PROXY IMPACT
The power to change business as usual

Meta Platforms Inc. (FB)
Proposal #11–Child Sexual Exploitation Online

Annual Meeting May 25, 2022
Contact: Michael Passoff, CEO, Proxy Impact michael@proxyimpact.com

RESOLVED CLAUSE: *Shareholders request that the Board of Directors issue a report by February 2023 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 on 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

Meta plays a central role in online child sexual exploitation

- In 2021 there were nearly 29 million reported cases of online child sexual abuse material (CSAM), nearly 27 million of these (92%) stemmed from Meta platforms including Facebook, WhatsApp, Messenger and Instagram.
- This represents an increase of 69% from Meta's nearly 16 million reports in 2019 when shareholders first raised this issue with the company.

The impact of end-to-end encryption on children

- Meta's plan to apply end-to-end encryption to its platforms, without first stopping CSAM, could effectively make invisible 70% of its CSAM incidents that are currently being detected and reported.
- Meta stopped reporting CSAM in the EU for several months in 2021 which led to a 58% decrease in EU CSAM reports.
- Meta's rush to expand end-to-end encryption has led to an immense backlash and poses extreme risk to children worldwide.
- Governments, law enforcement agencies and child protection organizations have harshly criticized Meta's planned encryption, claiming that it will cloak the actions of child predators and make children more vulnerable to online sexual abuse.

Financial risk

- Pending legislation in the European Union, U.S. Congress and other countries could make Meta legally liable for CSAM and subject to costly fines and lawsuits.
- The company is facing increasing regulatory, reputational and legal risk due to this issue.

This is not a choice between internet privacy or child safety

- Proponents of this resolution are not opposed to encryption and recognize the need for improved online privacy and security.
- Meta has promoted a false narrative that end-to-end encryption requires a choice between privacy *or* child safety.
- There are a number of technological developments that should allow anti-CSAM practices to coexist with encryption.

THE LINK BETWEEN SOCIAL MEDIA AND CHILD SEXUAL ABUSE

Reported incidents of child sexual exploitation have increased dramatically from year to year over the past decade from 100,000 CSAM incidents twelve years ago to nearly 70 million incidents in 2019.[1] The exponential growth of CSAM is tied directly to the growth of the internet and social media.[2] The 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. [3]

META'S CENTRAL ROLE

Meta is the world's largest social media company with over 3.6 billon active monthly users. Its platforms include Facebook with 2.9 billion monthly users, WhatsApp with over 2 billion users, Facebook Messenger with 1.3 billion users, and Instagram topping 1.2 billion users.[4] These four social media platforms alone account for nearly half of the world's monthly social media use.

In 2021, there were more than 29.1 million online CSAM reports. More than 20.3 million reports – or 92% – stem from Meta and its platforms.[5] As the world's largest social media company and the largest source of reported child sexual exploitation online, Meta's actions will, for better or worse, have a major impact on global child safety.

THE IMPACT OF END-TO-END ENCRYPTION ON CSAM

To be clear, shareholders are not opposed to encryption, but we believe that Meta should apply new privacy technologies in a way that will not pose additional threats to children, like sexual grooming (i.e., the luring or enticement of children for sexual purposes) or exploitation itself. Enhanced internet privacy is important, but it should not come at the expense of unleashing a torrent of virtually undetectable child sexual abuse materials on Meta.

In January 2021, Monika Bickert, Facebook's head of global policy management, testified at a hearing in the British House of Commons and in response to a question about how many CSAM cases would "disappear" if the company implements end-to-end encryption, she said, "I don't know the answer to that. I would expect the numbers to go down. If content is being shared and we don't have access to that content, if it's content we cannot see then it's content we cannot report."[6] Meta's Facebook Messenger platform stopped scanning for CSAM in the European Union (EU) for several months, which led to a 58% decrease in EU CSAM reports.[7] [8]

The National Center for Missing and Exploited Children (NCMEC) is the national clearinghouse for CSAM materials in the U.S. According to NCMEC, "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."[9] NCMEC estimates 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 that are currently being detected and reported.[10]

Meta's current plan to apply end-to-end encryption to its platforms 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 FALSE CHOICE OF PRIVACY OR CHILD PROTECTION

Proponents of this resolution are not opposed to encryption and recognize the need for improved online privacy and security. The proponents do not believe that being for child protection means you are against internet privacy or vice-versa. Tech experts such as Hany Farid, a professor at the University of California, Berkeley, points out that the technology exists to protect privacy while still allowing a search for CSAM in 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.[11] We simply believe that these, and other types of child safety protections, need to be in place before expanding end-to-end encryption to other Meta platforms; and that not doing so will result in increased physical and mental risk to children, and financial risk to investors.

RRGULATORY, LEGAL AND FINANCIAL RISKS TO META

In the U.S., Electronic Service Providers (ESP)—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 Act.[12] Meta, 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, lawmakers "have identified child sexual abuse imagery and exploitation on the internet as an urgent problem." [13] It has brought intense regulatory scrutiny and a growing number of CSAM-related Congressional letters, hearings and legislation—all with strong bipartisan support—that raises the likelihood of regulatory action that could expose Meta to legal liability in some form that it has not had to face before.

Legislative action and bills introduced over the last few years that take aim at online child safety include:

- The Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act was introduced in 2020 and continues to advance to a Senate vote.[14] This bill takes aim at the Section 230 exemption [15] 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." [16]
- The Platform Accountability and Transparency Act would require social media companies to provide data about their companies that can be used for National Science Foundation social research. Companies could face losing immunity under Section 230 for failure to comply with research requests.[17]
- The Lawful Access to Encrypted Data Act would end warrant-proof encryption in devices, platforms and systems, and require ESPs and device manufacturers to assist law enforcement in decrypting data once a warrant has been issued.[18]
- A bipartisan bill called for $5 billion to help law enforcement and NGOs deal with the overwhelming flood of online CSAM.[19]
- The END Child Exploitation Act,[20] was introduced in both the House and Senate and seeks to improve how tech companies can provide law enforcement with information in a timely manner related to evidence of CSAM crimes.

- In 2019, the Senate Judiciary Committee held a hearing on encryption and public safety that included representatives from Meta and Apple. Child sexual abuse was repeatedly used as an example of harms that need to be addressed stemming from encrypted communication, and many comments from bipartisan Committee members threatened legislative action.[21]
- In 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 asked them, "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?"[22]
- In 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." [23] [24]
- In 2018, the U.S. House and Senate passed the Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) bills. This legislation made it illegal to knowingly facilitate child sex trafficking and removes Section 230 immunity from Electronic Service Providers that do so.[25] It also opened the door for a set of lawsuits that Facebook now faces.[26]

Facebook has lobbied for the defeat or weakening of numerous bills that sought or currently seek to protect children from sexual abuse online. [27] [28] [29]

Meta is facing its strongest regulatory challenges overseas:

- The UK Online Safety Bill (May 2022) will make companies responsible for user safety. One of the bill's primary goals is to end online child sexual abuse and exploitation. Social media companies can be hit with multibillion-dollar fines if they fail to adequately tackle illegal content when the law comes into force. [30] [31] [32]
- The European Union's Digital Services Act (April 2022) has been called "the most significant piece of social media legislation in history" by Facebook whistle blower Frances Haugan, and that it "will for the first time pull back the curtain on the algorithms that choose what we see and when we see it in our feeds."[33]
- In 2019, Australia passed the TOLA Act, an anti-encryption law that allows law enforcement to require companies to assist them in decrypting user data.
- Even countries as varied as Belgium and the Philippines that don't yet have legislation have been warning Meta that CSAM will no longer be tolerated.[34] [35]

CALLS FOR ENCRYPTION DELAY FRON LAW ENFORCEMENT AND CHILD PROTECTION AGENCIES

Facebook regularly 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 child sexual exploitation crisis.

A 2020 letter to Facebook, signed by child protection organizations from over 100 countries stated, "We therefore urge you not to proceed with the rollout until and unless you can demonstrate there will be no reduction in children's safety as a result of this decision." And, "end-to-end encryption will embolden abusers to initiate and rapidly escalate abuse on Facebook's

services … This presents an unacceptable risk to children, and would arguably make your services unsafe." [36] [37]

Law enforcement agencies have been equally vocal in their opposition to encryption. In 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. [38] [39] A letter from law enforcement leaders from the U.S., UK 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." [40]

META'S RESPONSE

In March 2019, Mark 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." [41] Since then, Zuckerberg and other Meta executives have acknowledged that encryption would limit the fight against child abuse, [42] [43] while claiming they are committed to prioritizing user privacy, but inexplicitly at the expense of children's privacy.

In May 2021, Meta launched Instagram for Kids. This drew an immediate rebuke from 44 attorneys general who wrote Meta asking it to scrap this idea and stated "Facebook has historically failed to protect the welfare of children on its platforms." [44] [45] One of the main concerns was the use of the platform by predators to target children. The letter references "an increase of 200% in recorded instances in the use of Instagram to target and abuse children over a six-month period in 2018, and UK police reports documented more cases of sexual grooming on Instagram than any other platform" [46] [47]

Meta's lack of response to shareholders should also be noted. Proponents originally filed this resolution in 2020 and received the support of over 712 million shares or about 43% of the vote not controlled by CEO Mark Zuckerberg and other management insiders. In 2021, support for this resolution increased as nearly 980 million shares voted for it (which represented about 56% of the non-management controlled vote). Since 2019, shareholders have requested to talk with the company about this issue, yet despite large and growing shareholder support, Meta has only offered one call with shareholders in response to our repeated requests beginning 30 months ago.

By comparison, shareholders have had productive dialogues and withdrawn resolutions, or not filed resolutions, at Apple, Alphabet, ATT and Verizon and others, as those companies have engaged shareholders on this issue.

Meta's Opposition Statement

Meta's opposition statement lists the actions it is taking regarding the *prevention, detection, and response* to CSAM.

First and foremost, the company does not answer the resolution request for an assessment of what will be the impact of end-to-end encryption on child sexual exploitation – a question that law

enforcement, government, child protection organizations, and investors have all been asking the company since 2018.

Secondly, proponents acknowledge that the company has been involved with a number of initiatives focused on preventing CSAM online, and that it has partnered and invested in technology tools to better identify CSAM and child abuse videos, and has also improved its public reporting on this issue.

Yet, Meta's tools, content moderators, and AI have not been enough to keep child sex abuse imagery, live-streaming, and videos off of its platforms even while unencrypted. In fact, Meta's nearly 27 million CSAM reports in 2021 is up more than 10 million reports (a 69% increase) from Meta's nearly 16 million reports in 2019 when shareholders first raised this issue with the company. If the company is unable to keep CSAM off the unencrypted platforms, what will the status be when those channels "go blind" and are masked from the company's eyes?

Thirdly, Meta provides a list of its actions, but does not offer any data to show the scope of these efforts or if they are successful. Quantitative data is needed to assess the effectiveness of Meta's policies and practices.

As for specific examples raised by Meta's opposition statement:

Prevention:
Meta states that "in October and November of 2020, 90% of the illegal child exploitative content was the same as or visually similar to previously reported content," and "just six videos were responsible for more than half of the child exploitative content that we reported in the time period." Child safety experts we conferred with were skeptical of this claim and felt that much more context was needed such as the definition of "visually similar," the number and type of images, if the data was from one platform or multiple ones, if the search was just for known material or if it included new images. It should also be noted that this is the same example Meta used in its 2021 opposition statement, as apparently the company had no new or more detailed information to provide.

Even if we accept Meta's assertion that 90% is reshared or similar content, Meta filed 26,885,302 reports in 2021, which implies that 2,688,530 (10%) was new content. It should also be noted that it doesn't matter if the content is being reshared or is visually similar; it can still be going to (millions of) new viewers each time, and each time is a crime. Once child abuse images get online and are shared, children are victimized over and over again as images continue to circulate globally for years.

Meta has little to say about its failed age enforcement verification policies that are likely a major contributor to sexual grooming, sextortion and sex trafficking. Easy access by under-age participants to the new MetaVerse will only exacerbate more direct inappropriate and dangerous contact access for predators.[48]

Detection:
Meta describes the technology it uses to detect images and content. What it does not describe is how much of this will be ineffective once encryption hides content. That is the crux of this resolution.

Despite its new policies, the number of CSAM reports from Meta to NCMEC has escalated dramatically year over year. Meta has not made any estimate of the impact that encryption will have on its reporting. But NCMEC has estimated that it would lose 75% of reports due to encryption. Based on Meta's 26.8+ million reports in 2021 that would mean approximately 20.1 million reports would never be made.

Meta describes new policies for removing accounts, new educational efforts and age-related privacy measures. We commend Meta on these efforts and hope they are successful. But the company again fails to provide any data to indicate the scope or effectiveness of these efforts.

Meta highlights its content review teams, yet fails to mention that it had to settle a multi-employee lawsuit around the failure to act when content moderators were reporting severe PTSD symptoms related to their jobs, and without adequate mental health support.[49] [50] While this issue is now sadly common in the industry, it also shows how difficult it is to retain and hire content moderators, who are on the very frontlines in the internet battle against child sexual abuse.[51]

The leaked Facebook Papers also highlights that although most of Meta's users are outside of the U.S., (the largest sources of CSAM are believed to be Asia, Africa and the Middle East) its content moderators are mostly focused on U.S. content.

Response:
Meta provides a list of actions it has taken, mainly related to improving reporting. We applaud the company for taking these actions. Yet, as mentioned above, Meta provides qualitative assurances that this issue is being address but no quantitative data to support it.

In short, the opposition statement provides a list of actions without any assessment of their overall effectiveness at preventing, detecting or responding to CSAM on its services. The company also fails to address the resolution's request for information on how privacy and encryption tools will impact child sex crimes and online safety.

CONCLUSION
Support for this resolution is not a vote against internet privacy, it is a message to management that it needs to take extra precautions to protect the world's most vulnerable population – children. Meta is by far the world's largest source of online child sexual exploitation materials. The company has been harshly criticized by governments, law enforcement and child protection organizations for its insufficient efforts to stop CSAM. Its determination to apply end-to-end encryption to its platforms without ensuring that this won't lead to further sexual exploitation of children has led to legislation, global negative media coverage, and reputational risk that can affect its core business model. 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 Child Sexual Exploitation Online shareholder resolution was filed by Proxy Impact (on behalf of Lisette Cooper), Adrian Dominican Sisters, CommonSpirit Health, Congregation of St. Joseph, Dana Investment Advisors, Maryknoll Sisters, Providence St. Joseph Health, Sisters of the Presentation of the Blessed Virgin Mary, and Ms. Linda Wisnewski.

[1] https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html
[2] https://web.archive.org/web/20190928174029/https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf
[3] https://medium.com/modernslavery101/the-impact-of-covid-19-on-sex-trafficking-and-csam-e70ec788c93b
4 https://incredítools.com/meta-statistics/sApp
[5] https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf
[6] https://www.vice.com/en/article/88akbx/facebook-finally-admits-its-pivot-to-privacy-will-help-child-abusers
[7] https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/
[8] https://www.theguardian.com/technology/2021/jan/20/facebook-under-pressure-to-resume-scanning-messages-for-child-abuse-in-eu
[9] https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption
[10] https://www.justice.gov/opa/press-release/file/1207081/download
[11] https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/
[12] https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change
[13] https://www.nytimes.com/2020/05/05/us/child-abuse-legislation.html?action=click&module=News&pgtype=Homepage
[14] https://www.washingtonpost.com/technology/2022/02/10/senators-earn-it-privacy-children-safety/?utm_campaign=wp_post_most&utm_medium=email&utm_source=newsletter&wpisrc=nl_most&carta-url=https%3A%2F%2Fs2.washingtonpost.com%2Fcar-ln-tr%2F3600b02%2F620545689
[15] http://broadbandbreakfast.com/2020/03/big-tech-must-combat-child-sexual-abuse-material-online-or-lose-section-230-protection-say-senators/
[16] https://www.nytimes.com/2020/03/05/us/child-sexual-abuse-legislation.html
[17] https://thehill.com/policy/technology/585069-senators-unveil-bipartisan-unveil-bill-requiring-social-media-giants-to/
[18] https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity
[19] https://www.nytimes.com/2020/05/05/us/child-abuse-legislation.html?action=click&module=News&pgtype=Homepage
[20] https://anthonygonzalez.house.gov/news/documentsingle.aspx?DocumentID=179
[21] https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy
[22] https://www.blumenthal.senate.gov/imo/media/doc/11.18.19%20-%20Google%20-%20CSAM.pdf
[23] https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-query-facebook-on-messenger-kids-design-flaw
[24] https://www.theverge.com/2019/8/28/20837552/facebook-messenger-kids-bug-markey-blumethal-letter
[25] https://en.wikipedia.org/wiki/Stop_Enabling_Sex_Traffickers_Act
[26] https://www.occrp.org/en/daily/12224-us-court-approves-sex-trafficking-lawsuits-against-facebook
[27] https://www.protocol.com/earn-it-act-hearing-section-230
[28] https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/
[29] https://www.wsj.com/articles/facebook-whistleblower-pushback-political-spin-zuckerberg-11640786831
[30] https://www.lexology.com/library/detail.aspx?g=a95b4497-8b25-4469-96de-df29132a9bb1
[31] https://www.wired.com/story/uk-trying-to-stop-facebook-end-to-end-encryption/
[32] https://digitalprivacy.news/?p=10499
[33] https://www.nytimes.com/2022/04/28/opinion/social-media-facebook-transparency.html?smid=em-share
[34] https://www.politico.eu/article/encryption-could-hinder-childrens-safety-brussels-warns-facebook/
[35] https://www.philstar.com/headlines/2021/03/03/2081676/senator-urges-facebook-twitter-crack-down-exploitation-activities
[36] https://www.nspcc.org.uk/globalassets/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf
[37] https://timesofindia.indiatimes.com/business/india-business/ngos-working-against-child-sex-abuse-urge-facebook-ceo-mark-zuckerberg-to-rethink-encryption-plans/articleshow/73984126.cms
[38] https://www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitation-cases
[39] https://www.wpxi.com/news/politics/doj-says-facebooks-encryption-plan-will-hinder-child-sex-crimes-investigations/993718808/
[40] https://www.washingtonpost.com/world/national-security/us-allies-ask-facebook-not-to-encrypt-its-messaging-service/2019/10/03/9180d27c-e5f0-11e9-a6e8-8759c5c7f608_story.html
[41] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/
[42] https://uk.reuters.com/article/uk-facebook-security-zuckerberg/facebooks-zuckerberg-defends-encryption-despite-child-safety-concerns-idUKKBN1WJ02N
[43] https://www.theguardian.com/technology/2021/jan/21/facebook-admits-encryption-will-harm-efforts-to-prevent-child-exploitation
[44] https://ag.ny.gov/sites/default/files/naag_letter_to_facebook_-_final.pdf
[45] https://news.sky.com/story/instagram-investigated-over-alleged-illegal-processing-of-childrens-data-12108202
[46] https://www.nspcc.org.uk/about-us/news-opinion/2019/over-5000- grooming-offences-recorded-18-months/
46 https://www.proxyimpact.com/facebook
47 https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/
48 https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/?utm_campaign=wp_post_most&utm_medium=email&utm_source=newsletter&wpisrc=nl_most&carta-url=https%3A%2F%2Fs2.washingtonpost.com%2Fcar-ln-tr%2F35f92fe%2F62014ca29d2fda518038bac3%2F5976b1b7ae7e8a6816daa3f0%2F8%2F74%2F62014ca29d2fda518038bac3