







## NOTICE OF EXEMPT SOLICITATION

NAME OF REGISTRANT: Facebook Inc.

NAME OF PERSONS RELYING ON EXEMPTION: Proxy Impact

ADDRESS OF PERSON RELYING ON EXEMPTION: 5011 Esmond Ave, Richmond CA. 94805

**WRITTEN MATERIALS**: The attached written materials are submitted pursuant to Rule 14a-6(g)(1) (the "Rule") promulgated under the Securities Exchange Act of 1934,\* in connection with a proxy proposal to be voted on at the Registrant's 2021 Annual Meeting. \*Submission is not required of this filer under the terms of the Rule but is made voluntarily by the proponent in the interest of public disclosure and consideration of these important issues.

# Facebook, Inc. (FB) Vote Yes: Item #6-Child Sexual Exploitation Online

Annual Meeting May 26, 2021 Contact: Michael Passoff, CEO, Proxy Impact michael@proxyimpact.com

## THE PROPOSAL

**ITEM 6 RESOLVED CLAUSE:** Shareholders request that the Board of Directors issue a report by February 2022 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**

In 2020 there were nearly 22 million reported cases of online child sexual abuse material (CSAM), 94% of which stemmed from Facebook. This represents an increase of 28% from Facebook's nearly 17 million reports in 2019. 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 that are currently being detected and reported.

Facebook's rush to expand end-to-end encryption across its platforms, without addressing the issues of child sexual exploitation, has led to an immense backlash and poses legitimate risk to children worldwide. 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 and other countries could make Facebook legally liable for CSAM, The company is facing increasing regulatory, reputational and legal risk due to this issue.

Proponents of this resolution are not opposed to encryption and recognize the need for improved online privacy and security. There are a number of technological developments that should allow anti-CSAM practices to coexist with encryption. Support for this resolution is not a vote against privacy, but a message to management that it needs to take extra precautions to protect the world's most vulnerable population – children.

1

Consequently, shareholders believe that the company needs to assess 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

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. The exponential growth of CSAM is tied directly to the growth of the internet and social media. 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. The link between child sex abuse searches by child predators on public search engines during the COVID pandemic.

## FACEBOOK'S CENTRAL ROLE

Facebook is the world's largest social media company with 2.8 billon active monthly users. Facebook's other platforms include WhatsApp with 2 billion users, Facebook Messenger with 1.3 billion users, and Instagram topping 1.2 billion users. These four social media platforms alone account for nearly half of the world's monthly social media use.

In 2020, there were more than 21.7 million online CSAM reports, containing 65.4 million images and videos. More than 20.3 million reports – 94% of that – stem from Facebook and its platforms, including Messenger and Instagram.<sup>7</sup>

As the world's largest social media company and the largest source of reported child sexual exploitation online, Facebook'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 Facebook 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. 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.

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." Later that month, Facebook stopped scanning for CSAM in the EU for three weeks, which resulted in a "46% fall in referrals for child sexual abuse material." <sup>9</sup>

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." <sup>10</sup> 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. <sup>11</sup>

The company's current plan to apply end-to-end encryption to all 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. We do not believe that being for child protection means you are against 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. 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 Facebook platforms; and that not doing so will result in increased physical and mental risk to children, and financial risk to investors.

## FINANCIAL RISK TO FACEBOOK

## Regulatory and Legal Risk

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. 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, lawmakers "have identified child sexual abuse imagery and exploitation on the internet as an urgent problem." <sup>14</sup> 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 Facebook to legal liability in some form that it has not had to face before.

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. 15 It also opened the door for a set of lawsuits that Facebook now faces. 16

## Proxy Impact: Vote Yes on Facebook Item #6-Child Sexual Exploitation Online

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." <sup>17</sup>

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 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?" <sup>19</sup>

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 of harms that need to be addressed stemming from encrypted communication, and many comments from bipartisan Committee members threatened legislative action.<sup>20</sup>

Also in December 2019, a bipartisan bill was introduced in both the House and Senate called the END Child Exploitation Act,<sup>21</sup> which seeks to improve how tech companies can provide law enforcement with information in a timely manner related to evidence of CSAM crimes.

In March 2020, the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act was introduced.<sup>22</sup> <sup>23</sup> This bill takes aim at the Section 230 exemption <sup>24</sup> 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." <sup>25</sup>

In May 2020, a bipartisan bill called for \$5 billion to help law enforcement and NGOs deal with the overwhelming flood of online CSAM.<sup>26</sup>

In June 2020, the Lawful Access to Encrypted Data Act was introduced. This bill 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.<sup>27</sup>

Facebook has lobbied for the defeat or weakening of numerous bills that sought or currently seek to protect children from sexual abuse online. <sup>28</sup> <sup>29</sup> <sup>30</sup> Facebook is facing even stronger regulatory pressure overseas.

In May 2021, the UK released its draft Online Safety Bill that will make companies responsible for user safety. One of the bill's primary goals is to end online child sexual abuse and exploitation. Facebook's encryption plans have made it a regular target of the UK Home Secretary and Home Office. <sup>31 32 33</sup> 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 that don't yet have legislation have been warning Facebook that CSAM will no longer be tolerated. <sup>34 35</sup>

## Calls for Encryption Delay From 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 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." <sup>36</sup> <sup>37</sup>

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. <sup>38</sup> <sup>39</sup> 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." <sup>40</sup>

## FACEBOOK'S RESPONSE

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." <sup>41</sup> Since then, Zuckerberg and other Facebook executives have acknowledged that encryption would limit the fight against child abuse, <sup>42 43</sup> while claiming they are committed to prioritizing user privacy, but inexplicitly at the expense of children's privacy.

In May 2021, in a move that is shockingly tone deaf given the number of concerns raised about child safety, Facebook announced that it is launching Instagram for Kids. This drew an immediate rebuke from 44 attorneys general who wrote Facebook asking it to scrap this idea and stated "Facebook has historically failed to protect the welfare of children on its platforms." <sup>44 45</sup> 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" <sup>46 47</sup>

Facebook's response to shareholders should also be noted. Proponents filed a similar resolution last year and the resolution received the support of over 712 million shares valued at more than \$163 billion on the date of the annual meeting. The resolution received 12.6% of all shares voted. This comes out to about 43% of the shares not controlled by Facebook CEO Mark Zuckerberg and other management insiders. Yet apparently 712 million shares and 43% of non-management vote was not enough to get a response from the company. It took over a year for Facebook to respond to proponents' requests for a company dialogue. Our first request for a dialogue was in December 2019 but our first call with the company was not until May 2021.

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

## **Facebook's Opposition Statement**

Facebook'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 since 2018 in its Community Standards reports. Yet, 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 even while unencrypted (much less when those channels "go blind" and mask the content from the company's eyes) and in fact, the number of its CSAM reports has increased by millions every year.

Thirdly, Facebook does not put its list of actions into context. It had 20,307,216 CSAM reports in 2020, but we do not know, for instance, how many incidents were prevented by its actions. Quantitative data is needed to assess the effectiveness of Facebook's actions.

As for specific examples raised by Facebook:

## **Prevention:**

Facebook states that "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," and from that they estimate that "more than 75% of the accounts that we reported to NCMEC during July and August of 2020 and January of 2021 appeared to share for reasons other than malicious intent."

Our response is 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 afterwards.

Also, Facebook is only describing what it found during a short-term study. Plus, its AI detection is mostly geared to find 'known' content, not new content, so there could be a large amount of new content that Facebook is missing. Even if 90% is reshared or similar content, Facebook had 20,307,216 reports in 2020, which implies that 2,030,721 (10%) were new content. Similarly, Facebook says that 75% of accounts were not malicious, but that means that 25% – or 5,076,804 – are malicious. This is still an enormous amount of sexual exploitation taking place on Facebook's platforms.

## Detection:

Facebook 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. Facebook 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 Facebook's 20+ million reports in 2020 that would mean 15,230,412 reports would never be made.

Facebook also fails to address or mention that a significant amount of its content still has to be verified by thousands of humans, and the significant psychological trauma of viewing the graphic images that these content moderators live with daily. 48 49 Hundreds of low-paid workers sent a letter demanding safer working conditions and stated that "Without our work, Facebook is unusable ... Your algorithms cannot spot satire. They cannot sift journalism from disinformation. They cannot respond quickly enough to self-harm or child abuse. We can." 50

In May 2020, Facebook settled 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.<sup>51 52</sup> 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 sexual abuse.

## **Response:**

Facebook touts WhatsApp as a leader in online safety. Here are some things it did not mention:

- A survey of over 2000 kids found that "60% of 8-year-olds and 90% of 12-year-olds reported using a messaging app with an age restriction of 13 or older. Three quarters of 12-year-olds reported using Whatsapp, despite the minimum age requirement for this platform being 16."
- "Whatsapp was not only the most widely used platform across our sample, but it was also rife with underage users: 37% of 8 year olds and 72% of 12 year olds had used the platform in the four weeks prior to the survey despite the fact that Whatsapp has a minimum age of 16." 53

In fact, Facebook has faced numerous user data privacy complaints and its success at circumventing the Children's Online Privacy Protection Act (COPPA) is well documented. <sup>54</sup>

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**

Facebook 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 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 6: 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.

- <sup>1</sup> https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html
- $^2\ https://web.archive.org/web/20190928174029/https://storage.googleap is.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf$
- <sup>3</sup> https://www.scientificamerican.com/article/the-coronavirus-pandemic-puts-children-at-risk-of-online-sexual-exploitation/
- 4 https://www.netclean.com/2021/04/06/we-have-seen-a-definite-increase-in-child-sexual-abuse-crime-during-the-covid-19-pandemic/
- <sup>5</sup> https://medium.com/modernslavery101/the-impact-of-covid-19-on-sex-trafficking-and-csam-e70ec788c93b
- <sup>6</sup> https://www.businessofapps.com/data/facebook-statistics/
- <sup>7</sup> https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf
- 8 https://www.vice.com/en/article/88akbx/facebook-finally-admits-its-pivot-to-privacy-will-help-child-abusers
- https://www.theguardian.com/technology/2021/jan/20/facebook-under-pressure-to-resume-scanning-messages-for-child-abuse-in-eu
- <sup>10</sup> https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption
- 11 https://www.justice.gov/opa/press-release/file/1207081/download
- 12 https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/
- 13 https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change
- 14 https://www.nytimes.com/2020/05/05/us/child-abuse-legislation.html?action=click&module=News&pgtype=Homepage
- <sup>15</sup> https://en.wikipedia.org/wiki/Stop\_Enabling\_Sex\_Traffickers\_Act
- <sup>16</sup> https://www.occrp.org/en/daily/12224-us-court-approves-sex-trafficking-lawsuits-against-facebook
- 17 https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-query-facebook-on-messenger-kids-design-flaw
- <sup>18</sup> https://www.theverge.com/2019/8/28/20837552/facebook-messenger-kids-bug-markey-blumethal-letter
- 19 https://www.blumenthal.senate.gov/imo/media/doc/11.18.19%20-%20Google%20-%20CSAM.pdf
- <sup>20</sup> https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy
- <sup>21</sup> https://anthonygonzalez.house.gov/news/documentsingle.aspx?DocumentID=179
- 22 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
- <sup>23</sup> https://anthonygonzalez.house.gov/news/documentsingle.aspx?DocumentID=321
- <sup>24</sup> http://broadbandbreakfast.com/2020/03/big-tech-must-combat-child-sexual-abuse-material-online-or-lose-section-230-protection-say-senators/
- <sup>25</sup> https://www.nytimes.com/2020/03/05/us/child-sexual-abuse-legislation.html
- <sup>26</sup> https://www.nytimes.com/2020/05/05/us/child-abuse-legislation.html?action=click&module=News&pgtype=Homepage
- <sup>27</sup> 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
- <sup>28</sup> https://www.protocol.com/earn-it-act-hearing-section-230
- <sup>29</sup> https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/
- <sup>30</sup> https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html
- <sup>31</sup> https://www.lexology.com/library/detail.aspx?g=a95b4497-8b25-4469-96de-df29132a9bb1
- <sup>32</sup> https://www.wired.com/story/uk-trying-to-stop-facebook-end-to-end-encryption/
- 33 https://digitalprivacy.news/?p=10499
- $^{34}\ https://www.politico.eu/article/encryption-could-hinder-childrens-safety-brussels-warns-facebook/$
- 35 https://www.philstar.com/headlines/2021/03/03/2081676/senator-urges-facebook-twitter-crack-down-exploitation-activities
- $^{36}\ https://www.nspcc.org.uk/globalassets/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf$
- <sup>37</sup> 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
- <sup>38</sup> https://www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitation-cases
- <sup>39</sup> 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
- $^{46}\ https://www.nspcc.org.uk/about-us/news-opinion/2019/over-5000-\ grooming-offences-recorded-18-months/.$
- 47 https://www.bbc.com/news/uk-47410520.
- 48 https://techcrunch.com/2020/05/12/facebook-moderators-ptsd-settlement/
- 49 https://www.bandt.com.au/they-suggest-karaoke-or-painting-facebook-content-moderator-questions-support-systems/

## Proxy Impact: Vote Yes on Facebook Item #6-Child Sexual Exploitation Online

 $<sup>\</sup>overline{^{50}\,\text{https://www.npr.org/2020/11/18/936282353/facebook-contract-workers-demand-safer-conditions-amid-pressure-to-return-to-off}$ 

<sup>51</sup> https://www.forbes.com/sites/angelauyeung/2021/01/29/facebook-content-moderators-in-ireland-meet-deputy-prime-minister-speak-out-against-working-conditions/?sh=1a8b6b65321d

<sup>&</sup>lt;sup>52</sup> https://www.tampabay.com/news/business/2020/05/12/facebooks-52-million-settlement-goes-to-content-moderators-who-faced-trauma-on-the-job/

<sup>&</sup>lt;sup>53</sup> https://www.childrenscommissioner.gov.uk/wp-content/uploads/2020/12/cco-access-denied.pdf

<sup>&</sup>lt;sup>54</sup> https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1721&context=shlr