law enforcement agencies around the globe. The ability for tech companies to "see" online abuse and report it is often the only way that law enforcement can rescue a child from an abusive situation and identify and arrest an offender." ⁸ NCMEC estimates

2

⁴ https://www.scientificamerican.com/article/the-coronavirus-pandemic-puts-children-at-risk-of-online-sexual-exploitation/

⁵https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5ebc58d038eb072b909874ca/158940 1809129/Impact+of+COVID-19+on+Online+Child+Sexual+Exploitation.pdf

⁶ https://www.hrw.org/news/2020/04/09/covid-19s-devastating-impact-children

⁷ https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

⁸ https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

that If end-to-end encryption is implemented without a solution in place to safeguard children, it could effectively make invisible 70% of CSAM cases—an estimated 12 million instances—that are currently being detected and reported"⁹

FINANCIAL RISK TO FACEBOOK

Regulatory and Legal Risk

In 2018, the U.S. House and Senate, with strong bi-partisan support, passed the SESTA and FOSTA bills. This new legislation made it easier for users of Electronic Service Providers (ESPs) to sue platforms when they knowingly facilitated child sex trafficking and exploitation. At the time, the sex trafficking scandals at Backpage were still making the news, and some in the tech community invested to support the Backpage legal defense. This bill was one of several regulatory salvos thrown at the industry, including Facebook.

It also opened the door for a set of lawsuits that the company now faces. A group of victims have sued Facebook, the first one in Texas courts, over Facebook knowingly allowing posts that sold sex acts with minors on the company platform. The company has attempted to have the suits overturned, to no avail. ¹⁰

Electronic Service Providers—websites, email, social media, and cloud storage—currently are not liable for what users say or do on their platforms. Many ESPs rely on a carve-out intentionally made by legislators in the early booming years of the U.S. Internet which gave them immunity from liability for what others post on their platforms or services, an exemption known as Section 230 of the Communications Decency Act¹¹. Facebook, YouTube, Twitter, and many other user-generated content platforms heavily rely on this exemption for their business model. But as child sex abuse continues to surge on such platforms, it has brought intense regulatory scrutiny and a number of serious discussions by U.S. lawmakers on ways to revoke that exemption from liability for content related to CSAM.

Those discussions most recently led to the introduction of the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act, introduced on March 5 2020.¹² The EARN IT Act takes aim at the Section 230 exemption¹³ and "would carve out an exception to that rule. Companies that don't follow the recommended standards would lose civil liability protections for that type of content. The legislation would also lower the bar for suing those tech firms." ¹⁴

The EARN IT Act is the culmination of multiple efforts by Congress to get the tech industry to find a balance between increased privacy and allowing for law enforcement action. Actions leading up to the EARN IT Act include:

⁹ https://www.justice.gov/opa/press-release/file/1207081/download

¹⁰ https://www.occrp.org/en/daily/12224-us-court-approves-sex-trafficking-lawsuits-against-facebook

¹¹ https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change

https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-hawley-feinstein-introduce-earn-it-act-to-encourage-tech-industry-to-take-online-child-sexual-exploitation-seriously

¹³ http://broadbandbreakfast.com/2020/03/big-tech-must-combat-child-sexual-abuse-material-online-or-lose-section-230-protection-say-senators/

¹⁴ https://www.nytimes.com/2020/03/05/us/child-sexual-abuse-legislation.html

- In August 2019, Senators sent a letter to Facebook about the company's Messenger Kids app, which was designed specifically to only allow kids 12 and under to interact only with approved users. Facebook admitted that, "a design flaw allowed children to circumvent those protections and chat with unapproved strangers." It took Facebook approximately nine months to discover the flaw, and another month before they notified parents.
- In November 2019, Senators from both parties wrote Facebook and 35 other tech companies chastising the industry for its failure to live up to the 2008 Protect Our Children Act and for its current insufficient effort to address this problem. It reminded these companies that "Technology companies have a vital and irreplaceable role in stemming this flood of child exploitation and abuse" and asked them specifically: "What measures have you taken to ensure that steps to improve the privacy and security of users do not undermine efforts to prevent the sharing of CSAM or stifle law enforcement investigations into child exploitation?" ¹⁷
- In December 2019, the Senate Judiciary Committee held a hearing on encryption and public safety that included representatives from Facebook and Apple. Child sexual abuse was repeatedly used as an example for harms that need to be addressed stemming from encrypted communication, and many comments from bipartisan Committee members' threatened legislative action.

Judiciary Chairman Lindsey Graham (R-SC) firmly stated "You will find a way to do this or we are going to do it for you. We are not going to live in a world where a bunch of child abusers can have a safe haven to practice their craft. Period. End of discussion. You are either the solution or you are the problem." Senator Graham latter added, "My advice to you is to get on with it, because this time next year, if we haven't found a way that you can live with, we will impose our will on you." ¹⁸

- Also in December 2019, a bipartisan bill was introduced in both the House and Senate called the END Child Exploitation Act, ¹⁹ which seeks to improve how tech companies can provide law enforcement with information in a timely manner related to evidence of CSAM crimes.
- Three months after the END Child Exploitation Act, the Senate introduced the EARN IT Act. Two months later it followed up with a bill in May 2020 calling for \$5 billion to help law enforcement and NGOs deal with the overwhelming flood of online CSAM.

Lawmakers "have identified child sexual abuse imagery and exploitation on the internet as an urgent problem." This series of CSAM-related Congressional letters, hearings and legislation—all with

¹⁵ https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-query-facebook-on-messenger-kids-design-flaw

https://www.theverge.com/2019/8/28/20837552/facebook-messenger-kids-bug-markey-blumethal-letter

https://www.blumenthal.senate.gov/imo/media/doc/11.18.19%20-%20Google%20-%20CSAM.pdf

¹⁸ https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy

¹⁹ https://anthonygonzalez.house.gov/news/documentsingle.aspx?DocumentID=179

https://www.nytimes.com/2020/05/05/us/child-abuse-

legislation.html?action=click&module=News&pgtype=Homepage

strong bipartisan support-raises the likelihood of regulatory action that could expose Facebook to legal liability in some form that it has not had to face before.

Reputational Risk

Facebook was heavily featured in the 2019 NY Times series 'Exploited' which lent energy and additional momentum to Congressional scrutiny, hearings and legislation that take a dim view of Facebook's actions, and other tech leaders

Media coverage of the regulatory initiatives and law enforcement concerns mentioned above, as well as general coverage of such issues as online CSAM, privacy and encryption has resulted in a substantial amount of international negative media for the company.

A February 2020 letter to Facebook, signed by 126 leading child protection organizations from over a dozen countries, ²¹ also resulted in negative media coverage for the company and further tarnished the company's reputation among the NGO community and their organizations members. ²²

In mid-May, when Facebook announced the first wave of members for its Content Advisory Committee, the press covered the announcement quite negatively, and in some cases with disdain, noting that the group would be debating a single decision for weeks or months while that harmful content continued to be shared globally. Another critique was that while committee members had stellar resumes, none of them had any practical experience with the job at hand—content moderation, content blocking, or other tools or approaches used by the company to assess inappropriate or harmful content. ²³ ²⁴ ²⁵

Clash with Law Enforcement

In October 2019, a letter from U.S. Attorney General William Barr and Homeland Security Chief Kevin McAleenan, as well as law enforcement leaders from the U.K and Australia, asked that "Facebook not proceed with its end-to-end encryption plan without ensuring there will be no reduction in the safety of Facebook users and others." ²⁶

Also in October 2019, the U.S. Department of Justice held a public hearing entitled Lawless Spaces: Warrant-Proof Encryption and its Impact on Child Exploitation Cases, wherein nearly 20 leading Attorneys General, FBI agents, Police Chiefs, Sheriffs and child-protection leaders described the harm that encryption would do to law enforcement efforts to protect kids and arrest child predators. 27 28

²¹ https://www.nspcc.org.uk/globalasse<u>ts/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf</u>

https://timesofindia.indiatimes.com/business/india-business/ngos-working-against-child-sex-abuse-urgefacebook-ceo-mark-zuckerberg-to-rethink-encryption-plans/articleshow/73984126.cms

https://www.washingtonpost.com/opinions/will-facebooks-oversight-board-actually-hold-the-companyaccountable/2020/05/17/e1d46f50-93cd-11ea-9f5e-56d8239bf9ad_story.html

24 https://techcrunch.com/2019/09/21/meet-facebooks-latest-fake/

https://hbr.org/2020/01/can-facebooks-oversight-board-win-peoples-trust

²⁶ https://www.usatoday.com/story/tech/2019/12/10/facebook-william-barr-encryption-coming-messengerinstagram/4391220002/

https://www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitationcases

FBI Director Christopher Wray stated "Most of the tips Facebook currently provides are based on content. With end-to-end encryption, those would dry up. Facebook itself would no longer be able to see the content of its users' accounts," and "Facebook would transform from the main provider of child exploitation tips to a dream-come-true for predators and child pornographers. A platform that allows them to find and connect with kids, and like-minded criminals, with little fear of consequences. A lawless space created not by the American people, or their elected officials, but by the owners of one big company." ^{29 30}

PREVENTIVE OPTIONS

Law enforcement can only do so much and only after these terrible crimes have been committed. Once child abuse images get online and are shared, children are victimized over and over again as images continue to circulate globally for years afterwards. Solutions must be found that can prevent CSAM from ever making it online.

There are a number of practices that Facebook has failed to implement that would have an impact:

- 1. Developing technology—either itself or in partnership with industry peers—that verifies the age of users on its platforms. Though Facebook sets a minimum age of 13 for regular accounts and parental permission for child-targeted accounts like Facebook Messenger Kids, it has consistently been ineffective in enforcing its own policies on age limitations for users.
- 2. Facebook could set a standard that any user under 18 years of age would not be allowed to access encrypted communications, so that at minimum, the accounts of child users could be monitored by Artificial Intelligence (AI) or Machine Learning, for grooming³¹, sextortion,³² and other CSAM-related abuses.
- 3. Live streaming has been a growing tool for sexual exploitation, and Facebook has yet to address how it will identify and block/remove child rape and exploitation happening in real-time. ³³ The likelihood of this technology being used at even higher rates in an encrypted environment alarms child protection advocates.
- 4. While WhatsApp has recently reported that it is now shutting down about 250,000 accounts per month due to child sex exploitation online,³⁴ it is unclear how it is deploying technology to do that and why such strategies would not also apply to other Facebook platforms.
- 5. Facebook could partner with device makers to improve design and functionality to allow for better online safety monitoring, identification of threats to safety, and CSAM at the device level, but there is little evidence that it has sought such innovations.

 $[\]frac{^{28}}{\text{https://www.wpxi.com/news/politics/doj-says-facebooks-encryption-plan-will-hinder-child-sex-crimes-investigations/993718808/}$

https://www.reuters.com/article/us-facebook-security/fbi-director-warns-facebook-could-become-platform-of-child-pornographers-idUSKBN1WJ1NQ

https://sociable.co/social-media/fbi-worries-facebooks-privacy-first-policy-will-be-a-child-predators-dream/
https://www.psychologytoday.com/us/blog/protecting-children-sexual-abuse/201901/what-parents-need-know-about-sexual-grooming

³² https://en.wikipedia.org/wiki/Sextortion

https://www.npr.org/sections/coronavirus-live-updates/2020/04/08/828827926/child-sex-abuse-livestreams-increase-during-coronavirus-lockdowns

³⁴ https://www.livemint.com/technology/apps/circulation-of-child-sexual-abuse-material-still-rampant-on-whatsapp-report-1556089054250.html

Tech experts such as Hany Farid, a professor at the University of California, Berkeley, point out that the technology exists to protect privacy while still allowing to search for CSAM on encrypted data and that this "provides no information about an image's contents, preserving privacy, unless it is a known image of child sexual abuse." There is also the ability to do this search at the point of transmission before it is encrypted. 35

FACEBOOK'S RESPONSE

How has Facebook CEO Mark Zuckerberg responded to all this concern about encryption's potential to put children at more risk?

In March 2019, Zuckerberg posted a blog outlining his privacy-focused vision for social networking in which he stated: "Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion." ³⁶

In October 2019, when addressing an employee question about online child abuse, "Zuckerberg acknowledged that losing access to the content of messages would mean "you're fighting that battle with at least a hand tied behind your back." 37

Recognizing early on that encryption would limit the fight against child abuse, and acknowledging that privacy rights—including those of "people doing bad things"—supersedes the physical safety and rights of children going online, has only fueled the criticism of Facebook further.

Facebook's Opposition Statement

Facebook's opposition statement in its 2020 proxy claims that it has sufficient policies in place, takes proactive measures at reporting and has ongoing relationships with law enforcement and NGOs.

Investor proponents acknowledge, even in the resolution, that the company has been involved with a number of NGOs and initiatives focused on preventing CSAM online, and that it has partnered and invested in technology tools to better identify CSAM and child abuse videos. It has also improved its public reporting on this issue since 2018 in its Community Standards reports. It has brief but clear policies for users prohibiting CSAM on its platforms, as well as age requirements for most of its accounts.

Facebook notes "we fundamentally do not allow content or behavior on our services that puts the safety of children at risk." But shareholders filed the resolution because it has not been enough for Facebook to simply say it prohibits CSAM or harmful content that endangers children.

For starters, it has not stopped countless children under the age of 13 from accessing and posting to its platforms in prohibition of its policies. ^{38 39} In fact, as a company it has faced numerous user data

³⁵ https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/

³⁶ https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

³⁷ https://uk.reuters.com/article/uk-facebook-security-zuckerberg/facebooks-zuckerberg-defends-encryption-despite-child-safety-concerns-idUKKBN1WJ02N

³⁸ https://techcrunch.com/2019/12/03/instagram-age-limit/

privacy complaints and Facebook's success at circumventing the Children's Online Privacy Protection Act (COPPA) is well documented.⁴⁰

The company states that it applies Artificial Intelligence (AI) and Machine Learning in searching for CSAM and we acknowledge that this has increased reporting. But for an issue like CSAM, where someone is being charged with a federal crime of child sexual abuse or the production or sharing of child pornography, it requires human staff or content moderators to verify what AI has flagged.

And even though Facebook has heavily invested in content moderators and AI over the last few years, it has not seemed able to keep pace with the sheer volume of content on its various platforms to be scrutinized, nor with the complexity of so many decisions about content decisions that need to be made under the specific context of the imagery or posting considered.

Facebook also fails to address or mention the significant psychological trauma of viewing the graphic content that these content moderators live with daily. 41 In May 2020, Facebook settled a multiemployee lawsuit around the failure to act when content moderators were reporting severe PTSD symptoms related to their jobs, and without adequate mental health support. 42 While this issue is now sadly common in the industry, it also shows how difficult it is to retain and hire workers in these positions, who are on the very frontlines in the Internet battle against child sex abuse on the Internet.

Facebook's recent \$5.9 billion stake in Reliance Jio in India further raises alarms amongst some child protection experts. 43 Even pre-COVID-19 crisis, CSAM online was surging in India, and initial reports during the crisis show those numbers escalating, along with a significant increase in Internet users searching for CSAM in the region. $^{\rm 44~45}$

Overall, Facebook's tools, content moderators, and AI have not been enough to keep child sex abuse imagery, live-streaming, and videos off of its platforms that are unencrypted—much less when those channels "go blind" and mask the content from the company's eyes.

Facebook highlights its work with law enforcement and NGOs, but fails to state that law enforcement and NGOs are among its fiercest critics on how it has responded to this crisis. Facebook has also lobbied for the defeat of numerous bills that sought or currently seek to protect children from sexual abuse online. 46 47 48

³⁹ https://www.theverge.com/2019/7/22/20<u>706250/facebook-messenger-kids-bug-chat-app-unauthorized-</u>

⁴⁰ https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1721&context=shlr

⁴¹ https://techcrunch.com/2020/05/12/facebook-moderators-ptsd-settlement/

⁴² https://www.tampabay.com/news/business/2020/05/12/facebooks-52-million-settlement-goes-to-contentmoderators-who-faced-trauma-on-the-job/

⁴³ https://www.deccanchronicle.com/technology/in-other-news/260420/ncpcr-issues-notice-to-googlewhatsapp-twitter-over-child-sexual-abu.html

⁴⁴ https://timesofindia.indiatimes.com/<u>india/icpf-report-warns-of-sharp-rise-in-demand-for-online-child-</u> pornography-during-lockdown/articleshow/75127399.cms

https://www.thehindu.com/news/national/most-online-content-on-child-sexual-abuse-fromindia/article31377784.ece https://www.protocol.com/earn-it-act-hearing-section-230

In short, the opposition statement provides a list of actions without any assessment of their overall effectiveness at decreasing the growth or demand for CSAM on its services. The company also fails to directly address the resolution's request for information of how privacy and encryption tools will impact child sex crimes and online safety. The company has also failed to speak with the resolution co-filers despite our request for dialogue. By contrast, shareholders have had productive dialogues on this issue with other companies including Verizon, AT&T, Apple and Alphabet that led to the withdrawal of similar shareholder resolutions.

CONCLUSION

Facebook is by far and away the world's largest source of online child sexual abuse materials. The company has been harshly criticized by governments, law enforcement and child protection organizations for its insufficient efforts to prevent or stop CSAM. Its determination to apply end-to-end encryption to all its platforms without ensuring that this won't lead to further sexual exploitation of children has led to threats of governmental regulation, global negative media coverage, and reputational risk. Shareholders believe that the company needs to report on its assessment of the risk of increased sexual exploitation of children as it develops and offers additional privacy tools such as end-to-end encryption.

We ask that you vote for Item 10: Report on Online Child Sexual Exploitation

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY ONE OR MORE OF THE CO-FILERS. PROXY CARDS WILL NOT BE ACCEPTED BY ANY CO-FILER. PLEASE DO NOT SEND YOUR PROXY TO ANY CO-FILER. TO VOTE YOUR PROXY. PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.

⁴⁷ https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/

⁴⁸ https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html