ARISE The Frontline of Abolition

Written evidence submitted by Arise Foundation (OSB0198)

The Digital Supply Chain and Online Sexual Exploitation of Children (OSEC)

ABOUT ARISE

Arise is an anti-slavery NGO working across the world to protect communities from exploitation. We believe that local groups and their networks hold the key to ending slavery and human trafficking. Arise provides funding and training to frontline groups, build anti-slavery networks, commission relevant research, amplify frontline voices and advocate for change.

SUMMARY

The draft Online Safety Bill aims to establish a regulatory framework for online safety, addressing both harmful and illegal content. A primary focus of the Bill lies with ensuring the safety of children, namely the distribution of child sexual abuse material and any other illegal activity that threatens the safety of children, in addition to preventing children from accessing material that is inappropriate.

It is well documented that child sex offenders often use the internet to view and share child sexual abuse material online. Understanding the role that the digital supply chain plays in the Online Sexual Exploitation of Children (OSEC) will allow for better regulation of the internet, putting provisions in place for companies to take effective steps to keep their users safe.

The current conversation surrounding suggested recommendations for the Bill have been centred on the topics of privacy[1], free speech,[2] and the spread of misinformation[3] on social media platforms.

We believe that this Bill offers a rare opportunity to address the long neglected issue of the digital supply chain, and make our approach to value chain transparency consistent between the physical and digital worlds.

INTRODUCTION

Just as the clothing you wear is the end product of a long supply chain—from farm, to factory, to fashion—the videos, photos, files you view and share online are also products of a supply chain; a digital one. The clothing supply chain has multiple stages, dotted around the world. Raw materials are grown, harvested and processed, made into garments which are sent to distributors, and then to vendors, to finally be bought and worn by consumers. Awareness of and concern about the exploitation that can occur in supply chains like these, such as forced labour, and sweatshops, has grown in recent years. In 2015, the UK Government introduced section 54 of the Modern Slavery Act.[4] This Act requires some commercial organisations to produce an annual statement, detailing the measures they have taken to ensure that slavery and human trafficking is not taking place at any point in its supply chains, or in its own business. It places both a disclosure and transparency obligation on organisations, requiring them to make the requisite facts (demonstrating an avoidance of modern slavery) both publicly available, and easily accessible and intelligible.

[1] https://www.openaccessgovernment.org/online-safety-bill-poses-threats-to-encryption/118481/

[2] https://www.bbc.co.uk/news/technology-57569336

[3] https://www.cnbc.com/2020/12/15/uk-online-harms-bill-tech-giants-face-big-fines-and-blocked-sites.html

[4] https://www.legislation.gov.uk/ukpga/2015/30/section/54/enacted

The recent draft Online Safety Bill looked to impose a duty of care on websites hosting user-generated content (including social media sites) to their users. It would require providers of these services to do more to tackle online harm, including the spread of child sexual exploitation abuse material (CSAM). It also invoked users 'right to freedom of expression, and would introduce greater protections for journalism and democratic political debate.[5]

Regulating the Internet is no easy task. It transcends borders, and cuts across some of the most complex and contentious political and social issues we face today. While many campaign for privacy rights and free speech to be upheld online, the rates of online sexual exploitation of children are on the rise.[6] Although increasingly effective technologies have been developed to fight OSEC, at a legislative level many players in the Internet supply chain are not held responsible for the abuse and exploitation their services enable.

A central problem facing any attempt to address OSEC is the tension between the greater protections needed to address it and privacy rights. In this report, we will address this tension, and make the case for more extensive Internet regulations to combat OSEC. We will begin by explaining the digital supply chain. We will then outline the exploitation that occurs on it—namely, OSEC, and the production and distribution of Child Sexual Abuse/Exploitation Material (CSAM/CSEM). We will set out possible approaches to regulating it. After addressing concerns about privacy, we will make some recommendations related to the draft Online Harms Bill.

THE DIGITAL SUPPLY CHAIN

Information moves through the Internet as packets of data. This data is transmitted digitally, along optical fibre cables that run along sea beds and across continents, between "'point[s] of presence"'[7] – devices connected to the Internet. Each node of this vast, global network is identified by a unique string of numbers – an IP address. Like a postal address, IP addresses can tell you the origin of a packet of data, and its destination. A file you send from your computer will be linked to the IP address assigned to that computer, and it will go to the computer associated with the destination IP address. Similarly, a URL is the address for a website.

For this exposition of the digital supply chain, we will use the example of a video, recorded digitally and sent from one computer to another.

Packets of data begin their journey through the digital supply chain at a source—some supplier of information on the Internet. This supplier could be an individual sending out a video from their laptop, or a big server that many individuals are connecting to to access this video.[8]

Content is produced and captured in digital format; on a camera, or a smartphone. It is then uploaded onto a computer, and compressed to allow it to be stored and transmitted via broadband. If this digital media is hosted on a website, it may also be subject to quality control and digital asset management (publishing rights, or copyright).

---

[5] https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

[6] https://www.iwf.org.uk/news/%E2%80%98definite-jump%E2%80%99-as-hotline-sees-50-increase-public-reports-of-online-child-sexual-abuse-during

[7] Zittrain, J. (2003) 'Internet Points of Control', *Boston College Law Review,* 44 (2): p.656.

[8] A server is essentially a computer programme, often run on large computers that many users can connect to, that provides a particular service to users. For example, when you go to a website on your web browser, you connect (over the internet) to a web server which pulls up the website you want. Web servers store IP addresses, and contain all a website's data and run the software for it. Similarly, you connect to a media server to stream a video, or an email server to send and receive emails.

Next, the video (or packet of data) passes through the Internet Service Provider (ISP) to which the source computer is connected. An Internet Service Provider connects computers, or other devices, to the Internet, transmitting digital signals carried by fibre optic cables through a router which provides internet connection, either through wires or wirelessly. In this way, the ISP acts as the gateway to the Internet.

The video then travels through the "middle"[9] of the Internet. This virtual space, sometimes referred to as 'the cloud', is where multiple, smaller networks and ISPs come together to 'logically construct the single Internet'.[10] Here, the video is passed between ISPs until it reaches the ISP linked to its destination—the recipient computer to which the ISP is connected. The video is then processed by this 'destination ISP'.[11] Finally, it is transmitted from the ISP to the IP address to which it was sent. Behind this IP address is another individual who has either requested, or is simply receiving this packet of data from the sender.

ONLINE EXPLOITATION

At any one time, around 750,000 people are looking to engage with children in sexual activities online.[12] Children make up one third of internet users worldwide.[13] During the pandemic, remote schooling has meant that children are spending more time online than ever. The Internet Watch Foundation (IWF) reported a 50% increase in the number of reports of child sexual abuse online during the first lockdown period in 2020, compared to the same time the previous year.[14] IWF also

> OSEC Definition: The production, for the purpose of online publication or transmission, of visual depictions (e.g., photos, videos, live streaming) of the sexual abuse or exploitation of a minor for a third party who is not in the physical presence of the victim, in exchange for compensation.
>
> Child Sexual Exploitation Material (CSEM): Any visual or audio representation of minors (under 18) engaged in sexual activity or of minors engaging in lewd or erotic behavior recorded, produced and/or published to arouse the viewer's sexual interest. Child sexual abuse material (CSAM), which depicts the contact sexual abuse of a child, is a subset of CSEM.

recorded 8.8 million attempts by UK internet users alone to access child sexual abuse materials during April 2020.[15] This is an acceleration of a trend that had already emerged prior to the pandemic.[16]

This is a global problem that transcends national borders and jurisdictions. Indeed, the IWF has highlighted that much of the illegal content accessed by individuals in the UK is hosted on URLs in other countries. Following the publication of the government's Online Harms White Paper in April 2019, IWF pointed out that, although the legislation proposed was significant, it only applied to the

---

[9] Zittrain, J. (2003) 'Internet Points of Control', *Boston College Law Review,* 44 (2): p.656.

[10] Zittrain, J. (2003) 'Internet Points of Control', *Boston College Law Review,* 44 (2): p.656

[11] Zittrain, J. (2003) 'Internet Points of Control', *Boston College Law Review,* 44 (2): p.657

[12] https://www.end-violence.org/safe-online

[13] https://www.end-violence.org/safe-online

[14] https://www.iwf.org.uk/news/%E2%80%98definite-jump%E2%80%99-as-hotline-sees-50-increase-public-reports-of-online-child-sexual-abuse-during

[15] Greierson, J. 'Watchdog reveals 8.8m attempts to access online child abuse in April', *The Guardian*, 20 Mat 2020, accessed at https://www.theguardian.com/society/2020/may/20/watchdog-reveals-88m-attempts-to-access-online-child-abuse-in-april

[16] IJM, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society ' (2020), p.64

UK.[17] The facilitators and perpetrators of child sexual abuse and exploitation are many miles away, far beyond the reach of the UK law enforcement. International Justice Mission (IJM) published a report last year on OSEC in the Philippines—'the largest known source of OSEC cases'[18] in the world. It found that the typical 'customers 'were older, Western men.[19]

FIGHTING OSEC

Given this explanation of the digital supply chain, there are three main points at which regulation and monitoring could be implemented.

1. *The source of the data*

Victor Julian, co-founder of the Underground Child Foundation (UCF), argued that the key to finding and prosecuting facilitators of OSEC, and protecting victims, is collaboration with local law enforcement and organisations on the ground.[20] In this respect, offline solutions may well be the most effective and sustainable.

Terres des Hommes developed Sweetie—a computer-animated young girl that was operated by Victor Julian for several years. Sweetie is used to communicate with and identify sexual predators online.[21] While it is effective in exposing perpetrators, and revealing the shocking scale of the demand for CSAM, it has not led to many more prosecutions. As Julian explained, Sweetie was operated by civilians, so the information gathered could not be used by law enforcement as legitimate evidence with which to prosecute offenders; it merely pointed them towards the possible perpetrators. Tilburg University produced a report detailing these legislative challenges faced in using investigative technologies such as Sweetie.[22]

At UCF, Julian still uses virtual agents like Sweetie to identify and locate victims and facilitators of OSEC. However, once victims and facilitators have been found, the focus of their work moves offline. UCF collaborates with NGOs and local authorities and organisations in source communities to raise awareness of the dangers of OSEC, build resilience and rescue both victims and those at risk. Julian pointed to poverty as the main driving factor that results in children falling victim to OSEC. Facilitators of OSEC are often relatives of the child, or friends of the family, and their incentives are predominantly financial.[23] [24]

2. *The destination*

---

[17] Internet Watch Foundation (2019) Annual Report, p.4, accessed at https://www.iwf.org.uk/sites/default/files/reports/2020-04/IWF_Annual_Report_2020_Low-res-Digital_AW_6mb.pdf

[18] IJM, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society ' (2020), p.12

[19] IJM, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society ' (2020), p.52.
Also DeMarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation. NatCen Social Research Final Report

[20] Interview with Victor Julian, 24th June 2021.

[21] https://www.terredeshommes.nl/en/programs/sweetie

[22] Schermer, B.W., Geogrieve, I, Van der Hof, S and Koops, B-J (2016) 'Legal Aspects of Sweet 2.0', *Tilburg University*.

[23] IJM, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society ' (2020), p.12.

[24] IJM, 'Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society ' (2020), p.56/

Computers or smartphones can block or filter out CSAM online. These disruptive technologies can be implemented at the level of the browser. A browser is the programme on your computer that allows you to access websites. Popular browsers include Google Chrome, Firefox, Safari and Microsoft Edge. Blocks and filters can be installed in web browsers by individual users, meaning that illegal content and websites that host it will not show up in search results. However, leaving it up to the individual to install these does little to prevent access to those who are actively seeking out CSAM.

Google and Microsoft implemented blocking technology, disrupting searches for images of sexual abuse. This reduced the number of these searches by 67% over the course of a year, compared to a non-blocking search engine.[25] While it is possible for filtering software to be built directly into web browsers,[26] this is neither a legal requirement nor an industry norm. IWF found that 'dedicated sexual abuse websites'[27] that were blocked by most browsers could be accessed via the Tor browser which preserves users 'anonymity. Even Google 'returns 920 million videos on a search for "young porn"'.[28]

Victor Julian pointed to the possibility of pre-installing filters into devices themselves. He suggested that child-friendly smartphones could be created, with pre-installed age-verification technologies and other filters that would prevent children being groomed and exploited online (in the absence of a facilitator).

Microsoft has created PhotoDNA, a technology which detects and reports abuse images.[29] This has been used by organisations such as the National Centre for Missing and Exploited Children (NCMEC) and the Internet Watch Foundation (IWF) to block and remove CSAM online. Technologies such as PhotoDNA and Sweetie are very effective, but costly, which has limited their scalability.

3. Internet Service Providers

Regulation can also be directed towards the middle of the digital supply chain—ISPs. As the conduit for packets of data travelling between users, connecting suppliers and consumers to the Internet, and also hosting online content (acting as Online Service Providers), ISPs are a key 'part of the distribution chain of child-abusive material'.[30] ISPs can filter content, or block access to IP addresses.

In the UK in 2013, default blocking of websites associated with containing illicit content, including pornography, was implemented by four major ISPs: BT, Sky, TalkTalk and Virgin Media.[31] However, customers were free to opt-out of this, resulting in an average of just 13% of new customers taking up the offer.[32] Among the customers who accepted the filtering, there were complaints of both over- and under-blocking. In some instances, websites offering support services for rape and domestic abuse victims were blocked.[33] At the same time, between 5-35% of adult content continued to get past parental controls.[34]

---

[25] Koukopoulos, N. and Quayle, E. (2018) 'Deterrence of Online Child Sexual Abuse and Exploitation', *Policing*, 13 (3): p.353.

[26] Zittrain, J. (2003) 'Internet Points of Control', *Boston College Law Review,* 44 (2): p.669.

[27] Internet Watch Foundation, 'Annual Report 2020'

[28] Kristof, N, 'The Children of Pornhub', *The New York Times,* 4 December 2020.

[29] https://www.microsoft.com/en-us/photodna

[30] Eneman, M. (2010) 'Internet service provider (ISP) filtering of child-abusive material: A critical reflection on its effectiveness', *Journal of Sexual Aggression,* 16 (2): p.226

[31] BBC News, 'Online pornography to be blocked by default, PM announces', 22 July 2013.

[32] Ofcom, 'Ofcom Report on Internet Safety Measures', 22 July 2014.

The possibility of over-blocking has led to one of the main objections levelled against ISPs filtering and blocking content—that it is a form of censorship, and 'a threat to important civil liberties such as freedom of expression'.[35] It is important that there is full disclosure and transparency about which IP addresses are blocked by ISPs, and why. In the UK, the IWF is responsible for compiling the list of IP addresses to be blocked by ISPs. This argument is part of the wider debate that has arisen from the tension between online privacy rights and the monitoring and controls needed to combat OSEC.

WOULD THIS BE THE BEGINNING OF THE END FOR INTERNET PRIVACY?

In recent years, privacy rights have been the focus of Internet regulation and the debates surrounding it. The introduction of GDPR in 2018 was a watershed moment for data protection, Facebook's CEO has been held to account on the global stage for violating his users 'privacy rights. Most recently, Apple has come under criticism for changes to its operating systems which attempt to address the balance between privacy and protection.[36] These changes have introduced two new features: CSAM detection for photos stored in iCloud, and 'Communication safety in Messages'[37] which scans images sent or received via Messages on any child account. Concerns have been raised about the apparent 'backdoor'[38] this creates—jeopardising the privacy of users 'messages and photos.

Apple has been quick to emphasise the safeguards it has in place to allay fears that authoritarian governments could exploit this loophole in Apple's encrypted services.[39] A question-and-answer document reassures Apple customers that the CSAM detection 'is designed to keep CSAM of iCloud Photos without providing information to Apple about any photos other than those that match known CSAM images',[40] and that Apple cannot gain access to communications as a result of the new safety feature for Messages.

This debate highlights a tension fundamental to Internet regulation—between privacy and protection. The former invokes the right to personal autonomy, to be free from monitoring and control, and the right to freedom of expression and opinion. But in centring arguments around these rights, the fundamental human rights underpinning protective Internet regulations risk being overlooked. The freedom of the individual is the cornerstone of any democracy. However, for democracy to work, the individual must sacrifice some freedoms so other rights can be upheld, and society can function. Your right to freedom from coercion is balanced against the right of *everyone* to be free from coercion (ergo we accept that murderers should be jailed). The right to freedom of expression stops at hate speech.

Similarly, our right to privacy cannot be illimitable. In the case of OSEC, a balance must be struck between preserving privacy and upholding the rights of the child. The UN Convention on the Rights

---

[33] Vincent, J., 'Abuse Support and Sex Education Sites Blocked by ISP's 'Porn Filters'', *The Independent,* 19 December 2013.

[34] Hörnle, J. (2014) 'Protecting children from hardcore adult content online', *Oxford University Press Blog*, accessed at https://blog.oup.com/2014/01/protecting-children-from-hardcore-adult-content-online/

[35] Eneman, M. (2010) 'Internet service provider (ISP) filtering of child-abusive material: A critical reflection on its effectiveness', *Journal of Sexual Aggression,* 16 (2): p.224.

[36] McKinney, I. and Portnoy, E., 'Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life', *Electronic Frontier Foundation*, 5 August 2021.

[37] https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf

[38] McKinney, I. and Portnoy, E., 'Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life', *Electronic Frontier Foundation*, 5 August 2021.

[39] BBC News, 'Apple defends new photo scanning child protection tech', 9 August 2021.

[40] https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf, p.2

of the Child sets out every child's basic human right to protection from violence, abuse, neglect and exploitation.[41] Those who resist the regulation and monitoring needed to stop the continued proliferation of OSEC must acknowledge that, to insist on their privacy rights in this way, is also to deny the children appearing in these images and videos their own right to privacy.[42] Put simply, failing to prevent access to OSEC is a failure to respect the basic human rights of children across the globe. As Apple has tried to show, increasing online protections does not by any means entail an end to user privacy.[43] In the ongoing debate around Internet regulation, it is important to remember that 'a privacy solution must be balanced with the reality that many members of the public use the internet for illegal and abusive conduct'.[44]

[41] Articles 19 and 36, UN Convention on the Rights of the Child.

[42] Article 16, UN Convention on the Rights of the Child.

[43] https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf

[44] https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

RECOMMENDATIONS

- Place a statutory duty upon ISPs, browser developers and others to take all reasonable steps to prevent the transmission of CSAM/CSEM through their services. Where such companies which fail to make reasonable adjustments to their services to ensure this duty is fulfilled, a claim against them can be made.
- Create a statutory offence for companies which knowingly allow for the transmission of CSAM/CSEM through their services.
- Increase funding for the UK Council for Child Internet Safety to enable it to better monitor and investigate efforts to end OSEC.
- Increase funding for civil society organisations specialising in detecting and/or preventing OSEC.
- Place upon relevant companies a duty to publish a CSAM/CSEM Statement - a reporting obligation[45] for ISPs and browser developers to make public the steps they have taken to prevent the transmission of CSAM/CSEM through their services. Regulatory bodies and/or civil society organisations should also be free to request further information from the digital service providers, which should be obliged to provide it.
- Giving a regulatory body (possibly the UK Council for Child Internet Safety) responsibility for oversight and enforcement of statutory duties. This body should have investigative powers, such that if an ISP or browser developer is said to not be meeting its obligations as set out in (e.g. Online Harms Bill) then it can investigate it, and set out a list of required actions to be implemented within a specified time frame to remedy its shortcomings. If an organisation fails to comply, it will face fines and criminal penalties (such as company disqualification).

Prepared by: Eliza Baring and Jaya Pathak

28 September 2021

[45] https://www.allenovery.com/en-gb/global/news-and-insights/publications/mandatory-human-rights-due-diligence-laws-the-netherlands-led-the-way-in-addressing-child-labour-and-contemplates-broader-action