Uncovering and Overcoming Offender Tactics for Distributing Child Sexual Abuse Material on File-Hosting Services

Kelly Barker, Katelin H.S. Neufeld, Jacques Marcoux, and Oleksandr Podprugin

Abstract. File-hosting services play a major role in facilitating the online distribution of child sexual abuse material and child sexual exploitation material (CSAM/CSEM). For example, hundreds of file hosts across the globe have received millions of removal notices issued by the Canadian Centre for Child Protection since 2018. Yet no known research has investigated how offenders exploit file hosts for CSAM/CSEM distribution purposes, or the characteristics of the services they exploit. To address these gaps, we thematically analyzed offenders' posts on 15 Tor-based child sexual abuse and exploitation forums (Study 1) and quantified the characteristics of 93 clear web file hosts known to have hosted CSAM/CSEM (Study 2). Results bring to light several tactics offenders use to distribute CSAM/CSEM stored on file hosts, including sharing tutorials on how to safely upload CSAM/CSEM, "link protection" methods to hide CSAM/CSEM from automated detection (e.g., encryption, altering URLs), and creating Tor-based file hosts designed to store CSAM/CSEM. They have also created Tor-based web applications where offenders can employ all these tactics at once. Further, results demonstrate that offenders tend to use file hosts that facilitate easy, anonymous, and enduring distribution. As such, offenders preferred file hosts that retain files for long periods of time, accept archive files, allow uploads originating from the Tor network, and do not require that users enable JavaScript. These findings highlight several platform design risk factors and point to data-driven, practical, and cost-effective measures that policymakers and online service providers (including file hosts and the Tor Project) can implement to reduce the availability of CSAM/CSEM and the revictimization of children and survivors.

doi:10.54501/jots.v3i2.287

1 Introduction

In 2021, our organization, the Canadian Centre for Child Protection Inc. (C3P) released a report detailing the availability of online child sexual abuse material and child sexual exploitation material, or "CSAM/CSEM"[1] (C3P 2021). CSAM/CSEM refers to any image, video, or other recording of a child being sexually abused or exploited, and includes depictions of sexual assault, bondage, or bestiality (C3P 2016; Salter et al. 2025). The report found that Project Arachnid, a victim-centric set of tools that combat the proliferation of CSAM/CSEM, had detected 5.4 million of these images from 2018 to 2020, leading to the issuance of millions of removal notices to over 760 online service providers. One service provider stood out, hosting *nearly half* of the detected media: a file-hosting service[2] (a type of website that allows users to upload, store, and retrieve files remotely) operated by French telecommunications giant Free.

Why was Free's service hosting so much CSAM/CSEM? It's likely that several characteristics made this file host especially attractive to offenders who wanted to distribute CSAM/CSEM (C3P 2021). Users could upload very large files for free, and they could do so while masking their IP address through the use of the Tor network without the need to create an account or provide any identifying information about themselves. Then, they could generate download links to their uploaded files that could be shared with anyone, with the ability to password protect the file. Project Arachnid found a significant number of these download links and passwords for accessing the files on dark web forums dedicated to child sexual abuse and exploitation. Free's lack of responsiveness to Project Arachnid's content removal requests suggests there was little-to-no content moderation by the website administrators, and thus files often remained available online indefinitely.

Things drastically changed after our organization's report (C3P 2021) and international news coverage (Dawkins 2021a) publicized details about Free's role in facilitating the distribution of CSAM/CSEM online. Mere days later, Free deleted all files C3P had previously reported to them and began only allowing file uploads from registered accounts belonging to their internet service customers. As *Forbes* reporter Dawkins (2021b) put

1. Throughout this paper the term "child sexual abuse material" or "CSAM" is used when referring to images that meet or are likely to meet a criminal law threshold across multiple jurisdictions—that is, images that are often referred to as "child pornography" in criminal law in many countries. In contrast, the term "child sexual abuse material and child sexual exploitation material," or "CSAM/CSEM" refers to a broader range of imagery associated with child sexual abuse. This category includes child sexual abuse material. It also includes images depicting children that do not appear to meet a criminal law threshold across multiple jurisdictions but may nonetheless violate an online service provider's Terms of Service, violate the privacy or safety of a child, or be associated with child sexual abuse or exploitation. Examples of child sexual exploitation material include: images from a known sexual abuse video where the child is still clothed or semi-clothed that is taken during the progression of the sexual abuse; images of children in bathing suits taken from social media accounts, then distributed on websites dedicated to the sexualization of children; sexualized content of children that includes images where there is an attempt to portray adult sexual positions or acts that suggest the sexual availability of the child.

2. For brevity, we use the term "file-hosting services" to also encompass image-hosting services and cyberlockers. Popular mainstream file-hosting services include Dropbox, Google Drive, and Flickr. For clarity, peer-to-peer ("P2P") file-sharing services are typically neither websites nor cloud-based and are therefore not considered file-hosting services.

it, "the service was now useless to pedophiles—most of whom are likely not Free home internet customers, while those who are [customers] would risk making themselves known to law enforcement by displaying their IP address."

These events demonstrate the powerful role file hosts can play in both facilitating and mitigating the distribution of CSAM/CSEM. Although it is established that offenders use file-hosting services to store and distribute CSAM/CSEM (C3P 2021; IWF 2025), we are unaware of research that has detailed the ways offenders do so, or the characteristics of the services they use. The goal of this report is to address these gaps, and in turn, generate knowledge that will help curb the distribution of CSAM/CSEM and victimization of survivors. We first provide context on the online distribution of CSAM/CSEM broadly and then the role of file hosts and dark web forums specifically.

1.1 Online distribution of CSAM/CSEM

CSAM/CSEM has a substantial impact on the lives of survivors. Survivors have shared how these records of abuse can result in ongoing trauma (Leonard 2010; Martin 2016). Many feel they are revictimized each time someone views the abuse material (Leonard 2010), and others worry that a viewer will recognize them (C3P 2017, 2024; Gewirtz-Meydan et al. 2018). In some cases, survivors have been recognized and then further victimized in person or online, including being stalked, doxed, or physically or sexually abused (C3P 2017, 2024).

These physical and psychological impacts of CSAM/CSEM can be intensified when the material is widely circulated online. Indeed, the widespread adoption of largely unregulated online spaces has facilitated the mass distribution of CSAM/CSEM (C3P 2024). Whereas offenders once traded physical photos and videos in person or through the mail, they can now trade electronic files using a wide range of online services, including social media, forums, content delivery networks, adult pornography sites, peer-to-peer networks, and file-hosting services (Bissias et al. 2016; Brown 2023; C3P 2021; NCMEC 2024; Salter and Richardson 2021; Steel et al. 2020; Westlake 2020).

1.2 The role of file-hosting services and the Tor Network in CSAM/CSEM distribution

1.2.1 File-Hosting Services

File-hosting services play a key role in the online CSAM/CSEM distribution ecosystem. C3P's 2021 analysis of Project Arachnid data found that, even when excluding images that had been hosted by Free, file hosts accounted for the vast majority of online service providers to whom Project Arachnid sent removal notices (C3P 2021). Relatedly, since at least 2009, file hosts have consistently been among the top online services where the UK's Internet Watch Foundation ("IWF" hotline) finds child sexual abuse material (e.g., IWF 2010, 2012, 2016, 2018, 2023); in 2024, file hosts accounted for 93% of their found

child sexual abuse material (IWF 2025).[3] Moreover, in 2025, Ofcom, the UK's media and communications regulator, launched investigations into seven file-hosting services over the possible failure to prevent the upload of child sexual abuse material (Ofcom 2025). Although file hosts exist on both the clear and dark web, evidence suggests offenders tend to use those on the clear web to store child sexual abuse material (Salter et al. 2025), with some preferring "bulletproof" file-hosting services, which have "little to no restrictions on what kind of content can be hosted on their site, that do not, and are not required to, cooperate with law enforcement" (US Dept. of Justice 2023, 7).

Once an offender has uploaded CSAM/CSEM onto a file host, they may create a link to the material and share it widely across a number of online communities whose users in turn may view, download, store, and further distribute the material, even if the original file is removed from a file-hosting site (US Dept. of Justice 2023; WeProtect 2021). Often, offenders share these links on popular child sexual abuse and exploitation forums on dark web networks (US Dept. of Justice 2023), such as the Tor network (C3P 2021; Salter et al. 2025).

This practice of distributing CSAM/CSEM by sharing download links on Tor-based forums that point to clear web file-hosting services is especially problematic, as a single download link shared in a forum can be accessed and downloaded by a potentially unlimited number of users. Often, the number of times any given file behind a link is accessed or downloaded is only known by the file-hosting service's administrators. However, a study of one Tor-based child sexual abuse and exploitation forum found that 94% of its members, translating to 90,934 members, had attempted to download CSAM/CSEM using a link shared on the forum (Bruggen et al. 2022). This finding highlights the potential for significant distribution and re-distribution of CSAM/CSEM as a result of link sharing within these online communities.

1.2.2 The Tor Network

Short for "The Onion Router," Tor is an open-source privacy network operated by the Tor Project, Inc., a US-based not-for-profit, and is among the most popular dark web networks (Levine and Lynn 2020). The Tor Project distributes software called the Tor Browser, which masks the origin of server traffic and provides anonymity for both the user and the website or service being accessed. This anonymity is achieved by routing traffic through a volunteer-operated, multilayered network (composed of what are known as "nodes" and "relays") on the Tor network.

3. Note that the statistics from Project Arachnid and IWF do not represent the totality of CSAM/CSEM on the internet, but rather the media found and/or reported by each entity. For example, Project Arachnid does not crawl most major social media platforms, due to their closed or semi-closed designs—often described as "walled gardens" because only the provider controls access to data (C3P 2021). The extent to which these online services are used to facilitate CSAM/CSEM distribution cannot generally be independently measured due to their closed nature; however, mandatory reporting obligations in some key jurisdictions, such as the US, do result in a degree of transparency about the volume of intercepted material. We do not believe the measurability limitations of CSAM/CSEM across online ecosystems have an effect on this research, as the objective of this study is to assess risk factors and characteristics of certain file-hosting services, and not to establish or compare the scale of the CSAM/CSEM distribution across various online mediums.

The Tor network contains Tor-based websites (often referred to as "hidden services" or "onion services") that are only accessible through Tor-enabled browsers such as the Tor and Brave browsers. These browsers also enable users to anonymously access clear web sites. When using the Tor network to access the clear web, the website being visited by the user does not know the true IP address of the user; rather, it can only see the Tor IP address of the final relay (also called an "exit node"). In this form of use, the Tor Browser functions somewhat like a virtual private network (VPN). For these reasons, the identities of Tor network users, including Tor-based website administrators and hosting providers, are largely masked (for a discussion of Tor software security vulnerabilities, see Levine and Lynn (2020)).

There are legitimate uses of the Tor network's anonymity function, which include facilitating whistleblowing, anonymous communication with journalists, circumventing censorship in repressive countries, and enhancing privacy (Minárik and Osula 2016). That said, many Tor users leverage anonymity protections for illegitimate criminal purposes, including crimes related to CSAM/CSEM (Levine 2022; Liggett et al. 2020). In fact, prior research has estimated that the majority (over 80%) of the traffic directed to Tor-based websites is related to sexual abuse, typically involving children (Owen and Savage 2016), and that one-fifth of Tor-based websites share child sexual abuse material (Nurmi et al. 2024). Recent numbers published by C3P (2025) showed that since 2017, Project Arachnid has identified 44,336 unique Tor-based websites that have directly hosted more than 2.85 million images or videos of CSAM/CSEM. Additionally, Project Arachnid has found 29.9 million images or videos of confirmed or suspected CSAM/CSEM that were hosted on clear web file-hosting services, but were promoted on Tor-based websites through link sharing.

Many such websites are forums created by offenders to build communities that normalize and are dedicated to exchanging child sexual abuse and exploitation information and material. In addition to sharing CSAM/CSEM, or links to it, offenders in these communities share links to other such forums, provide advice on how to abuse and exploit children, and distribute pedophilia-related news and research (Gannon et al. 2023; Kokolaki et al. 2020; US Dept. of Justice 2023). They discuss how they would like to further abuse survivors of child sexual abuse material and share information about these survivors, such as current photos of them, their real names, and where they live (Salter et al. 2025). Most notably, offenders on these forums also share best practices regarding file hosts and CSAM/CSEM distribution, such as which characteristics to look for or avoid when selecting a file host to use (Kokolaki et al. 2020; US Dept. of Justice 2023). Nonetheless, no known research has investigated this phenomenon in depth.

1.3 The current research

To better understand file-hosting services' role in distributing CSAM/CSEM, we sought to answer two main research questions: (1) What are the tactics offenders use to distribute CSAM/CSEM stored on file hosts, and (2) What are the characteristics of file hosts that

offenders use to distribute CSAM/CSEM? To do so, we studied offenders' posts on Tor-based child sexual abuse and exploitation forums and documented characteristics of 93 file hosts known to have hosted CSAM/CSEM. Based on these insights, we present recommendations for governments, file hosts, and the Tor Project, among others, that could significantly reduce the distribution of CSAM/CSEM and victimization of survivors.

2 Study 1: Offenders' preferred file-hosting services and tactics for distributing CSAM/CSEM

In this study, we analyzed offenders' posts on Tor-based child sexual abuse and exploitation forums to gain insight into their preferred characteristics of file-hosting services and the tactics they employ for distributing CSAM/CSEM using file hosts.

2.1 Method

In addition to crawling Tor-based child sexual abuse and exploitation forums in search of CSAM/CSEM links, Project Arachnid also has a built-in feature that archives and enables review of forum posts (i.e., discussions between offenders) in a controlled environment, free of images or other media. This environment provides a comprehensive and near real-time view into several of the most serious child abuse forums on the internet, while protecting researchers from exposure to images and videos.

As part of our approach, we searched the forum archives to find references to the use of file-hosting services for CSAM/CSEM distribution. The resulting analytic sample consisted of posts offenders made on 15 forums archived by Project Arachnid between 2018 and 2025. These forums are focused on extreme forms of child sexual abuse. For instance, one was dedicated to the sexual abuse of infants, and we observed discussions of such abuse across several other studied forums. Disturbingly, a number of these forums had hundreds of thousands of registered members. Consistent with our goal of better understanding offenders' experiences using file-hosting services to distribute CSAM/CSEM, we took an experiential qualitative approach (Braun and Clarke 2013) wherein we focus on their understandings and practices (as opposed to, say, using their claims as the basis of empirical tests). The first author reviewed and thematically analyzed (Braun and Clarke 2006) these forum posts and refined the themes through several rounds of discussion with the second author. The themes were further refined based on input from the other authors, who have technical and frontline expertise in online CSAM/CSEM distribution and removal.

To protect CSAM/CSEM survivors, we do not provide offender usernames and forum names, which often describe child sexual abuse or include the names of real survivors. Similarly, we do not provide the names of file hosts or other tools offenders use to distribute CSAM/CSEM. We have observed offenders discussing and sharing insights from

various research studies on Tor-based child sexual abuse and exploitation forums.

2.2 Results

Members of the studied offending communities were highly motivated to provide fellow offenders with long-term, reliable access to CSAM/CSEM. They understood that the moment a CSAM/CSEM file is uploaded to a file-hosting service, there is a risk that the file will soon be inaccessible. In some cases, CSAM/CSEM becomes inaccessible because a file host removes it upon learning it is CSAM/CSEM, either through their own content moderation or through external reports from the public, law enforcement, hotlines, or child protection organizations. To avoid such file loss, the offenders on the studied forums curated and communicated lists of file hosts that forum members should and shouldn't use to distribute CSAM/CSEM, as well as tactics to distribute CSAM/CSEM on the forums. Much of this advice had the dual goal of preventing law enforcement from identifying the offender.

2.2.1 File-hosting characteristics offenders prefer and avoid for CSAM/CSEM distribution

Many of the studied Tor-based forums maintained lists of file-hosting services their members should and should not use for distributing CSAM/CSEM. Though the exact terminology varied, these lists typically categorized file hosts as "preferred," "not preferred," and "banned." These lists exclusively contained non-mainstream and lesser-known file-hosting services—some of which would fall under the classification of bulletproof file-hosting services. In fact, the use of mainstream file-hosting services (e.g., Dropbox, Google Drive) was strongly discouraged: Offenders recognized that some of these services use moderation tools to detect and block the upload of CSAM/CSEM and send tips to law enforcement and child protection agencies, often under legal mandatory reporting obligations.

On these lists, offenders often noted the key characteristics of each file host that led to its categorization. Within and across the studied forums, there was general agreement on these characteristics, with one notable exception: Using Tor-based file hosts to distribute CSAM/CSEM was highly contested.

Characteristics of preferred file-hosting services. Offenders tended to prefer file-hosting services with characteristics that facilitated CSAM/CSEM distribution and prolonged its online availability. Most often, these included file hosts with "long" or "good" file-retention periods, which were often dependent on user traffic: A CSAM/CSEM file would remain available online if other offenders visited or downloaded it, and if not, the file would expire and no longer be available. Typically, offenders were satisfied with retention periods of at least one to three months, as stated by this offender:

> "[File host][4] retains files for 3 months without downloads, which is pretty much best in class among the current popular hosts."

Offenders also valued fast upload and download speeds as well as maximum file size, typically 500 mb or more. They also preferred file hosts that allowed offenders to upload archive files, a type of file that can contain many compressed files. Doing so enables offenders to upload sections of large videos and collections of images that would otherwise surpass a file host's maximum allowed file size. This offender explains the additional benefits of uploading archive files:

> "Sometimes, a file is so large that it's impractical to put it into only one compressed file [...]. That's where multi-part downloads come in handy!! For example, if a video is 1GB, it can be separated into four 250MB compressed files, allowing for quicker and easier downloading with less chance of failure."

Another preferred file host characteristic was the ability to rename files. An offender might have a file-naming system for CSAM/CSEM files they store on their personal devices that conflicts with the file-naming rules of the forum where they intend to share the download link. Being able to rename files directly on the file host saves offenders the time and work of making a local copy of a file, changing the file name (to adhere to the rules of the forum where they'd like to share it), uploading the file to the file host, and then deleting the copy from their device. Renaming the file in a way that is not explicit, obvious, or well-known to law enforcement can also help avoid detection. Though many offenders do not use this countermeasure for child sexual abuse material stored on clear web (Guerra and Westlake 2021) or dark web (Westlake and Guerra 2023) sites dedicated to hosting or displaying CSAM/CSEM, offenders on the studied forums instructed and even mandated this of their members:

> "The best way to help your files stay up longer without extraordinary means like (assuming anti's[5] don't report) is to: Use file names that are completely irrelevant. Name them as if you are sharing recipes, vacation photos, technical specs, really anything other than what it is."

Characteristics of "not preferred" file-hosting services. On Tor-based child sexual abuse and exploitation forums, offenders also described characteristics of their "not preferred" file-hosting services. Generally, these were file hosts that created barriers to uploading CSAM/CSEM and required more time and effort to upload and download files. These file hosts had shorter retention times than preferred file hosts and, in some cases, limited the number of times a file could be downloaded. Offenders deemed some of these file hosts unreliable in that the services would often display various error codes (e.g.,

4. We've redacted the names of file hosts, as explained in sections 2.1 and 3.1.
5. This is a term that online child sexual abuse offenders use to refer to groups and individuals who work against them to disrupt the online distribution of CSAM/CSEM.

bad gateway errors). Other characteristics of not preferred file hosts were Captchas[6] and the blocking of some, but not all, Tor traffic.

Captchas are a routine and often frustrating experience for users of the Tor Browser because clear web sites have difficulty determining if a user of the Tor Browser is a human, or automated traffic (Tor Project, n.d.-a). Offender posts confirmed that clear web file hosts frequently require users of the Tor Browser to solve Captchas, sometimes many in a row. One offender expressed frustration with having to solve "over 15 Captchas," for example.

In the view of offenders, another file host characteristic that created a barrier for CSAM/CSEM distribution was blocking some, but not all, Tor traffic. However, offenders explained how they circumvent these blocks with relative ease:

> "Use **"New Tor Circuit for This Site"** located in the Tor Menu, or **Ctrl+Shift+L**. This will solve the error messages and forbidden messages."

> "After changing Tor exit node, try visiting [file host] again to see if it works. You might have to repeat this a few times, until you arrive at a Tor exit node that is not blocked by [file host]."

Although the above characteristics created barriers to uploading and accessing CSAM/CSEM, offenders were willing to endure these when file hosts with "preferred" characteristics were inaccessible. This was not true of all file host characteristics, though.

Characteristics of banned file-hosting services. On the Tor-based child sexual abuse and exploitation forums we studied, "banned" file-hosting services generally had one or more characteristics that could threaten an offender's anonymity. Because these offenders were dedicated to using the Tor Browser to help mask their identity, any file host that blocked traffic from the Tor network was banned. It is important to note that online service providers can distinguish Tor from non-Tor web traffic by referring to the real-time exit node IP address list, which is made available by the Tor Project on their website (Tor Project, n.d.-b). When a file host blocked only some Tor traffic, offenders could reconnect to the file-hosting service by creating a new Tor circuit for themselves, which would effectively allocate them a new source IP address on a new Tor exit node using a simple keyboard shortcut or browser menu option (explained above). However, these circumvention methods were ineffective on file hosts that kept their blocklist up to date with the current list of Tor exit nodes.

File hosts could also be banned if they required payment for uploads and downloads or required the use of JavaScript, as these characteristics also compromise an offender's anonymity. Payment processors may require and collect identifying information about an

6. Captchas are online tests that assess whether traffic to a website is human or not and prevent automated traffic from accessing the website (IBM, n.d.).

offender, such as their name and home address, and accessing a website that requires enabling JavaScript could expose identifying information about an offender's device, including its IP address—even if they are using the Tor Browser.

To avoid having to constantly re-upload files, studied forums also banned offenders from sharing links to CSAM/CSEM on file hosts that had an extremely short file-retention period, anywhere from hours up to a couple of days.

Sharing a link to CSAM/CSEM stored on a file host with one or more of these characteristics could result in the offender's post being reported or removed, or the offender being reprimanded by the community:

> "Please upload to a host that doesn't require JavaScript. I've removed your link."

> "[This post was] removed for using a pay [file] host. This is not allowed. Use only approved file hosts."

> "This host blocks Tor connections and who would trust just using a VPN unless you love wearing handcuffs???"

Offenders generally agreed on the characteristics of file-hosting services that facilitated or created barriers to uploading CSAM/CSEM, and the characteristics that ought to be avoided for security reasons. However, we observed one characteristic that caused notable disagreement across and within forums.

Tor-based file-hosting services. Analyzed posts indicated that the use of file-hosting services on the Tor network was a polarizing topic. Some of the studied forums banned these services, whereas others named them among their preferred file hosts. And within forums that did not have a stance on Tor-based file hosts, members were often debating the merits of these file hosts.

Typical arguments against using Tor-based file hosts for storing CSAM/CSEM pertained to their instability, smaller storage size, and slower speeds relative to clear web services:

> "[Tor-based file hosts] are simply not that reliable. Both uploads and downloads tend to be extremely slow and unstable. And [Tor-based file hosts] tend to be short lived, with many shutting down after a couple of months at most."

> "Basically [Tor-based file hosts] don't have the same capacity and don't scale as well as clearnet [file] hosts, has much more limited storage, bandwidth etc."

For some offenders, though, these costs of using Tor-based file hosts were outweighed by their benefits. The Tor network is designed to anonymize the identity of its users,

including website administrators. This means there is minimal risk that administrators of Tor-based file hosts will have harmful or illegal online activities that occur on their services traced back to them. Also, Tor-based file hosts typically do not have Terms of Service, nor do they provide any contact information, making it impossible to report abusive content. As one offender explained it:

> "As quite few [Tor-based file hosts] have no contact information, this means content can't be reported by White Knights[7] and thus cannot be taken down by them."

Whereas some Tor-based file hosts allow any content (legal or illegal), others are designed for hosting illegal content, some even for CSAM/CSEM specifically. Below, an offender highlights the benefits of using such a file host:

> "Hi everyone!
> I have fantastic news to share with you. A new Tor-only file host has been introduced to our community. This new host has some neat features that will definitely come very handy for us girl|boy lovers.
>
> - The host doesn't block or remove [child sexual abuse material].
> - The host is a hidden service, accessible only on Tor, making it hard for [law enforcement authorities] to shut down.
> - The download speed is very high, so it will match the top speed of your Tor browser."

Offenders who endorsed Tor-based file hosts recognized that, compared to clear web file hosts, CSAM/CSEM was less likely to be removed from Tor-based file hosts because they have limited or no reporting options, and their administrators are typically anonymous and can't be made to remove CSAM/CSEM. CSAM/CSEM therefore tends to stay on Tor-based file hosts for a long time, exacerbating risks and harms for survivors whose abuse material is available on these services.

Regardless of whether the studied forums allowed or banned the use of Tor-based file hosts, Tor-based child sexual abuse and exploitation forums' lists of file hosts helped ensure their members had access to a wide selection of file hosts with their preferred characteristics; one of the observed lists had 60 preferred file hosts. Once an offender had selected a file host, their offending community also provided advice on how to best distribute the CSAM/CSEM and preserve its availability.

7. This is another term that online child sexual abuse offenders use to refer to groups and individuals who work against them to disrupt the online distribution of CSAM/CSEM.

2.2.2 Tactics offenders use to distribute CSAM/CSEM using file-hosting services

On the forums we studied, offenders worked to ensure mutual access to CSAM/CSEM on file-hosting services. They did so by sharing tutorials on relevant countermeasures, which are ways to hide their activities or identities from detection. They also engaged in countermeasures when uploading or sharing links to CSAM/CSEM on file hosts, including creating multiple points of access to CSAM/CSEM and protecting links from being detected and processed by automated tools. Some offenders even created bespoke web applications to streamline these processes.

Tutorials. Nearly all studied forums had a tutorials section, with many related to file-hosting services. A common theme in these tutorials was how to "safely" share CSAM/CSEM on the forum, such as by obscuring an offender's identity. In these tutorials, offenders continually emphasized the importance of using the Tor Browser to remain anonymous while offending online. On top of being the only way to access Tor-based child sexual abuse and exploitation forums, most offenders regarded the Tor Browser as a necessary operational security measure when using file-hosting services. For example, one offender's tutorial advised:

> "If you're ever uploading anything directly to clearnet (i) only ever do it using Tor Browser and (ii) never turn on JavaScript to be able to use a site (many clearnet sites will require this e.g., to push an 'upload' button)."

Other forum tutorials also provided advice on how to disable and circumvent JavaScript requirements and explained how to use virtual machines and operating systems that operate only in volatile memory, a type of temporary computer memory that loses all stored data when the power is turned off (e.g., random access memory, or "RAM").

Another safety tutorial theme was countermeasures that hide CSAM/CSEM from detection and access. These tutorials provided detailed instructions on how to prepare files for upload onto a file-hosting service, including file-naming conventions to prevent the service from identifying the files as containing CSAM/CSEM. Tutorials also described how to share the download links in ways that would obscure the CSAM/CSEM from automated detection tools, such as how to password protect and encrypt files.

Other tutorials were narrowly focused on one aspect of a particular file host, with titles like, "How to download files on [file hosting service]," wherein offenders shared lessons learned to help others navigate a file host's unique characteristics (e.g., how to navigate file hosts in a different language). Tutorials also explained how to upload files that exceeded a file host's maximum file size (such as archive files, explained later) and troubleshoot common issues—all toward the goal of ensuring CSAM/CSEM remained available for the community on file-hosting services.

Mirror files and multi-upload sites. Another offender tactic for prolonging the availability of CSAM/CSEM on file-hosting services is to upload the same file onto multiple file hosts and share their unique download links ("mirrors") in a forum post. Doing so ensures that a CSAM/CSEM file is accessible in multiple locations. Offenders can create mirrors by uploading the same content onto several file hosts, one at a time. Far more efficient, though, is to use a clear web multi-upload website. Here users can simultaneously upload the same file onto several clear web file hosts. One clear web multi-upload site[8] that offenders frequently mentioned enabled users to upload content on more than 40 file hosts at once.

Forum administrators and members alike expected members to create and share mirrors of CSAM/CSEM files. The simplest reason was that if an offender "click[s] a link and it's dead or fails to load due to greater forces, the user might go back to the post and choose one of the alternative options." Another benefit of mirrors is that they help offenders minimize time spent re-uploading previously shared content, which one offender suggested could instead be devoted to uploading new content:

> "I recommend using multiple file hosts. Links are actively reported by the anti-[child sexual abuse material] script kiddies, and some just go offline for a while, or even permanent. If you spend all your time refreshing old links, you have no [time] left to upload other content, that maybe 1000 users here may have not yet seen."

By ensuring that CSAM/CSEM files had multiple access points, mirrors helped mitigate the chances of files being removed from the internet: Compared to when a file is uploaded on only one service, significantly more automated efforts and resources are required to detect this material and send removal notices to all file-hosting services.

Link protection. Some organizations (e.g., C3P) operate automated detection tools that crawl Tor-based forums to check whether posted URLs link to CSAM/CSEM, including CSAM/CSEM stored on clear web file hosts. To do this, automated tools often need to access the URL string (i.e., the direct path address to a web page). When these tools find CSAM/CSEM at a URL, the content is reported to an entity such as the hosting provider, website administrator, or law enforcement, which may result in the content being removed from a file host. Offenders on the studied forums were well aware of this possibility, and encouraged using "link protection"—their term for methods that make it difficult for automated tools to detect URLs in forum posts or determine if they link to CSAM/CSEM—to guard against it:

> "Link protection systems exist to prevent the use of bots crawling the forum and mass reporting links. They were implemented on [a child sexual abuse and exploitation forum] when German journalists used a script to scrape and report links. Since then, they have become a fundamental part of any [child

8. We've redacted the names of online services and tools, as explained in sections 2.1 and 3.1.

> sexual abuse and exploitation] forum. They cannot stop human link reporters, and they are not designed to."

> "Without link protection, one with malicious intent could just deploy a [automated detection tool] which gathers every unprotected link and then report them to [law enforcement authorities] or the file host."

Offenders discussed their main methods of link protection: encryption, password-protected archives, hyperlinks, Captchas, and altering URLs. These methods were used individually and in combination.

URL encryption appeared to be the most robust and relied-upon method of link protection. Offenders used third-party websites on the clear web and Tor network to encrypt CSAM/CSEM download links shared in their forum posts. To access these files, offenders must decrypt the URL address, such as by using the corresponding decryption key or a third-party decryption website. This is a popular countermeasure because decrypting URL addresses is a difficult task for automatic detection tools. Across studied forums, offenders continually underscored the utility of encrypting links:

> "Both [law enforcement authorities] and anti's use automated scripts to scan [child sexual abuse and exploitation forums] for links, then report the links in bulk to file hosts. encrypting links with a tool like [Tor-based encryption tool][9] prevents such scripts from working."

Archives often required a password to access the content. Offenders shared CSAM/CSEM download links to password-protected archives alongside a password hint—often based on offender knowledge—in the same forum post. One offender posted a victim's photo and hinted, "the password is the victim's name," for example. Typically, automated detection tools cannot decipher the clue to a password, let alone use the password to access the archive file.

Offenders also used various types of Captchas to add barriers to automated tools detecting and reporting CSAM/CSEM download links in their forum posts. Because Captchas are designed to distinguish between human users and automated activity, when they are used to "protect" CSAM/CSEM download links they can outright block certain automated tools from accessing these links.

Another link protection measure used by offenders is to take basic steps to avoid displaying the full CSAM/CSEM download link URL in plain text (e.g., https://wikipedia.com) on a forum. Instead, they will make the URL available by hyperlinking text that is not a URL (e.g., Wikipedia). This strategy, while generally unsophisticated, is based on the presumption that some automated detection tools are only designed to seek URL strings in plain text, and not designed to find URL text within its HTML code (shown in the example above). Whereas some automated detection tools

9. We've redacted the names of online services and tools, as explained in sections 2.1 and 3.1.

will skip the URL in the HTML code and miss the CSAM/CSEM, a human will recognize they can click on the hyperlinked text and access the CSAM/CSEM.

Offenders also altered the URLs for CSAM/CSEM download links in their forum posts. They added decoy characters to, or removed characters from, the URL and shared instructions for reconstituting the intended URL (e.g., "Remove all Chinese characters"). When an automated detection tool encounters an altered URL, it is directed to a webpage that does not contain CSAM/CSEM. Rather, a webpage may display a 404-error response code ("Page not found"), for example.

Several offenders deployed automated link protection systems. For example, an offender created a link protection plug-in that appeared to be used by members of different child sexual abuse forums. This plug-in allowed offenders to Captcha-protect, hyperlink, and encrypt links to CSAM/CSEM shared in their forum posts. By automating link protection and using multi-upload sites, offenders streamlined the process of accessing and distributing CSAM/CSEM—a process further streamlined by Tor-based multi-function web applications.

Multi-function web applications. On the Tor network, offenders have created multi-function web applications that one offender aptly described as a "pedo Swiss Army Knife." These web applications were created to increase capacity for various aspects of the CSAM/CSEM distribution process as well as making removal of CSAM/CSEM more complex. If an offender isn't using a multi-function web application, this process likely involves multiple steps on several different websites, such as first uploading CSAM/CSEM onto a clear web file-hosting service or multi-upload site, followed by encrypting the links on either a clear web or Tor-based website, and then sharing the links on a Tor-based forum. In contrast, offenders who use a multi-function web application can accomplish these steps (and more) in one place, and without leaving the anonymity and relative safety of the Tor network.

Offenders said that multi-function web applications can be used to upload CSAM/CSEM files onto, or download CSAM/CSEM files from, clear web file hosts, even those that use JavaScript or block Tor traffic, as they are able to circumvent these design characteristics. As a result, these web applications provided offenders with the ability to directly upload content onto file hosts that would otherwise be avoided or even banned. One offender explained the benefits of using these applications to download content: "JavaScript is needed for most download sites. That's why you use [multi-web application]. I never have JavaScript on and I download whatever I want." Multi-function web applications can also encrypt and decrypt CSAM/CSEM download links and help offenders translate their or others' forum posts to various languages.

We learned of three distinct multi-function web applications. One of these was embedded directly on a Tor-based child sexual abuse and exploitation forum, enabling offenders to upload CSAM/CSEM, protect the links, and share it on the forum. In effect, this provides a

"one-stop-shop" for offenders to share and access CSAM/CSEM. The other multi-function web applications had their own websites on the Tor network. These multi-function web application sites published guides on how to upload and download files across different file-hosting services as well as lists of proxy services that enable uploads on file hosts that block uploads from Tor.

2.3 Discussion

Offenders on the 15 studied Tor-based child sexual abuse and exploitation forums had clear preferences when it came to the file-hosting services members should and shouldn't use to host CSAM/CSEM, often enshrining these preferences in forum rules. Recommended file hosts were those that facilitated anonymous, fast, and easy distribution, such as allowing archive files and having long retention periods. Banned file hosts had characteristics that compromised offender anonymity, like blocking traffic from the Tor network and using JavaScript that offenders could not disable or circumvent. Tor-based file hosts were contentious, even banned on some of the studied forums for their slow speeds and instability relative to clear web file hosts, but recommended on other forums as it was unlikely that a Tor-based file host administrator would remove CSAM/CSEM, especially on file hosts created for the sole purpose of sharing CSAM/CSEM.

Offenders used several tactics to distribute CSAM/CSEM, all toward the goals of efficiency and making material available to their community for as long as possible. They shared tutorials on how to "safely" share and access CSAM/CSEM. They also engaged in "link protection," methods that make it difficult for automated tools to detect URLs in forum posts or determine if they link to CSAM/CSEM, including encryption, password-protected archives, hyperlinks, Captchas, and altering URLs. Recognizing that CSAM/CSEM may nonetheless be detected and removed from some file hosts, offenders would upload the same material to multiple file hosts at a time, and share unique download links (i.e., mirrors) in one forum post. Finally, to streamline the CSAM/CSEM distribution process, some offenders have created Tor-based multi-function web applications, which are websites where an offender can employ many of these tactics at once.

A potential limitation of this study and our experiential qualitative approach is that we have relied on offenders' attestations of how they use file-hosting services to distribute CSAM/CSEM, and we have not tested the veracity of each claim, strategy, or tool. However, testing these would be impractical and illegal, and would cause further harm to survivors: Tests would involve visiting the forums (not archives of their text) and not only risk researcher exposure to images and videos of child sexual abuse and exploitation, but also involve the distribution of such material. Further, in this study we observed that forum administrators, moderators, and members meticulously verify others' download links, tips, and tools, and remove or criticize forum posts using practices deemed risky or ineffective.

To those wishing to engage in similar future research, specifically a qualitative study of

offender conversations on child sexual abuse and exploitation forums, it is important to understand that doing so may present risks to researchers. In some jurisdictions, accessing written descriptions of child sexual abuse is illegal. Even if legal, immersing oneself in conversations among communities dedicated to sexually abusing children can be challenging, and includes risks of secondary traumatic stress or vicarious trauma and resultant symptoms (Berger 2021; Dickson-Swift 2022; Duran and Woodhams 2022; Guerzoni 2020). We encourage those considering undertaking similar research to carefully consider such risks and develop protocols to prevent, mitigate, and address these risks. One strategy could be to partner with organizations that are authorized to access this material and whose staff have been trained to analyze CSAM/CSEM (e.g., law enforcement, though they too may experience primary trauma due to continual immersion in CSAM/CSEM; see Rimer et al. (2025)). For further strategies, see Berger (2021), Dickson-Swift (2022), and Salter (2017).

3 Study 2: Characteristics of file-hosting services that have hosted CSAM/CSEM

The goal of this study was to describe the characteristics of clear web file-hosting services offenders use to distribute CSAM/CSEM. Such results can help deepen understandings about the types of file-hosting services that offenders gravitate toward, and in turn shape recommendations to file hosts, governments, and others wanting to reduce the distribution of CSAM/CSEM and victimization of survivors.

3.1 Methods

Our sample consisted of 93 clear web file-hosting services that have hosted CSAM/CSEM (based on Project Arachnid records) and allow users to upload files for free; we did not pay for any file-hosting services, nor did we upload any CSAM/CSEM files to conduct this study. File hosts in this sample closely resembled those described in Study 1: They were non-mainstream and lesser-known file hosts that appeared to have little to no content moderation. To minimize the possibility of pointing bad actors toward these services and causing further harm to survivors, we do not name these file-hosting services.

From 2022 to 2024, we collected observations on seven characteristics of these file hosts' free services: whether they accepted archives, required accounts for uploads, offered premium accounts for purchase, hosted third-party advertisements, and appeared to allow uploads from Tor; the maximum accepted file sizes; and the maximum storage sizes.

We determined the characteristics of most file hosts by browsing the services, including their Terms of Service and Frequently Asked Questions pages. When the service required users to create a free account to upload files, we created an account using the Tor

Browser. To understand whether the file hosts might accept uploads originating from the Tor Browser, we visited each file host three times (each visit from a new Tor Browser session) and attempted to upload an innocuous image; the image was the same across all tests. Relative to conducting one test per file host, conducting three allowed us to better assess the ability to upload from the Tor Browser and mirrors what offenders in Study 1 described doing when experiencing an upload error (see section "Characteristics of "not preferred" file-hosting services"). We calculated the proportion of file hosts that had each characteristic of interest.

3.2 Results

Table 1: Characteristics of clear web file-hosting services that have hosted CSAM/CSEM (*N* = 93)

	n	%
Accepted archives[a]	59	63
Required account for uploads	55	59
Offered premium accounts for purchase[b]	77	83
Hosted third-party advertisements[c]	65	70
Allowed uploads from Tor (of three test uploads)		
None	19	20
One	6	6
Two	5	5
Three	63	68
Maximum accepted file size		
Less than 50 mb	19	20
50 mb to 499 mb	10	11
500 mb to 1.9 gb	10	11
2 gb to 3.9 gb	13	14
4 gb and up	30	32
Unknown	11	12
Maximum storage size		
Less than 10 gb	6	6
10 gb to 59 gb	21	23
60 gb to 1,024 gb	20	22
Unlimited	19	20
Unknown	27	29

[a] We could not determine whether two file hosts accepted archives. [b] We could not determine whether one file host offered premium accounts for purchase. [c] We could not determine whether 11 file hosts hosted third-party advertisements.

The vast majority of the 93 file-hosting services offered premium accounts in addition to their free services (83%) and had advertisements on their website (70%). Nearly two-thirds of file hosts accepted archive files (63%). Most file hosts required that users create an account to upload files (59%), though we were able to make all accounts

anonymously and at no financial cost.

Our results indicate that most file hosts did not block all uploads from the Tor network: We were able to successfully make all three test uploads on two-thirds of the file hosts from our free accounts or as fully unregistered users (68%). Moreover, we were able to make at least one upload on 79% of the file hosts. When an upload failed, we usually received a message stating that uploads from the Tor network were not allowed or that they had blocked the (Tor) IP address we were connected to (in the remaining cases, we received other error messages).

The studied file hosts had a wide range of maximum accepted file sizes and storage space for their free services. For the file hosts that listed a maximum file size, the maximum ranged from 5 mb to 307 gb, with over half (57%) of file hosts accepting files larger than 500 mb, which offenders in Study 1 noted to be a favorable size. Of the file hosts that indicated their maximum storage space, it ranged from 5 mb to 1,240 gb; 19 file hosts provided unlimited storage space at no cost.[10]

3.3 Discussion

We analyzed the characteristics of 93 free file-hosting services that offenders have used to store CSAM/CSEM, based on Project Arachnid records.

In general, these file hosts had many characteristics that would be appealing to those wanting to host and distribute illegal content, such as CSAM/CSEM. Although most studied file hosts required users to create an account to upload files, we were able to do so without providing verifiable identifying information, such as a credit card or driver's license, meaning it was easy to anonymously create accounts to upload files for free. The studied file hosts also allowed users to upload and store large files; 46% of file hosts accepted files sized 2 gb or larger, for example. Moreover, most file hosts accepted archive files, which can contain compressed files that may otherwise surpass the file host's maximum allowed file size (e.g., videos, large collections of images).

We were also able to upload files from the Tor browser on most file hosts. In fact, 68% of the file hosts allowed us to upload files through three different Tor exit nodes, suggesting they likely do not block in real-time all active Tor exit nodes based on IP address. Of course, these results are not definitive, as the number of Tor exit nodes used in our testing represents a small proportion of the total exit nodes.

Consistent with offenders' experiences noted in Study 1, there were a few file hosts that blocked one or two of our three test uploads from the Tor Browser. This seeming inconsistency could be due to file hosts attempting to block Tor traffic, but doing so using

10. We conducted an exploratory test to evaluate whether a statistical relationship exists between free unlimited storage space and hosting third-party advertisements. A Fisher's exact test was not statistically significant (p = .99). This may be because no effect exists, or because a small effect exists but we lacked adequate statistical power to detect it, given our small cell sizes (e.g., only four file hosts did not host third-party ads and did not offer unlimited storage space) and small sample size.

outdated lists of Tor exit nodes, which are continuously updated. It is also possible that a file host previously blocked particular Tor exit nodes, not because they were Tor IP addresses, but because the service had previously determined that activity from that specific Tor IP address violated their Terms of Service and therefore blocked it.

70% of the file hosts studied displayed third-party advertisements. Given that website administrators monetize user traffic through ad revenue, and that all these services have hosted CSAM/CSEM, it is possible that the administrators have generated ad revenue from CSAM/CSEM-related traffic. We also found that most file hosts were seeking to generate revenue by offering premium or paid services, which may include revenue from accounts that store and share CSAM/CSEM.

Together, these findings illustrate some of the common characteristics of clear web file hosts that offenders have used to host CSAM/CSEM, and point to recommendations for file hosts, governments, and others wanting to help curb the distribution of CSAM/CSEM and further harm to survivors, discussed in the following section. Future researchers may wish to investigate the relationship between file host characteristics (alone and in combination) and the amount of CSAM/CSEM (found) hosted on a file host, as well as whether file host characteristics relate to one another (e.g., whether a file host offers free unlimited storage space and hosts third-party advertisements; see footnote 10).

4 General discussion

The goal of this research was to better understand how offenders leverage file-hosting services to store CSAM/CSEM and share it with other offenders, and the characteristics of these services. Toward this goal, we analyzed the characteristics of 93 clear web file hosts on which offenders have stored CSAM/CSEM, as well as offender conversations on 15 Tor-based child sexual abuse and exploitation forums. Offenders' preferred file hosts tended to have characteristics that facilitated easy, anonymous, and enduring distribution, such as long file-retention periods, allowing traffic from the Tor network, and allowing uploads of archive files. Common tactics offenders used to distribute CSAM/CSEM on file hosts centered on efficiency and ensuring material was online for as long as possible. This included uploading the same CSAM/CSEM to multiple file hosts at once and using several methods to prevent automated detection tools from detecting their distribution URLs or the linked CSAM/CSEM (e.g., encryption, altering URLs). Offenders have even created Tor-based multi-function web applications, which enable offenders to accomplish many of these tactics simultaneously.

This paper makes several important contributions to the scholarly literature. It is the first known work to detail CSAM/CSEM offenders' preferred file-hosting service characteristics and their tactics for distributing CSAM/CSEM on these services; often, these tactics are countermeasures to help evade or hinder efforts of child protection agencies, law

enforcement, and others aiming to remove CSAM/CSEM from the internet. We also add to the growing body of research documenting the intersections of the Tor network and child sexual abuse material (e.g., Biryukov et al. 2014; Faizan and Khan 2019; Gannon et al. 2023; Guitton 2013; Insoll et al. 2024; Nurmi et al. 2024; Owen and Savage 2016; Salter et al. 2025; Terbium Labs, n.d.), by, for instance, noting that offenders have begun using Tor-based websites to build CSAM/CSEM-dedicated file hosts and websites that make CSAM/CSEM distribution faster and less prone to detection and removal.

Accordingly, findings from both studies also have practical implications in that they provide insight into measures that may help curb the distribution of CSAM/CSEM and victimization of survivors. The following section presents data-driven recommendations for the Tor Project, file hosts, and governments.

4.1 Policy implications

4.1.1 The Tor Project: Tor-based websites

The Tor Project frames its core mandate as the defense and promotion of human rights to privacy and freedom by providing free, anonymous, and uncensored access to the internet (Tor Project 2019). However, the Tor Project's ongoing technical support for Tor-based websites (i.e., onion services) are arguably antithetical to this mandate. As Guitton (2013, 2812) puts it:

> Hidden services act as a protector of unethical content rather than as the promoter of a censor-free place for ethical content. By looking closely into it, one notices that Tor hidden services are mainly used to evade law enforcement agencies, but not from non-democratic states, but from liberal ones with laws that have strong moral and ethical grounds.

Indeed, many Tor-based websites grossly violate CSAM/CSEM survivors' rights to privacy and safety by enabling offenders to continually distribute child sexual abuse material and survivors' personal information (Salter et al. 2025).

Echoing others (Guitton 2013; Levine and Lynn 2020), we contend that the benefits of Tor-based websites do not outweigh the harms and rights violations they facilitate and, consequently, the Tor Project should cease development work on Tor-based websites on their network. We would add that if the Tor Project continues to support the creation of Tor-based websites ("onion services"), they should develop safeguards to minimize child abuse and exploitation (for specifics, see Owen and Savage (2015)). These proposals would not fundamentally undermine the core function of the Tor network, which is to navigate the internet anonymously.

4.1.2 File-hosting services and other online service providers

Our findings indicate that simple, practical, and cost-effective measures could make file-hosting services less vulnerable to the upload of CSAM/CSEM. While our study focused on file hosts, the following measures are applicable to many other online services that allow the upload of user-generated content, such as the multi-upload sites discussed in Study 1.

To reduce the risk of their services being used by CSAM/CSEM offenders, we recommend that online service providers use proactive and reactive measures. Proactive measures, such as automated image hash detection tools, help ensure that when offenders attempt to upload known CSAM/CSEM onto services, it is immediately blocked and never made accessible to other users. Reactive measures are those that provide a second line of defense when CSAM/CSEM goes undetected by proactive measures (for more information, see C3P (2024)).

Another measure is to take steps to block or discriminate against certain actions, such as the upload of user-generated content from anonymous users who mask their identity. This can include those using anonymity browsers (e.g., the Tor Browser) and virtual private networks (VPNs), both of which are routinely misused by bad actors to carry out online abuse (C3P 2021; eSafety Commissioner 2025; Levine 2022). Indeed, offenders in Study 1 frequently cited the importance of the Tor Browser for uploading CSAM/CSEM because it allowed offenders to do so while masking their identity and location. In fact, restricting uploads from anonymization networks, like Tor, has been identified as a best practice for reducing the risk of having offenders exploit online services for the purpose of child sexual abuse material distribution (Project Arachnid 2026). Some website administrators have reported that doing so decreased the amount of child sexual abuse material uploaded onto their services (see also Krawetz 2016).

The Australian Signals Directorate (2021), for example, proposes a tiered risk management strategy for services. They recommend blocking Tor traffic as the first line of defense against malicious Tor traffic, for reasons that extend beyond online child sexual exploitation. However, they state that if there is evidence that blocking Tor traffic could limit access from a significant number of legitimate users, a service could instead closely monitor Tor traffic and subject it to additional layers of scrutiny.

An indirect measure file hosts can use to combat the upload of CSAM/CSEM is requiring the user to enable JavaScript in order to functionally use a website. Although Study 1 found that some offenders use tools that allow them to circumvent JavaScript, requiring that JavaScript be enabled would nonetheless deter other offenders from uploading and downloading CSAM/CSEM. To illustrate, a file host could require users to solve a JavaScript Captcha before accessing upload and download functions. As shown in Study 1, this measure would deter some users from uploading CSAM/CSEM—not specifically because of the Captcha itself, but because of the requirement to use JavaScript to

complete the Captcha, which could expose information about an offender's device, such as an IP address

To further shield their services from being used to store CSAM/CSEM, file hosts could adopt robust "know your client" (KYC) practices, such as user-verification policies. In practice, this would guard against offenders using file hosts with complete anonymity and prevent those who have previously uploaded CSAM/CSEM from creating new accounts. Our findings underscore the importance of KYC practices: Studied offenders weren't deterred from using file hosts that required an account, so long as an account could be created without providing any personal or identifiable information. File hosts that lack such practices may wish to consider significantly limiting the services available to unverified users. This could include limiting file-retention periods and offering minimal storage space, for example.

File hosts could also prohibit uploading password-protected archive files from anonymous users. Our research found that CSAM/CSEM offenders highly valued this characteristic, as archive files often shield the nature of the content from file hosts and automated detection tools, decreasing the possibility of detection and therefore removal. Removal is further complicated when the archive contents are password-protected (C3P 2021). This measure is particularly important, given the volume of content that is distributed using archive file formats. To illustrate, from 2018 to 2020, Project Arachnid detected more than 18,000 archive files that contained nearly 1.1 million CSAM/CSEM files (C3P 2021).

4.1.3 Advertisers and operators of advertising vendors

Website administrators often monetize user traffic to their web services by displaying third-party advertisements to users. To do so, they typically employ a third-party advertising network to identify and place advertisements throughout the administrator's web services. This practice can generate revenue for website administrators who are hosting illegal and harmful content. For example, an investigation by Adalytics (2025) found that numerous major companies have had their ads hosted on, and thus may have financially contributed to the operation of, a free clear web file-hosting service that hosted child sexual abuse material.

In Study 2 we found that over two-thirds of file-hosting services—all of which had hosted CSAM/CSEM—displayed third-party advertisements on their websites. To prevent administrators of websites hosting illegal material (including CSAM/CSEM) from generating advertisement-driven profit, there are safeguards that advertising vendors, and the advertisers themselves, could take. Robust KYC practices can help ensure that their advertisements do not appear on websites known to host harmful or illegal content. Advertisers and vendors could, for example, take steps to confirm whether a website is known to have a history of facilitating harmful online behaviors, hosting CSAM/CSEM, or is noncompliant with requests to remove illegal or harmful content.

4.1.4 Government

Above we detailed several measures that the Tor Project, file-hosting services, advertising networks, and other online service providers can take to curb the distribution of CSAM/CSEM. While some services voluntarily adopt these measures, others may not outside of a regulatory framework that incentivizes online services to adopt risk reduction measures. As governments around the world increasingly move toward implementing legal frameworks for online safety that address, among other harms, CSAM/CSEM distribution, we recommend they adopt aspects of the above recommendations and best practices.

A concrete example of government action is the mandatory illegal content risk assessment duties for online services under the UK's Online Safety Act (*Online Safety Act* 2023). Under this framework, factors known to increase the risk of certain types of online services are identified; the ability to upload user-generated content anonymously is among the key factors. Services that report higher-risk profiles are expected to implement proportionate safety measures to mitigate the potential for online harm.

It is important to note that government regulators and law enforcement agencies continue to face an uphill compliance battle with not only bulletproof file-hosting sites specifically, but also bulletproof hosting services more generally. Hosting services provide the underlying infrastructure—servers, storage, and network connectivity—necessary for operating file-hosting services and other online services. Bulletproof hosting services often operate in parts of the world that do not have (strong) laws regarding illegal content moderation and removal. They may also ignore or refuse to comply with law enforcement requests for information about the activities of their customers (e.g., administrators operating a file-hosting service). Overcoming this constantly evolving challenge will likely require more robust international collaboration between governments and industry members (e.g., Joint Ransomware Task Force 2025).

Ultimately, governments must carefully consider and debate the trade-offs of policy decisions that shape online experiences. With regards to Tor, the technology is well-established among the suite of tools that can help individuals for whom privacy and the ability to express themselves without fear of repercussions is a priority or even a necessity. Likewise, this same technology is a tool of choice for bad actors, including CSAM/CSEM offenders. As with all technologies and policies surrounding their use and reach, we believe trade-offs must be considered within a broad and relative context, while steering clear of arguments that may pit rights or freedoms against one another in absolute terms. Jardine's (2018, 451) conclusion provides a potentially helpful framing through which governments can evaluate some facets of the trade-offs within their own borders and abroad:

> The Tor network is probably more prone to abuse in liberal countries where opportunity is the underlying driver of use than in repressive regimes where

people might only turn to the network because they need to do so. The ancillary expectation here is that the social costs and benefits to the Tor network are not evenly distributed globally (Jardine 2015). Liberal countries plausibly have to deal with relatively more of the negative implications (i.e. crime and child abuse imagery) of the technology of Tor than repressive societies. In contrast, the social benefits of Tor likely cluster disproportionately in repressive regimes.

4.2 Strengths, limitations, and directions for future research

In terms of strengths, this is the first known research to thoroughly investigate how file-hosting services have been used by offenders for distributing CSAM/CSEM and the characteristics of such services. Further, Study 1 is the first known study to report that members of CSAM/CSEM forums are making tools available on the Tor network that allow easy file upload to multiple file-hosting sites at once. Another strength of Study 1 is its data source: archived conversations among CSAM/CSEM offenders who congregate within the Tor network, many of whom were actively sharing CSAM/CSEM, clearly possess a high degree of technological skill, and were presumably not incarcerated at the time of the study. The insights garnered from this subgroup of offenders expand understandings of countermeasures offenders use to avoid having their identity revealed or CSAM/CSEM detected and removed, complementing, for instance, findings from anonymous surveys of previously convicted child sexual abuse material offenders (e.g., Steel et al. 2022, 2024).

A potential limitation of this research is our focus on free file-hosting services. In Study 2, we studied these because offenders in Study 1 preferred the anonymity afforded by free services (e.g., not having to provide a credit card). That said, some CSAM/CSEM offenders do use paid-for premium file-hosting services to distribute child sexual abuse material (Centeno 2025; ICMEC 2014; Stroebel and Jeleniewski 2015), and it is possible that these offenders use different tactics than described in Study 1 and that the premium file-hosting services have different characteristics than those described in Study 2. As such, future researchers may wish to study the tactics of offenders who prefer premium services and the characteristics of these services, such as their additional benefits (e.g., faster download and upload speeds, greater retention periods).

There are other valuable directions for future research. In particular, we encourage collaborations between researchers and file-hosting services to test whether and to what extent implementing our suggested measures decreases the amount of CSAM/CSEM found on the file-hosting service.

4.3 Conclusion

The online distribution of CSAM/CSEM violates all children's rights to privacy, safety, and freedom from this material (UN Human Rights 1989, 2000, 2021) and puts survivors at

risk for further victimization from offenders who view the recordings of their abuse (C3P 2017, 2024; Salter et al. 2025). This paper focused on how offenders congregate on Tor-based child sexual abuse and exploitation forums to share links to CSAM/CSEM stored on certain file-hosting services. Offenders' use of file-hosting services is not new: The IWF (2007) flagged this issue nearly two decades ago. Without meaningful online safety regulation, file hosts have become a major source of online CSAM/CSEM distribution. Though a longstanding and large problem, it is not an insurmountable one. Our findings point to measures that file hosts, the Tor network, and even advertising vendors can voluntarily take, or be compelled to take through online safety regulations, and create a safer internet for CSAM/CSEM survivors.

References

Adalytics. 2025. *Are Ad Tech Vendors Facilitating or Monitoring Ads on a Website That Hosts Child Sexual Abuse Material?* January. https://adalytics.io/blog/adtech-vendors-csam-full-report.

Australian Signals Directorate. 2021. "Defending Against the Malicious Use of the Tor Network," October. https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Defending%20Against%20the%20Malicious%20Use%20of%20the%20Tor%20Network%20%28October%202021%29.pdf.

Berger, Roni. 2021. "Studying Trauma: Indirect Effects on Researchers and Self – and Strategies for Addressing Them." *European Journal of Trauma & Dissociation* 5 (1). https://doi.org/10.1016/j.ejtd.2020.100149.

Biryukov, Alex, Ivan Pustogarov, Fabrice Thill, and Ralf-Philipp Weinmann. 2014. "Content and Popularity Analysis of Tor Hidden Services." In *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW),* 188–93. IEEE. https://doi.org/10.1109/ICDCSW.2014.20.

Bissias, George, Brian Levine, Marc Liberatore, Brian Lynn, Juston Moore, Hanna Wallach, and Janis Wolak. 2016. "Characterization of Contact Offenders and Child Exploitation Material Trafficking on Five Peer-to-Peer Networks." *Child Abuse & Neglect* 52:185–99. https://doi.org/10.1016/j.chiabu.2015.10.022.

Braun, Virginia, and Victoria Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101. https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.

———. 2013. *Successful Qualitative Research: A Practical Guide for Beginners.* Sage Publications Ltd.

Brown, Rick. 2023. "Eliminating Online Child Sexual Abuse Material." Chap. 4. Routledge.

Bruggen, Madeleine van der, Inge van Balen, Arthur van Bunningen, Petra Talens, Jessica N. Owens, and Karlene Clapp. 2022. "Even 'Lurkers' Download: The Behavior and Illegal Activities of Members on a Child Sexual Exploitation Tor Hidden Service." *Aggression and Violent Behavior* 67:101793. https://doi.org/10.1016/j.avb.2022.101793.

Canadian Centre for Child Protection. 2016. *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis.* https://protectchildren.ca/en/resources-research/child-sexual-abuse-images-report/.

———. 2017. *Survivors' Survey: Full Report 2017.* https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf.

———. 2021. *Project Arachnid: Online Availability of Child Sexual Abuse Material.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf.

Canadian Centre for Child Protection. 2024. *Experiences of Child Sexual Abuse Material Survivors: How Technology Companies' Inaction Leads to Fear, Stalking, and Harassment.* https://protectchildren.ca/pdfs/C3P_ExperiencesOfCSAMSurvivors_en.pdf.

———. 2025. "CSAM Distribution on Tor Is Not Inevitable; The Network's Creators Have the Power to Act," August 22, 2025. https://www.protectchildren.ca/en/press-and-media/blog/2025/tor-backgrounder.

Centeno, Loraine. 2025. "AI is Fueling an Alarming Surge of Child Sexual Abuse Material in Canada: What Parents Need to Know." *The Hamilton Spectator* (May 2, 2025). https://www.thespec.com/news/ai-in-digital-child-abuse/article_cbcd0e05-e2a5-5893-9275-b242fbd4081e.html.

Dawkins, David. 2021a. "Billionaire Xavier Niel's Telecom Giant, Free, Hosted 48% of Child Sex Abuse Imagery Found During Two-Year Investigation, Says Nonprofit Group." *Forbes* (June 9, 2021). https://www.forbes.com/sites/daviddawkins/2021/06/09/billionaire-xavier-niels-telecom-giant-free-hosted-48-of-child-sex-abuse-imagery-found-during-two-year-investigation-says-nonprofit-group/.

———. 2021b. "War of Words Erupts over How Billionaire-Owned Telecom Giant Handled Child Pornography Alerts." *Forbes* (July 23, 2021). https://www.forbes.com/sites/daviddawkins/2021/07/23/war-of-words-erupts-over-how-billionaire-owned-telecom-giant-handled-child-pornography-alerts/.

Dickson-Swift, Virginia. 2022. "Undertaking Qualitative Research on Trauma: Impacts on Researchers and Guidelines for Risk Management." *Qualitative Research in Organizations and Management: An International Journal* 17 (4): 469–86. https://doi.org/10.1108/QROM-11-2021-2248.

Duran, Fazeelat, and Jessica Woodhams. 2022. "Impact of Traumatic Material on Professionals in Analytical and Secondary Investigative Roles Working in Criminal Justice Settings: A Qualitative Approach." *Journal of Police and Criminal Psychology* 37 (4): 904–17. https://doi.org/10.1007/s11896-022-09532-8.

eSafety Commissioner. 2025. "Anonymity and Identity Shielding," February 2, 2025. https://www.esafety.gov.au/industry/tech-trends-and-challenges/anonymity.

Faizan, Mohd, and Raees Ahmad Khan. 2019. "Exploring and Analyzing the Dark Web: A New Alchemy." *First Monday* 24 (5). https://doi.org/10.5210/fm.v24i5.9473.

Gannon, Colm, Arjan A.J. Blokland, Salla Huikuri, Kelly M. Babchishin, and Robert J.B. Lehmann. 2023. "Child Sexual Abuse Material on the Darknet." *Forensische Psychiatrie, Psychologie, Kriminologie* 17 (4): 353–65. https://doi.org/10.1007/s11757-023-00790-8.

Gewirtz-Meydan, Ateret, Wendy Walsh, Janis Wolak, and David Finkelhor. 2018. "The Complex Experience of Child Pornography Survivors." *Child Abuse & Neglect* 80:238–48. https://doi.org/10.1016/j.chiabu.2018.03.031.

Guerra, Enrique, and Bryce G. Westlake. 2021. "Detecting Child Sexual Abuse Images: Traits of Child Sexual Exploitation Hosting and Displaying Websites." *Child Abuse & Neglect* 122:105336. https://doi.org/10.1016/j.chiabu.2021.105336.

Guerzoni, Michael. 2020. "Vicarious Trauma and Emotional Labour in Researching Child Sexual Abuse and Child Protection: A Postdoctoral Reflection." *Methodological Innovations* 13 (2): 205979912092634. https://doi.org/10.1177/2059799120926342.

Guitton, Clement. 2013. "A Review of the Available Content on Tor Hidden Services: The Case Against Further Development." *Computers in Human Behavior* 29 (6): 2805–15. https://doi.org/10.1016/J.CHB.2013.07.031.

IBM. n.d. "What is CAPTCHA?" Accessed April 2, 2026. https://www.ibm.com/think/topics/captcha.

Insoll, Tegan, Valeriia Soloveva, Eva Díaz Bethencourt, Anna Katariina Ovaska, Juha Nurmi, Arttu Paju, Mikko Aaltonen, and Nina Vaaranen-Valkonen. 2024. "Factors Associated with Help-Seeking Among Online Child Sexual Abuse Material Offenders: Results of an Anonymous Survey on the Dark Web." *Journal of Online Trust and Safety* 2 (4). https://doi.org/10.54501/JOTS.V2I4.205.

International Centre for Missing & Exploited Children. 2014. *Confronting New Challenges in the Fight Against Child Pornography: Considerations for Protecting Children & Your Company's Reputation When Engaging with Digital Businesses.* January. https://www.icmec.org/wp-content/uploads/2015/10/APAC-FCACP-Engaging-with-Digital-Businesses.pdf.

Internet Watch Foundation. 2007. *Annual and Charity Report 2006.* https://www.iwf.org.uk/media/0abk5xtw/2006-annual-report.pdf.

———. 2010. *2009 Annual and Charity Report.* https://www.iwf.org.uk/media/xumn3ojr/2009-annual-report.pdf.

———. 2012. *2011 Annual and Charity Report.* https://www.iwf.org.uk/media/0yghwzsg/2011-annual-report.pdf.

———. 2016. *Annual Report 2015.* https://www.iwf.org.uk/media/r2ndzbac/iwf-2015-annual-report-final-for-web.pdf.

———. 2018. *Annual Report 2017.* https://annualreport.iwf.org.uk/pdf/IWF_2017_Annual_Report.pdf.

———. 2023. *Annual Report 2022: Site Types.* https://annualreport2022.iwf.org.uk/trends-and-data/site-types/.

———. 2025. *Site Types.* https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/site-types/.

Jardine, Eric. 2018. "Tor, What Is It Good For? Political Repression and the Use of Online Anonymity-Granting Technologies." *New Media & Society* 20 (2): 435–52. https://doi.org/10.1177/1461444816639976.

Joint Ransomware Task Force. 2025. "Bulletproof Defense: Mitigating Risks from Bulletproof Hosting Providers," November 19, 2025. https://www.cyber.gov.au/sites/default/files/2025-11/Bulletproof%20Defense%20-%20Mitigating%20Risks%20from%20Bulletproof%20Hosting%20Providers.pdf.

Kokolaki, Emmanouela, Evangelia Daskalaki, Katerina Psaroudaki, Meltini Christodoulaki, and Paraskevi Fragopoulou. 2020. "Investigating the Dynamics of Illegal Online Activity: The Power of Reporting, Dark Web, and Related Legislation." *Computer Law & Security Review* 38:105440. https://doi.org/10.1016/j.clsr.2020.105440.

Krawetz, Neal. 2016. "This Is What a TOR Supporter Looks Like." *The Hacker Factor Blog* (April 14, 2016). https://www.hackerfactor.com/blog/index.php?/archives/720-This-is-what-a-TOR-supporter-looks-like.html.

Leonard, Marcella Mary. 2010. "'I Did What I Was Directed to Do but He Didn't Touch Me:' The Impact of Being a Victim of Internet Offending." *Journal of Sexual Aggression* 16 (2): 249–56. https://doi.org/10.1080/13552601003690526.

Levine, Brian. 2022. *Increasing the Efficacy of Investigations of Online Child Sexual Exploitation.* National Institute of Justice, May. https://web.archive.org/web/20220926163037/https://www.ojp.gov/pdffiles1/nij/grants/301590.pdf.

Levine, Brian, and Brian Lynn. 2020. "Tor Hidden Services Are a Failed Technology, Harming Children, Dissidents and Journalists." *Lawfare* (January 17, 2020). https://www.lawfaremedia.org/article/tor-hidden-services-are-failed-technology-harming-children-dissidents-and-journalists.

Liggett, Roberta, Jin R. Lee, Ariel L. Roddy, and Mikaela A. Wallin. 2020. "The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance,* 91–116. Springer. https://doi.org/10.1007/978-3-319-78440-3_17.

Martin, Jennifer. 2016. "Child Sexual Abuse Images Online: Implications for Social Work Training and Practice." *The British Journal of Social Work* 46 (2): 372–88. https://doi.org/10.1093/bjsw/bcu116.

Minárik, Tomáš, and Anna-Maria Osula. 2016. "Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law." *Computer Law & Security Review* 32 (1): 111–27. https://doi.org/10.1016/J.CLSR.2015.12.002.

National Center for Missing and Exploited Children. 2024. "CyberTipline Reports by Electronic Service Providers (ESP)." https://www.missingkids.org/content/dam/missingkids/pdfs/2023-reports-by-esp.pdf.

Nurmi, Juha, Arttu Paju, Billy Bob Brumley, Tegan Insoll, Anna K. Ovaska, Valeriia Soloveva, Nina Vaaranen-Valkonen, Mikko Aaltonen, and David Arroyo. 2024. "Investigating Child Sexual Abuse Material Availability, Searches, and Users on the Anonymous Tor Network for a Public Health Intervention Strategy." *Scientific Reports* 14 (1): 7849. https://doi.org/10.1038/s41598-024-58346-7.

Ofcom. 2025. "Enforcement Programme into Measures Being Taken by File-Sharing and File-Storage Services to Prevent Users from Encountering or Sharing Child Sexual Abuse Material (CSAM)," March 17, 2025. https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/enforcement-programme-into-measures-being-taken-by-file-sharing-and-file-storage-services-to-prevent-users-from-encountering-or-sharing-child-sexual-abuse-material-csam.

Office of the High Commissioner for Human Rights. 1989. "United Nations General Assembly Resolution 44/25 Convention on the Rights of the Child," November 20, 1989. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

———. 2000. "United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography," May 25, 2000. https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child.

———. 2021. "United Nations General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," March 2, 2021. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

Online Safety Act. 2023. C. 50 (UK). https://www.legislation.gov.uk/ukpga/2023/50/enacted.

Owen, Gareth, and Nick Savage. 2015. *The Tor Dark Net.* Technical report. Global Commission on Internet Governance, September 15, 2015. https://www.cigionline.org/sites/default/files/no20_0.pdf.

———. 2016. "Empirical Analysis of Tor Hidden Services." *IET Information Security* 10 (3): 113–18. https://doi.org/10.1049/iet-ifs.2015.0121.

Project Arachnid. 2026. "Best Practices for Reducing the Availability of CSAM on Internet Based Services." https://projectarachnid.ca/en/best-practices/#restrict-anon-network-uploads.

Rimer, Jonah R., Shannon Brown, Jennifer Martin, and Andrea Slane. 2025. "'Once You See It You Can't Unsee It': Law Enforcement Trauma and Immersion in Child Sexual Abuse Material." *Child Protection and Practice* 4:100085. https://doi.org/10.1016/j.chipro.2024.100085.

Salter, Michael. 2017. "Doing Trauma Research in a Sustainable Way." *Dignity: A Journal on Sexual Exploitation and Violence* 2 (1): 5. https://doi.org/10.23860/dignity.2017.02.01.05.

Salter, Michael, and Lloyd Richardson. 2021. "The Trichan Takedown: Lessons in the Governance and Regulation of Child Sexual Abuse Material." *Policy & Internet* 13 (3): 385–99. https://doi.org/10.1002/poi3.256.

Salter, Michael, Lloyd Richardson, Jacques Marcoux, Katelin H.S. Neufeld, and Kelly Barker. 2025. "The Child Sexual Abuse Material Survivor as *Homo sacer*: Bare Life Under Cyber-Libertarianism." *Journal of Gender-Based Violence* 9 (4): 598–617. https://doi.org/10.1332/23986808Y2025D000000091.

Steel, Chad, Emily Newman, Suzanne O'Rourke, and Ethel Quayle. 2020. "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders." *Forensic Science International: Digital Investigation* 33:300971. https://doi.org/10.1016/j.fsidi.2020.300971.

———. 2022. "Technical Behaviours of Child Sexual Exploitation Material Offenders." *Journal of Digital Forensics, Security and Law* 17 (1): 2. https://doi.org/10.15394/jdfsl.2022.1794.

———. 2024. "Technical Profiles of Child Sexual Exploitation Material Offenders." *Psychiatry, Psychology and Law* 31 (1): 1–14. https://doi.org/10.1080/13218719.2022.2148305.

Stroebel, Melissa, and Stacy Jeleniewski. 2015. *Global Research Project: A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges.* National Center for Missing & Exploited Children. https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/grp.pdf.

Terbium Labs. n.d. "Separating Fact from Fiction: The Truth About the Dark Web." Accessed April 2, 2026. https://web.archive.org/web/20221003195659/https://dsimg.ubm-us.net/envelope/385643/510233/The%20Truth%20About%20The%20Dark%20Web.pdf.

Tor Project. 2019. "Digital Rights are Human Rights." Tor Blog, https://blog.torproject.org/digital-rights-are-human-rights/, December 10, 2019.

———. n.d.-b. "Bulk Tor Exit Exporter." Accessed April 2, 2026. https://check.torproject.org/api/bulk.

———. n.d.-a. "Captcha." Accessed April 2, 2026. https://web.archive.org/web/20250522085314/https:/support.torproject.org/glossary/captcha/.

United States Department of Justice. 2023. "Technology." https://www.justice.gov/d9/2023-06/technology_2.pdf.

WeProtect. 2021. *Global Threat Assessment 2021.* https://www.weprotect.org/global-threat-assessment-21/#report.

Westlake, Bryce, and Enrique Guerra. 2023. "Using File and Folder Naming and Structuring to Improve Automated Detection of Child Sexual Abuse Images on the Dark Web." *Forensic Science International: Digital Investigation* 47:301620. https://doi.org/10.1016/j.fsidi.2023.301620.

Westlake, Bryce Garreth. 2020. "The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance,* 1225–53. Springer. https://doi.org/10.1007/978-3-319-78440-3_52.

Authors

Kelly Barker is a policy and research analyst at the Canadian Centre for Child Protection ("C3P"). She can be reached at kelly@protectchildren.ca.

Katelin H.S. Neufeld is a behavioural research scientist at C3P. She can be reached at katelin@protectchildren.ca.

Jacques Marcoux is director of research & analytics at C3P. As part of this role, he also engages in lobbying activities in Canada related to online safety for children. He can be reached at jacques@protectchildren.ca.

Oleksandr Podprugin is stakeholder relations manager - Project Arachnid at C3P.

Acknowledgements

We are grateful to our colleagues at C3P, whose unrelenting work toward child safety has contributed immensely to the insights of this paper.

Data availability statement

Due to its sensitive nature, Study 1 data is not publicly available. Anonymized copies of the Study 2 dataset (i.e., without file-hosting service names) may be available upon request. Please email the first author for more information.

Funding statement

This project did not receive funding.

We are disclosing that C3P receives funding from the Government of Canada, the Government of Manitoba, and the Government of Ontario. However, these funders did not directly fund the research project in our manuscript, and these funders did not review or have a say in our manuscript.

Keywords

Child sexual abuse material; child sexual exploitation material; file hosting services; file storage services; image hosting services; Tor; dark web; countermeasures.