University of Nottingham
Rights Lab

Ending encryption - potential implications on human trafficking

Research briefing by Henry Welch, 04/2022.[1]

This briefing provides a high-level summary of key stakeholder positions on end-to-end encryption (E2EE). The briefing explores the current discourse on E2EE and provides recommendations for further work to investigate the implications of encryption on efforts to address human trafficking and child sexual exploitation and abuse.

Key research findings

- Governments have sought to implement legal measures which limit the proliferation of E2EE, stating that it is incompatible with online service providers (OSPs) duty of care to protect internet users from exploitation, abuse and other online harms.
- However, cyber security experts believe that measures that seek to undermine E2EE damage the privacy and security of all online users and exacerbate the risks of harm to children and others. They suggest that these measures also challenge the popular notions of privacy and freedom of expression.
- OSPs believe that they can implement additional online safety measures without compromising on E2EE and user privacy.
- However, there is a lack of specificity from both sides of the debate. Those campaigning against the further rollout of E2EE have not provided significant evidence that demonstrates how stemming E2EE would significantly help to address child sexual exploitation and abuse (CSEA), and trafficking. Those supportive of E2EE have not yet provided detailed proposals for alternative measures should E2EE continue to be widely used.
- The current debate on E2EE is disproportionality focused on issues of child protection and doesn't adequately represent how the erasure or proliferation of E2EE impacts other social issues and harms, such as fraud and identity theft, freedom of expression, and the right to protest.

Why is this important?

E2EE is a method of secure communication that prevents third parties from accessing data while it is being transmitted from one system or person to another. In this process, data is encrypted (turned into a scrambled code) on the sender's system. Upon delivery, only the intended recipient can decrypt and unscramble the code. The contents of the message cannot be seen by anyone else.

Many popular messaging platforms use E2EE as a means of securing users' personal and private information. However, in recent years they have faced criticism as it makes it harder for OSPs to share data with authorities. Proponents of E2EE contend that it helps to protect the privacy and security of technology users, and there have been recent moves to widen its implementation further, most notably in services operated by Meta, which includes Facebook, WhatsApp and Instagram.

However, by protecting the privacy of everyone E2EE can also offer a degree of anonymity to those involved in illicit activities, enabling them to communicate securely, and without fear of interception from law enforcement.[2] Recently, child protection NGOs and the UK Government have argued that E2EE protects those involved in the production and distribution of CSEA material and governments have called for 'backdoors' into encrypted devices and services that enable authorities to circumvent encryption and to read the contents of messages and communications.

Recommendations

- For discourse to progress key stakeholders should depart from their polarised positions on E2EE. The implications – both technically and socially of encryption require frank and open discussion to identify measures that protect the privacy of users whilst also making positive strides to keep them safe from harm online.
- Further research into the investigative capacity and limitations of law enforcement digital-investigations teams, and the effectiveness of current legal provisions to identify and prosecute traffickers and perpetrators of CSEA is needed.
- Additional emphasis is needed non-enforcement-based measures, including the provision of support and rehabilitation for demand-side CSEA offenders– in recognition that paedophilia is a psychiatric disorder, as part of more holistic measures to address CSEA.
- The challenge of addressing issues associated with online harm further emphasises the need for 'safety by design' features to be embedded in future online services.[3]

[1] This research briefing was prepared by Henry Welch (University of Nottingham School of Politics) as part of a student placement with Dr. Ben Brewster (University of Nottingham, Rights Lab). For more information, please contact Ben.Brewster@nottingham.ac.uk

[2] Organization for Security and Co-operation in Europe, "Leveraging Innovation to Fight Trafficking in Human Beings: A Comprehensive Analysis of Technology Tools," 2020, 11–18, https://www.osce.org/files/f/documents/9/6/455206_1.pdf.

[3] World Economic Forum, "Safety by Design (SbD)," n.d., https://www.weforum.org/projects/safety-by-design-sbd.

Research overview

The remainder of this briefing is organised against what have been identified as four contrasting perspectives both in support and against E2EE, broadly organised by stakeholder group (governments, child protection NGOs, cyber-security and civil-liberty NGOs, and the tech industry). This is followed by a short consideration of other approaches that have been considered. The briefing is concluded by a short section discussing areas that require future work and research.

Governments

The UK's Department for Digital, Culture, Media & Sport (DCMS) argue that E2EE makes it more difficult to identify illegal and harmful content, and those responsible for its production and dissemination.[4] Furthermore, it is believed that E2EE allows criminals to 'go dark' and act anonymously, with governments and law enforcement requesting the implementation of 'backdoors' in services and devices that enable them to access the content of encrypted communications.[5]

E2EE has recently been targeted by a variety of legislation. In 2016, the British Investigatory Powers Act (IPA) granted the government increased oversight over OSPs, with sections 252 and 253 potentially imposing obligations upon them that undermine E2EE.[6] The IPA mandates that device manufacturers are required to remove the encryption on their devices and messages when requested to do so by the Secretary of State, and following approval from a judge.[7] Although it's understood that the IPA has not yet been exploited aggressively, it hold significant potential to push measures that undermine device encryption.[8]

The Australian government enacted the Telecoms and Other Legislation Amendment (TOLA) in 2018. TOLA mandates companies to create encryption 'backdoors' into their devices for use by authorities. Further bills are currently being drafted in both Britain and the United States, namely the Online Safety Bill (OSB) and the EARN IT act. The OSB includes a requirement for companies to prevent 'harmful or illegal' content on their services, and both bills create significant opportunities for their respective governments to push against and undermine E2EE without explicitly banning it.[9] The OSB has been supported by charities such as the National Society for the Prevention of Cruelty to Children (NSPCC) and the UK's children's commissioner.[10]

The British government in particular has also attempted to influence discourse around E2EE, notably through its #NoPlaceToHide campaign. The Campaign encourages "social media companies to make a commitment that they will only roll out E2EE when they have the technology to ensure children will not be put at greater risk as a result".[11] While the campaign doesn't explicitly call for the end of E2EE it does not offer any solutions that would address issues of child protection while maintaining it. Critics of the campaign have described it as anti-encryption propaganda, suggesting that it exploits the emotive nature of CSEA to undermine E2EE, without thoroughly considering all the implications of its prohibition.[12]

Anti-encryption positions at present also do not consider implications on the safety and privacy of those with lived experience of exploitation, or those individuals and communities considered most at risk of it or other crimes and abuses. They also disregard dominant perspectives from the cyber security industry which suggest that encryption must be absolute for it to be truly effective. Cyber security experts suggest that the inclusion of 'backdoors' that enable law enforcement and government to access data can be equally exploited by nefarious actors to cause additional harm.

As it stands, it is unclear whether an end to E2EE would lead to a significant reduction in trafficking and CSEA online, or what implications it would have on internet users' exposure to other forms of harm and abuse.

Child protection NGOs

Like governments, prominent child protection NGOs have also typically stood against the further proliferation of E2EE, believing that it inhibits efforts to end CSEA.[13] They believe that while children have the right to privacy and the protection of their personal data these are secondary to their specific rights to be protected from violence, abuse and exploitation.[14] While few would argue with the principles of stance, there are major questions regarding the extent to which E2EE can actually be regulated effectively, and what other risks are caused by its removal.[15]

The American National Centre for Missing & Exploited Children (NCMEC) argue that the ubiquitous rollout of E2EE would lead to significant reductions in reporting to its CyberTipline by OSPs (social media, websites, etc.), with abuse and exploitation material that would once be reported automatically now encrypted and hidden from view. NCMEC suggests that Facebook's plans to fully encrypt all of their messaging services may reduce overall CyberTipline reports by up to 80%.[16] In 2019, NCMEC received over 15.8 million reports of CSEA material from Facebook, accounting for over 94% of all reports to the CyberTipline service.[17] These reports are seen as an essential tool in the removal of CSEA material from the internet, and NCMEC's fears that the further rollout of E2EE would significantly reduce the number of reports made, and thus amount of content removed, are understandable.

NCMEC has itself offered an open letter with five principles that it believes, if followed, would increase the protection of children online. The majority of these are uncontentious and include calls for the wider adoption of tools to prevent the distribution of CSEA material and support for law enforcement to use legal processes to investigate the sexual exploitation of children.[18] However, their belief that E2EE should be banned for all users under eighteen is controversial. Some

[4] Department for Digital Culture Media and Sport, "Private and Public Channels: Improve the Safety of Your Online Platform," *Gov.UK*, 2021, https://www.gov.uk/guidance/private-and-public-channels-improve-the-safety-of-your-online-platform.
[5] Amie Stepanovich and Michael Karanicolas, "Why An Encryption Backdoor for Just the 'Good Guys' Won't Work," *Just Security*, 2018.
[6] Bhairav Acharya *et al.*, "Deciphering the European Encryption Debate: United Kingdom," *New America*, 2017, 4, https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-united-kingdom/.
[7] Acharya et al., 6.
[8] Acharya et al., 8.
[9] John Waterhouse, "Regulating Online Harms," *UK Parliment House of Commons Library*, 2022, 17, https://commonslibrary.parliament.uk/research-briefings/cbp-8743/; Callum Voge and Robin Wilton, "Internet Impact Brief: End-to-End Encryption under the UK's Draft Online Safety Bill," *Internet Society*, 2022, https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/.
[10] Waterhouse, "Regulating Online Harms," 13.
[11] UK Government, "Don't Give Child Sex Abusers a Place to Hide," n.d., https://noplacetohide.org.uk/.
[12] Connor Jones, "The Government's Anti-Encryption Campaign Shows It's Learned Nothing from the War on Drugs," *ITPro*, 2022, https://www.itpro.co.uk/security/encryption/361996/uk-anti-encryption-campaign-war-on-drugs.
[13] Daniel Kardefelt-Winther *et al.*, "Encryption, Privacy and Children's Right to Protection from Harm," *UNICEF*, 2020, https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children's_right_to_protection_from_harm.pdf; NSPCC, "End-To-End Encryption: Understanding the Impacts for Child Safety Online," 2021.
[14] Kardefelt-Winther *et al.*, "Encryption, Privacy and Children's Right to Protection from Harm."
[15] NSPCC, "End-To-End Encryption: Understanding the Impacts for Child Safety Online."
[16] Alex Hearn, "Facebook Admits Encryption Will Harm Efforts to Prevent Child Exploitation," *The Guardian*, 2021, https://www.theguardian.com/technology/2021/jan/21/facebook-admits-encryption-will-harm-efforts-to-prevent-child-exploitation.
[17] NSPCC, "End-To-End Encryption: Understanding the Impacts for Child Safety Online," 12.
[18] The National Center for Missing and Exploitated Children, "An Open Letter to the Technology Industry - End-to-End Encryption: Principles to Safeguard Children," 2020.

believe that such a move could have unforeseen consequences, suggesting that the lack of anonymity may prevent children undergoing abuse from speaking out due to concerns over their privacy and anonymity.[19] However, the longer-term implications of this are unclear. For example, would the prohibition of E2EE simply move both supply and demand-side offenders of CSEA onto other, and unregulated, platforms?

Currently, the number of prosecutions and law enforcement investigations into online CSEA are markedly lower than the volume of material that is identified and reported.[20] Pragmatic proposals for tech companies to work more closely with law enforcement have been made to ensure they are able to use existing legal process to investigate CSEA effectively. Significantly, however, the burden of cooperation lays largely with technology companies who have been historically slow and apprehensive to acknowledge and react to issues such as CSEA on their services.

NCMEC's predictions provide essential evidence for much of the anti-encryption lobby.[21] However, the efficiency of their CyperTipline has been questioned, as conviction rates are low compared to the volume of reports being made.[22] For websites hosted outside of the US NCMEC is reliant on national law enforcement acting on reports that they refer to. Moreover, for many reports, it is not possible to geolocate offences.[23] The capacity of law enforcement to conduct these investigations also varies significantly around the world, as does the extent to which these sorts of reports are prioritised.

Another issue is that many of the reports processed by NCMEC do not concern 'first generation' newly produced abuse material, meaning that content that is flagged is often copied and redistributed versions of 'known' CSEA material that is already in circulation.[24] The removal of this material is very important, but may not necessarily impact the supply of, or demand for, new content. Therefore, the relationship between reporting and the actions of law enforcement in investigating both supply and demand-side perpetrators is more complicated, and the impact that the mass rollout of E2EE would have on efforts to stem the production and demand of CSEA material is not clear.[25] However, the potential loss of a significant number of reports is concerning.

Cyber security and civil liberty NGOs

Both cyber-security and civil liberty groups tend to support widespread E2EE, believing that, above all, it protects the privacy and security of all internet users.[26] These industries typically oppose the engineering of backdoors into devices and web services. They discredit the concept of secure 'backdoors' which can only be accessed by law enforcement and suggest that these create pressure points that be equally exploited by hostile actors.[27] Legislating backdoors would also force tech companies to choose which nations should and would be allowed to access such backdoors and thus the content of users' devices and communications. This could lead to pressure from more autocratic nations for access, and heavily politicizes the actions of leading tech companies, forcing them to evaluate (or not) the human rights and democratic values of states.[28]

Civil liberty lobbyists also question the morality of ending E2EE, stating that they believe encryption to be a core component of freedom of speech and privacy. In their view if advocacy groups cannot share resources, engage stakeholders, or protect the anonymity of their supporters they cannot defend human rights.[29]

The viability of legislation targeting E2EE has also been criticized. The regulation of more mainstream platforms could result in the uptake and use of new and lesser-known platforms or techniques that subvert or operate outside of any proposed legal framework. This may also lead to criminals moving to unregulated products or the dark web, which would be counter-productive to law enforcement.[30] For example, work by Steel *et al* has highlighted how those who view and distribute illegal content online have continually adapted over the last 30 years.[31] Criminals have a vested interest in remaining anonymous and are likely to take measures to circumvent large OSPs operating within legislation like OSB and EARN IT.[32]

It's also suggested that laws will be difficult to enforce. Again, while it may be possible to work with established, Western-based organisations such as Meta, Google and Apple, open-source platforms, and those operated from Russia, China and other territories are likely to be much more difficult to police.[33] Furthermore, regulating users' access to certain websites has, historically, been easily circumvented through their use of VPNs, proxies, and more recently tools such as ToR.[34] Several services have sprung up in recent years in response to work by governments to undermine encryption and privacy within mainstream platforms. The terrorist group Al Qaeda, for example, introduced its own encrypted messaging software outside of US jurisdiction.[35] Moreover, Stepanovich and Karanicolas argue that leading organised criminal organisations and more sophisticated offenders are likely to continue to remain untouched by legislation, with it instead assisting in the identification of offenders who may have been identifiable via other and less contentious policing methods.[36]

These stakeholders are clear in their views regarding the importance of E2EE, and their view that E2EE must be absolute and widely implemented to protect the freedoms and privacy of all.[37] However, there remains little in the way of specific recommendations for other measures that could be taken to address trafficking and CSEA online.

---

[19] Hal Abelson et al., "Bugs in Our Pockets: The Risks of Client-Side Scanning," 2021, http://arxiv.org/abs/2110.07450.
[20] NCMEC, "National Centre for Missing and Exploited Children - CyberTipline," n.d., https://www.missingkids.org/gethelpnow/cybertipline.
[21] Hearn, "Facebook Admits Encryption Will Harm Efforts to Prevent Child Exploitation."
[22] Kardefelt-Winther et al., "Encryption, Privacy and Children's Right to Protection from Harm."
[23] The National Center for Missing and Exploitated Children, "2021 CyberTipline Reports by Country," 2022, https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf.
[24] Facebook, "Online Child Protection," n.d., https://www.facebook.com/safety/onlinechildprotection#:~:text=Across our family of apps,and victim resources and support.
[25] Kardefelt-Winther et al., "Encryption, Privacy and Children's Right to Protection from Harm," 9.
[26] Abelson et al., "Bugs in Our Pockets: The Risks of Client-Side Scanning"; Open Rights Group, "SAVE ENCRYPTION TO KEEP US SAFE," n.d., https://www.openrightsgroup.org/campaign/save-encryption/#:~:text=Join our campaign to ensure,encryption and free expression online.&text=If they get their way,and make us less safe.
[27] Abelson et al., "Bugs in Our Pockets: The Risks of Client-Side Scanning."
[28] Stepanovich and Karanicolas, "Why An Encryption Backdoor for Just the 'Good Guys' Won't Work."
[29] Internet Society, "Factsheet: How Encryption Can Protect Advocacy Groups and Social Change Movements," 2021, https://www.internetsociety.org/resources/doc/2021/factsheet-how-encryption-can-protect-advocacy-groups-and-social-change-movements/.
[30] Jones, "The Government's Anti-Encryption Campaign Shows It's Learned Nothing from the War on Drugs."
[31] Chad M.S. Steel et al., "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders," *Forensic Science International: Digital Investigation* 33 (2020): 4, https://doi.org/10.1016/j.fsidi.2020.300971.
[32] Steel et al., "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders."
[33] Riana Pfefferkorn, "THERE'S NOW AN EVEN WORSE ANTI-ENCRYPTION BILL THAN EARN IT. THAT DOESN'T MAKE THE EARN IT BILL OK," *The Center for Internet and Society*, 2020, http://cyberlaw.stanford.edu/blog/2020/06/there's-now-even-worse-anti-encryption-bill-earn-it-doesn't-make-earn-it-bill-ok.
[34] Stepanovich and Karanicolas, "Why An Encryption Backdoor for Just the 'Good Guys' Won't Work."
[35] Pfefferkorn, "THERE'S NOW AN EVEN WORSE ANTI-ENCRYPTION BILL THAN EARN IT. THAT DOESN'T MAKE THE EARN IT BILL OK."
[36] Jones, "The Government's Anti-Encryption Campaign Shows It's Learned Nothing from the War on Drugs."
[37] Dan Milmo, "End-to-End Encryption Protects Children, Says UK Information Watchdog," *The Guardian*, 2022, https://www.theguardian.com/technology/2022/jan/21/end-to-end-encryption-protects-children-says-uk-information-watchdog.

This position, at present, fails to properly engage with the justified fears of other stakeholders. The cyber-security industry must seek dialogue with the other groups presented in this report.

Tech companies

Social media platforms are being directly targeted by the UK government's attempts to legislate against E2EE. However, these companies, especially Meta, have repeatedly suggested that they can protect users without compromising on their commitments to E2EE.[38] Meta believes that they have adequate protections in place, including the ability to report those sending inappropriate content.[39] Controversially, they have announced plans to further rollout E2EE services across their services, believing that the priority of their users is their privacy.[40] This has now been delayed until 2023, and perhaps indicates some acknowledgement of the potential publicity issues this may cause unless additional measures to protect online users from abuse and exploitation are implemented.

Other measures have been suggested. Apple for example has attempted to find a compromise and implement an approach called Client-Side Scanning (CSS) onto their devices. CSS refers to systems that can scan the content of messages against a database of objectionable content before the message is encrypted and sent. Apple believes that this approach does not break E2EE and would assist in their efforts to prevent CSEA.[41] However, although CSS was initially planned it has now been paused, and all evidence of the plan has been removed from Apple's public material – leading some to suggest that concerns from civil liberty organisations have caused them to reconsider the viability of CSS.[42] Many see CSS as equivalent to ending E2EE.[43]

When looking at these contrasting organisations the polarisation of this debate is clear. Meta's attempts to increase the rollout of E2EE have led to condemnation from governments and child protection NGOs, while Apple's attempt to increase scanning has been shelved due to pressure from civil liberty groups.[44] Unfortunately, with all of these criticisms an adequate middle point or alternative has not been suggested, with these organisations unable to act either to increase E2EE or scanning without a barrage of negative responses from either side of the debate.

There has also been little consideration as to the role of privacy and encryption in increasing online safety. Technology access is increasingly important for all people and is often vital in protecting the privacy and human rights of many technology users. For instance in a study of adult survivors of modern slavery, Garbers *et al*, noted how technology was important in keeping people connected, and in some cases helped to negate some of the damaging impacts of their position as victims of exploitation.[45] E2EE may also be vital in these situations. Brunner notes that E2EE may provide those going through trafficking and abuse the confidence to contact NGOs for assistance anonymously.[46] The extent to which those with lived experience of exploitation rely on services that use E2EE is, however, as yet, inconclusive. For example, one study on technology related to trafficking repeatedly mentions the use of end-to-end encrypted WhatsApp by survivors. Though it cannot be reasonably assumed that this was due to its encryption and privacy features.

While it is clear that there is more to be done to protect users online, thorough consideration is needed to ensure that solutions do not have significant unforeseen ramifications on users' security and privacy.

Compromises

Within this debate, it is also important to question if any solutions have proposed which address the concerns of both sides of this debate. While proposals for approaches to address CSEA online have thus far been limited, the research did identify two different proposals, CSS, and the provision of therapeutic services for demand-side CSEA offenders.

Client-Side Scanning (CSS)

One area that is being explored is CSS. This allows a device to scan messages or data before it is encrypted and sent. Technically, this approach does not explicitly break encryption. If this scanned data is never seen by a human some believe this to be safer for people's privacy than removing E2EE entirely. However, many within the cyber security industry believe that CSS's promise to retail E2EE is little more than a technicality. Abelson *et al* argue that because a third-party is accessing data prior to its encryption, it is equivalent to breaking E2EE. Some see the approach as no different to a 'backdoor' and thus suggest that it poses the same questions in terms of privacy and security, with it still creating a weak spot through which data could still be targeted by hostile bodies.[47] Apple's apparent withdrawal of CSS potentially highlights fundamental flaws in the approach.[48]

Offender therapy

Offender therapy has also been rolled out more widely in recently years, and aims to work with CSEA material users to change their behaviour and stem the demand for new the production of new CSEA material. In a survey of CSEA material users on the Darkweb by Protect Children it was found that around 50% of CSEA material users wanted to stop accessing this material.[49] This informed the development of a self-help programme based on cognitive behavioural therapy to guide users away from CSEA. The Stop It Now Campaign by the Lucy Faithful Foundation took a similar approach. This campaign allows people to contact a secure messaging service and talk to a trained operator about their problematic behaviour.[50] These methods require CSEA offenders to recognise the problematic nature of their behaviour, and express desire to stop.

---

[38] Facebook, "Facebook's Response to Australian Government Consultation on a New Online Safety Act," 2020, https://about.fb.com/wp-content/uploads/2020/02/Facebook-response-to-consultation-new-Online-Safety-Act.pdf.
[39] Facebook.
[40] Dan Milmo, "Meta Delays Encrypted Messages on Facebook and Instagram to 2023," *The Guardian*, 2021, https://www.theguardian.com/technology/2021/nov/21/meta-delays-encrypted-messages-on-facebook-and-instagram-to-2023.
[41] Adi Robertson, "Apple's Controversial New Child Protection Features, Explained," *The Verge*, n.d., https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained.
[42] Ben Lovejoy, "Apple Quietly Removes All References to CSAM Scanning, but Says Nothing Has Changed," *9 to 5 Mac*, 2021, https://9to5mac.com/2021/12/16/apple-quietly-removes-all-references-to-csam-scanning/.
[43] Abelson et al., "Bugs in Our Pockets: The Risks of Client-Side Scanning."
[44] Lovejoy, "Apple Quietly Removes All References to CSAM Scanning, but Says Nothing Has Changed"; Hearn, "Facebook Admits Encryption Will Harm Efforts to Prevent Child Exploitation."
[45] Kate Garbers et al., "Impact of Mobile Technology for Survivors of Modern Slavery and Human Trafficking: A Mixed Method Study," 2021, https://www.unseenuk.org/wp-content/uploads/2021/10/FINAL-Unseen-BT-Evaluation-report_Technology-report_17MAY.pdf.
[46] Jessie Brunner, "Getting to Good Human Trafficking Data. Everyday Guidelines for Frontline Practitioners in Southeast Asia," 2018, https://humanrights.stanford.edu/publications/getting-good-human-trafficking-data-everyday-guidelines-frontline-practitioners.
[47] Abelson et al., "Bugs in Our Pockets: The Risks of Client-Side Scanning."
[48] Lovejoy, "Apple Quietly Removes All References to CSAM Scanning, but Says Nothing Has Changed."
[49] Tegan Insoll, Anna Ovaska, and Nina Vaaranen-Valkonen, "ReDirection Survey Report: CSAM Users in the Dark Web," *Protect Children*, 2021, https://protectchildren.fi/2021/09/23/redirection-survey-report/.
[50] The Lucy Faithfull Foundation, "FOR PEOPLE TROUBLED BY THEIR SEXUAL THOUGHTS ABOUT CHILDREN AND YOUNG PEOPLE," n.d., https://www.lucyfaithfull.org.uk/get-support-support-for-those-concerned-about-thoughts.htm.

Protect Children however indicate that around 50% of their respondents wanted to continue to view CSEA material. It has been suggested that media and education campaigns that aim to teach both perpetrators and potential victims of the risks and consequences associated with CSEA could be useful.[51] However, the Centre of Expertise on Child Sexual Exploitation note that the potential number of CSEA offenders far outweighs the capacity of current rehabilitative services.[52] Protect Children also suggest the need for more in-depth analysis to gain deeper insight into the thoughts, feelings, and behaviour of CSEA material users.[53]

Offender therapy and more holistic methods can help contribute to the reduction of users of online CSEA material and are favourably viewed. However, there is little chance that these solutions alone can deal with the problem of abuse material online, as they rely too much on people wanting to make a change and only work to target the demand for CSEA, rather than its supply.

Further research

The debate around E2EE will continue, with seemingly little sign of compromise between the four key stakeholders highlighted in this report. Before the anti-trafficking community can take a definite position on this situation certain areas need to be explored further.

Firstly, the impact of online reporting hotlines needs to be explored in more detail. One criticism of E2EE comes from its potential to greatly reduce reports made to reporting hotlines. However, some may consider this less consequential if reports are not adequately investigated by law enforcement – and make little difference in terms of addressing both the demand and supply of CSEA material. A large focus of reporting hotlines is on the removal of CSEA material, however it is unclear whether this has a tangible impact on the supply of material, or just on its accessibility.

It should also be questioned whether E2EE will push users away from mainstream platforms. The darkweb is already considered a hotspot for illegal activities, and platforms operated outside of the US and Europe are more challenging to regulate. Those involved in the production and consumption of CSEA material have a vested interest in maintaining their anonymity and privacy, [54] and ending E2EE could just move perpetrators onto less regulated services.

The extent to which measures can be widely enforced is also unclear and needs to be explored. The internet has long provided the infrastructure for users to circumvent and subvert restrictions imposed by governments on access to certain platforms and pages, and there is little evidence to suggest that those committed to remaining anonymous and communicating privately will not find the means to continue to do so.

The response of large technology companies must be considered before any changes implemented. These have previously resisted approaches from government and law enforcement to break their privacy policies. Apple for instance refused to provide access to the phones of those who perpetrated the San Bernardino shooting in 2015.[55]

While there is substantial media and public attention focused on this issue and CSEA, there should also be additional emphasis put on funding services and interventions which help to address these issues within current legislative frameworks.

[51] Derek Perkins et al., "Interventions for Perpetrators of Online Child Sexual Exploitation: A Scoping Review and Gap Analysis," *Centre for Expertise on Child Sexual Abuse*, 2018, https://www.csacentre.org.uk/documents/online-cse-interventions/.
[52] Perkins et al.
[53] Insoll, Ovaska, and Vaaranen-Valkonen, "ReDirection Survey Report: CSAM Users in the Dark Web," 18.
[54] Steel et al., "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders," 9.
[55] Stepanovich and Karanicolas, "Why An Encryption Backdoor for Just the 'Good Guys' Won't Work."