Chapter 42

"I Need You All to Understand How Pervasive This Issue Is": User Efforts to Regulate Child Sexual Offending on Social Media

Michael Salter and Elly Hanson

Abstract

This chapter examines the phenomenon of internet users attempting to report and prevent online child sexual exploitation (CSE) and child sexual abuse material (CSAM) in the absence of adequate intervention by internet service providers, social media platforms, and government. The chapter discusses the history of online CSE, focusing on regulatory stances over time in which online risks to children have been cast as natural and inevitable by the hegemony of a "cyberlibertarian" ideology. We illustrate the success of this ideology, as well as its profound contradictions and ethical failures, by presenting key examples in which internet users have taken decisive action to prevent online CSE and promote the removal of CSAM. Rejecting simplistic characterizations of "vigilante justice," we argue instead that the fact that often young internet users report feeling forced to act against online CSE and CSAM undercuts libertarian claims that internet regulation is impossible, unworkable, and unwanted. Recent shifts toward a more progressive ethos of online harm minimization are promising; however, this ethos risks offering a new legitimizing ideology for online business models that will continue to put children at risk of abuse and exploitation. In conclusion, we suggest ways forward toward an internet built in the interests of children, rather than profit.

The Emerald International Handbook of Technology Facilitated Violence and Abuse, 729–748
Copyright © 2021 Michael Salter and Elly Hanson
Published by Emerald Publishing Limited. This chapter is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of these chapters (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode.
doi:10.1108/978-1-83982-848-520211053

Keywords: Sexual abuse; social media; children; sexual exploitation; image-based abuse; justice; self-help

Introduction

The title of this chapter comes from a tweet made by Twitter user @AvriSapir (a pseudonym) on May 1, 2020,[1] in which she describes her efforts to have videos of her own child sexual abuse removed from Twitter. In this chapter, we examine the phenomenon of internet users attempting to report and prevent online child sexual exploitation (CSE) and child sexual abuse material (CSAM) in the absence of adequate intervention by internet service providers, social media platforms, and government. With reports of online CSAM to US authorities increasing by 50% per year for the past 20 years (Bursztein et al., 2019), it is now undeniable that the structure, administration, and regulation of online services and infrastructure have created a highly enabling environment for online CSE. We discuss the history of online CSE, focusing on regulatory stances over time in which online risks to children have been cast as natural and inevitable by the hegemony of a cyberlibertarian ideology that posits a factual and normative order in which it is not only impossible to regulate the internet but where such regulation is inherently authoritarian and unethical (Hanson, 2019). We illustrate the success of this ideology, as well as its profound contradictions and ethical failures, by presenting key examples in which internet users have taken decisive action to prevent online CSE and promote the removal of CSAM. Rejecting simplistic characterizations of "vigilante justice," we argue instead that the fact that often young internet users feel compelled to act against online CSE and CSAM (CBC News, 2018; Pauls & MacIntosh, 2020) undercuts libertarian claims that internet regulation is impossible, unworkable, and unwanted. The chapter argues that scholars of online abuse and policymakers need to pay closer attention to the ways in which exploitative modes of technological design and administration and government inaction have been mystified by cyberlibertarianism and contributed to the contemporary crisis of CSE and CSAM. Recent shifts toward a more progressive ethos of online harm minimization are promising; however, this ethos risks offering a new legitimizing ideology for online business models that will continue to put children at risk of abuse and exploitation. In conclusion, we suggest ways forward toward an internet built in the interests of children, rather than profit.

The History of Online Child Sexual Exploitation

While technology companies have been vocal in their commitment to child protection, the history of online CSE shows that industry has been largely unwilling to prioritize child safety over profits, a posture that has been accepted and, arguably, tacitly endorsed by governments. The authenticity of industry and government expressions of surprise at escalating reports of online CSE and CSAM is undermined by evidence that the use of the internet by

pedophiles has been known at the highest levels since the early days of networked computing. In 1986, the US Attorney General noted that the trade in CSAM had shifted online: "recently a significant amount of the exchange has taken place by the use of computer networks through which users of child pornography let each other know about materials they desire or have available" (US Attorney General, 1986, p. 407). Nonetheless, the approach of US legislators to internet regulation has been notoriously lax and oriented toward the growth and profitability of technology companies rather than child protection. This approach is exemplified in the passage of the *Communications Decency Act* (CDA) in 1996, a pivotal moment in the development of the modern internet. Section 230 of the CDA effectively immunized online service providers against legal liability for the content uploaded or provided by their users, paving the way for an internet whose consumer appeal and business model was based on the frictionless circulation of user's preferred content. The alignment of US legislators with the financial interests of the technology sector has created a powerful bloc that has dominated internet governance for a quarter of a century (Carr, 2015).

A pervasive cyberlibertarianism played a major role in legitimizing an anti-regulation ethos within industry and government despite recognition of the likely costs to children. Hanson (2019) defines libertarianism as a "distinct political stance and moral psychology whose guiding principle is the freedom of individuals, in particular from interference by the state" (p. 4), where concern for individual liberty from control and regulation is prioritized over altruistic moral values and responsibility to others. Libertarianism and new technologies emerged from the sociopolitical foment of the 1960s and 1970s as strange but intimate bedfellows and played a formative role in the culture and practices of Silicon Valley. From the 1970s, influential American counterculturalists came to believe that networked technology was the ideal instrument for personal liberation and alternative community building (Turner, 2010). They drew in particular on the libertarian rather than socialist and collectivist strains of the counterculture in ways that framed the developing internet as a transgressive, anarchist space, a new frontier full of possibilities and free of legal regulation. This characterization has been amplified in influential fictional and futurist portrayals of the internet as a parallel disembodied universe or "cyberspace" (Salter, 2017). As the internet and technology industries have taken center stage as global corporate behemoths, their marketing has enthusiastically adopted a countercultural style and promoted the view that their products are conducive to personal and collective freedoms. This view and its encompassing anarchist mystique have been prominent in media coverage and academic analysis of new technologies, promoting an idealized view of the lawlessness of the internet as both antiauthoritarian and radically democratic, despite it being anything but (Dahlberg, 2010). As the following section makes clear, cyberlibertarianism has mystified the monopolistic capture of online technologies by select corporate giants whose platforms closely regulate and manipulate user behavior (Zuboff, 2019, p. 109).

By the late 1990s, it was evident that CSAM and CSE were expanding online at an exponential rate. The prevalence and severity of this material was such that even skeptics such as sociologist Philip Jenkins, whose prior research had argued

that community concern over child sexual abuse was characterized by "moral panic" and overreaction, would declare CSAM an escalating and intolerable crisis (Jenkins, 2001). In 2002, as investigations into and prosecutions of CSAM in the United States underscored the seriousness of the problem, then-US Attorney General John Ashcroft held a meeting with the major technology companies calling them to action. In response, they formed an industry body called the Technology Coalition with the stated mission of "eradicating online child sexual exploitation" (Farid, 2017, para. 9). For 5 years, the Technology Coalition did not develop or deploy any effective technological solutions against the spread of CSAM. The Technology Coalition served instead to signal the concerns of technology companies to government and the public in the absence of measurable action or impact.[2] It was during this period of industry abeyance that major social media platforms were established and became the dominant players online. On social media, profit maximization depends on recruiting as many users as possible to circulate content and engage with each other as much as possible; whether this content and engagement is abusive or not does not impact the bottom line. Accordingly, social media platforms have a poor track record of addressing the specific needs and vulnerabilities of children or inhibiting sexual misconduct and coercion.

Social media platforms have sought to elide their responsibilities to users by describing their platforms as neutral, apolitical "facilities," comparable to the water system or electricity grid (Salter, 2017). In this model, the risk of online CSE and the availability of CSAM are positioned as a natural artifact beyond the control of any company or government. It was only in 2008 that Microsoft partnered with Professor Hany Farid to develop PhotoDNA technology, which enables the automatic matching of images against a database of known CSAM (Farid, 2017). This technology was then provided for free to appropriate organizations in order to identify and remove known CSAM. PhotoDNA technology is widely recognized as a major turning point in the fight against CSAM, and the determining factor in the dramatic numbers of CSAM currently being notified to US authorities. PhotoDNA made it possible, for the first time, to screen all images uploaded by users to ensure they were not sharing known CSAM. Nonetheless, it took large companies such as Google as long as five years before they were willing to implement PhotoDNA on their services (Farid, 2017). Furthermore, there has been a lack of significant industry investment in the further development and deployment of the technology. For example, PhotoDNA cannot detect new images of CSAM, nor can it scan video files; a significant drawback as reports of video CSAM are now more common than images (Dance & Keller, 2020). While a new tool, PhotoDNA for Video, was developed around 2018, the extent of its use across the sector is unclear.

In 2018, both Google and Facebook launched technology designed to detect new CSAM images – this is a positive step forward although they still require screening by a human moderator, which is necessarily an expensive proposition for platforms and comes with significant risk of harm and trauma to content moderation teams (Gillespie, 2018).[3] The cost of underinvestment in human moderation is exemplified in the history of Tumblr, the social media platform and

blogging site. In November 2018, the Tumblr app was removed from major online stores, effectively preventing new users from joining the platform. It subsequently emerged that the Tumblr app was removed due to the presence of CSAM on the platform (BBC News, 2018). While Tumblr used PhotoDNA to prevent the uploading of known CSAM to the site, an audit of Tumblr content identified that the platform was being used to circulate *new* CSAM that is undetectable to PhotoDNA (Silverstein, 2018). Such material can only be identified through human moderation. In December 2018, Tumblr announced that it was banning all pornographic content from the site, using an algorithm trained to automatically detect and delete photos with nudity (Liao, 2018). Users complained that the algorithm was producing a high level of false positives, with cartoons, dinosaur images, and even pictures of food wrongly flagged as "sensitive" content (Leskin, 2019). Within a year of the ban, Tumblr's unique monthly visitors decreased by more than 20%, and the site was sold in August 2019 for reportedly less than US$3 million, compared to its US$1.1 billion price tag in 2013 (Leskin, 2019).

Some nongovernment organizations have been able to integrate PhotoDNA into highly effective software platforms that proactively detect CSAM and request removal,[4] and other technological developments will make it easier to identify offenders and victims from images. However, these efforts are typically driven by civil society rather than industry. Meanwhile, the public condemnations of online abuse by industry figures too often segue into calls for more parental responsibility and internet safety programs for children, which effectively devolve responsibility for child safety to parents, schools, and children. Necessarily, these strategies are most effective at reaching the least at-risk children, that is, the children with engaged parents who are regularly attending school. Research has consistently shown that the children who are most at risk of online abuse are those who are already vulnerable offline due to disadvantage and prior experiences of abuse and neglect (Jones, Mitchell, & Finkelhor, 2013). Furthermore, a significant proportion of CSAM is, in fact, created by parents and other family members; an inconvenient fact that has been consistently sidestepped by industry and government authorities for decades despite the cumulative evidence (Itzin, 2001; Salter, 2013; Seto, Buckman, Dwyer, & Quayle, 2018). The focus of industry and other voices on "educating" children and parents neglects the children who are most likely to be abused, while deflecting attention from those features of internet services that put children at risk and occluding corporate responsibility for the harms that are facilitated by their online products. Furthermore, this selective focus on education, with its frequent emphasis on the importance of children "keeping themselves safe online," works to blame those who have been victimized (or go on to be) and reinforces the impact and messages of the abuse (Hamilton-Giachritsis, Hanson, Whittle, & Beech, 2017, p. 33). Nonetheless, these strategies remain consistent with the industry's preferred cyberlibertarian approach to CSE with a focus on individual risk and responsibility, even where those individuals are children. This approach is part of a broader rhetorical campaign aimed at responsibilization of targets of many other forms of technology-facilitated

violence and abuse (see Henry and Witt, this volume; Marganski and Melander, this volume).

User Regulation of Child Sexual Exploitation on Social Media Platforms

The inevitable result of 30 years of deferring responsibility for online CSAM and CSE has been that, in 2018–2019, US authorities received 70 million reports of suspected CSAM (Dance & Keller, 2020). As of 2018, there was a backlog of millions of suspected CSAM images and videos in need of assessment while police reported being overwhelmed by the increase in cases and the increased volume and severity of CSAM in each case (ECPAT, 2018), and given reported increases in online CSE activity during the pandemic (INTERPOL, 2020) that backlog may well have expanded. While tech and social media companies accumulate billions in profits, CSAM victims and survivors report an almost total lack of access to affordable, effective mental health care or practical assistance with the ongoing impacts of abuse (C3P, 2017; Salter, 2013). As the scale of the crisis has become undeniable, governments are now shifting to a more interventionist posture (see also Henry and Witt, this volume). For example, the UK government has begun developing a legislative regime around "online harms" that aims to hold technology companies directly responsible for social and individual impacts (HM Government, 2019). This move initiated the global drafting and endorsement of a global set of "voluntary principles" to prevent online CSE for industry implementation as a precursor to formal government regulation.[5] In 2018, the United States enacted the Fight Online Sex Trafficking Act (FOSTA, 2017) which removed internet companies' Section 230 protections from liability if they are found to knowingly facilitate sex trafficking, and there is now a further bipartisan proposal to remove these protections from those deemed to be failing to act on online CSE and CSAM (Keller, 2020). Meanwhile, governments such as Australia have been encouraged to move away from a "coregulation" model with industry in recognition of industry failure to comply with internet safety principles (Briggs, 2018). This shift in the tone and approach of governments to the technology industry is also evident in academic scholarship. Over the last 10 years, celebratory academic accounts of the new possibilities of the internet and globalization have given way to more pessimistic assessments of the impact of the internet on inequality, cultural homogenization, and democratic legitimacy. This so-called "techlash" is now interrogating the monopoly power of the technology industries and their role in violating consumer privacy and circulating (and arguably promoting) malicious, deceptive, and illegal content (Hemphill, 2019).

The "techlash" has come to encompass the issue of online CSE as an urgent priority. We are at a critical juncture where the cyberlibertarian posture of industry is being challenged rather than endorsed by governments, some technology companies are themselves asking to be regulated (Bloomberg, 2020), and the prevalence of online CSE and CSAM is such that it has become visible to everyday social media users. No longer the province of secret subcultures, CSAM

is prevalent on social media sites, file sharing networks, and free adult pornography "streaming" services (Solon, 2020). The fact that these same sites and services do not have adequate measures in place to prevent CSAM circulation (notwithstanding statements of zero tolerance for CSAM) has never been more evident, leading to increasing expressions of concern about lack of accountability and transparency (Pauls & MacIntosh, 2020) and a rapidly changing policy environment, at both industry and government levels.[6] To illustrate the hypocrisies and contradictions of this historical moment, this section describes the efforts of social media and internet users to police CSAM and CSE on their platforms. In doing so, this section reveals two key facts. First, there are amoral consequences arising from cyberlibertarianism, in which corporate and government responsibility for the prevention of CSE and CSAM has been deferred to the point where internet users themselves are performing this basic civic function. Perhaps the most shocking illustration of this regulatory vacuum is that self-identified CSAM survivors, some only teenagers, are themselves active in seeking out and reporting images and video of their abuse, despite the psychological and legal risks this may entail (C3P, 2020a, pp. 4–5; CBC, 2018; Pauls & MacIntosh, 2020). Second, the section undercuts claims by some in the technology industry, certain privacy advocates, and some in government that the proactive detection of CSAM is difficult or impossible from a practical standpoint. The fact that self-organizing networks of social media users and researchers have (sometimes accidently) identified and interrupted the tactics of online abusers, as indicated in the examples below, suggests that the problem of CSE and CSAM regulation has been at least partially one of political and corporate will.

There are multiple examples in which the efforts of users, rather than platforms, have been efficacious in identifying and publicizing the ways in which CSE is taking place on various services. Frequently, these efforts expose not only the presence and activities of child sexual abusers online but also the shortcomings of platform design that facilitate CSE and make reporting difficult. For example, YouTube is the popular online site in which users can make and upload their own video content. Despite stated policies against child abuse and exploitation, users have uploaded videos to YouTube of children in revealing clothing, and children restrained with ropes, sometimes crying or in distress. Some videos have remained online for years and accumulated millions of views before being removed, only after media reporting and public outcry (Warzel, 2017). In February 2019, YouTube user Matt Watson (who later faced criticism for his tactics and for content that he himself had posted (Alexander, 2019)) uploaded a viral video to YouTube documenting the way in which the YouTube "recommend" system – the machine learning process that automatically suggests and curates videos for users – was linking together self-created videos of young children engaged in activities such as dancing, doing gymnastics, and swimming (Orphanides, 2019).[7] Once YouTube detected a user preferentially seeking out and watching content of young children, the "recommend" system would then generate a playlist of similar content. In doing so, the algorithm was proactively curating videos of scantily clad children for those users who particularly enjoyed such content, that is, pedophiles (Kaiser & Rauchfleisch, 2019; Orphanides, 2019).

In the same month, *WIRED* reported finding videos on YouTube relating to similar kinds of images with high numbers of views and comments seeming to show pedophiles using the "comment" function of YouTube to provide time stamps for parts of the videos where the child may inadvertently expose body parts, posting links to other provocative YouTube videos of children, or exchanging contact details with one another (Orphanides, 2019). *WIRED* reported that these videos had been monetized by YouTube, including preroll and banner advertisements (Orphanides, 2019). After all, the videos themselves were not illegal content; rather, it was the recontextualization of those videos by the YouTube recommend system that generated what Matt Watson[8] called a "soft-core pedophile ring" on the platform (Alexander, 2019). YouTube's initial response to the scandal was to delete accounts and channels of those leaving disturbing comments, report illegal conduct to police, turn off the "comment" function on many videos depicting minors and delete inappropriate comments, while employing an automated comment classifier to detect inappropriate comments with greater speed and accuracy (Wakabayashi & Maheshwari, 2019; see also; YouTube, 2019).

In June 2019, *The New York Times* reported that three researchers from Harvard's Berkman Klein Center for Internet and Society had "stumbled upon" a similar issue while doing research about another topic on YouTube (Fisher & Taub, 2019). In all of these cases, action was seemingly only undertaken in the aftermath of significant reputation damage and the advertiser boycotts that followed the reports (Fisher & Taub, 2019). A critical point here is that this disturbing situation is a direct, though unintended, result of business models like YouTube's which seek to maximize profit by keeping users consuming online content in order to sell ads (Maack, 2019). In order to keep people consuming content, YouTube's algorithmic curation of user preference "promotes, recommends, and disseminates videos in a manner that appears to constantly up the stakes" (Tufekci, 2018, para. 6). Some have characterized this as a "rabbit hole effect" that can sometimes "lead viewers to incrementally more extreme videos or topics which are thought to hook them in" (Fisher & Taub, 2019). YouTube's 2020 Transparency Report provides an update on policies relating to child safety (YouTube, 2020).

TikTok is the hugely popular music-based social media platform with a particular focus on teenage users. While TikTok states that users under the age of 13 are not permitted to use the platform, the app's age verification system can be bypassed by entering a false birthdate (Common Sense Media, 2021). TikTok provides short clips of popular music for users to video themselves miming and dancing to. As a result, the platform features videos of children performing to sexually suggestive or explicit songs. TikTok's default privacy settings had been criticized for being low, with many child users not adjusting these settings to make their accounts private or disallow contact from strangers (Broderick, 2019). As was pointed out, the platform's inherent incentives discourage increased privacy settings which would reduce the number of views and interactions with user content (BBC News, 2020). Journalists have identified an active community of TikTok users who appear to be soliciting nude images from children, while minor

users are complaining about repeated solicitation for sexualized images (BBC News, 2020; Cox, 2018). As of 2018, some TikTok user profiles reportedly included open statements of interest in nude images and the exchange of sexual videos, including invitations to trade material via other apps (Cox, 2018). The presence of sex offenders on the app is further evident by reported instances of sexual comments left by men on videos of children (BBC News, 2020; Broderick, 2019). In response, networks of young users have been collecting those usernames who they accuse of sexual misconduct and sharing that information across social media platforms with the aim of shaming offenders and promoting safety on TikTok (Broderick, 2019). Concerned TikTok users have set up social media accounts that focus specifically on "creepy" TikTok interactions, and specific alleged offenders on TikTok have been widely discussed by users on various forums, alongside reports of lax or no response from TikTok to user reports and concerns (BBC News, 2020; Broderick, 2019). The fact that TikTok users are resorting to the self-policing of pedophile activity on the platform raises significant concern about the level of proactive regulation and monitoring of users who seek to engage in the sexual exploitation of children; however, at present, social media platforms are not obliged to publicly report their child protection standards and processes. In 2021, following considerable public pressure, TikTok amended its policies relating to users under 18, which included a change, so that the default setting for accounts created by users aged 13–15 is automatically set to "private" (Peters, 2021).

In 2020, TikTok removed an Australian account that was purporting to "hunt" pedophiles on social media by posing as children and luring men into meetings, which were then filmed (Taylor, 2020). This account was part of a broader pattern of online vigilantes who seek to entrap child sexual abusers by posing as children on social media. This phenomenon has been met with a mixed reception. Australian police have urged people with concerns about online abuse to report to law enforcement (Taylor, 2020) and so have UK police; nonetheless, research by the BBC found that over half of UK prosecutions for grooming in 2018 drew on evidence gathered by online vigilante groups (BBC, 2019). Previous dismissive accounts of online vigilantism have given way to more nuanced analyses of civilian efforts to prevent internet sexual offending, which situate the so-called "pedophile hunting" within an increase in "citizen-led, digitally mediated security initiatives" operating alongside, and often with the cooperation, if not endorsement, of state police and the private sector (Hadjimatheou, 2019, p. 2).

"Pedophile hunting" refers to the proactive luring and entrapment of suspected child abusers using social media (Hadjimatheou, 2019). In the cases described above, social media users are not seeking out sex offenders; they are not "vigilantes" in any meaningful sense. Instead, they are users who are reacting to the ubiquity of sexual misconduct and offending on popularly used platforms, and they are taking action in an attempt to improve their own and others' safety. Unlike "vigilante" groups, who frequently seek police intervention for suspected online misconduct, this form of social media activity tends to rely on social media platforms to take action, and in the absence of a response from platforms, they may seek publicity via online media and mass media. In effect, these users are

reacting to the failure of content regulation of which online abuse and exploitation is a symptom, and they are seeking to institute their own mechanisms of regulation where platforms and the state have failed.

In recent years, there has been significant debate over the status of pedophiles and the regulation of CSAM on social media platform Twitter (Gorman, 2020). Twitter is a major social media platform that was launched in 2006 and grew to 330 million monthly active users and 145 million daily users in 2019.[9] Unlike platforms such as Facebook, which aim to connect users with their friends and family, Twitter is famous for its "town hall" approach, in which users "tweet" short public messages which can be commented on by any other user. This focus on interaction between strangers has lent the platform a somewhat alienating and combative online culture that has inhibited its growth. However, it remains one of the most influential platforms among journalists, academics, and policymakers. Twitter is also one of the most libertarian of all social media platforms and was notoriously described as the "free speech wing of the free speech party" by a senior executive in 2012 (Halliday, 2012, para. 1). This enthusiasm for an online "free for all" on Twitter has been tempered over the last decade by the emergence of organized misogyny and far right groups on the platform, and a high prevalence of hate speech, which has directly impacted Twitter's reputation, share price, and investor appeal (Salter, 2018). Twitter has made a number of concessions to its critics, including providing users with more options to limit abuse online.

In a dramatic development, a group of self-identified survivors of CSAM took to Twitter to claim that videos and images of their abuse were circulating on the platform. The most prominent of these survivors is "Avri Sapir" (a pseudonym), who stated on Twitter that she is a teenaged woman who was abused and exploited in CSAM from infancy until the age of 15 (Gorman, 2020).[10] Avri joined Twitter in October 2018 and became increasingly vocal about the presence of her own CSAM on Twitter from early 2020. Along with a group of supportive users, Avri actively sought to police CSAM on the site by identifying and reporting accounts sharing illegal content to Twitter and US authorities. As a self-identified CSAM survivor, Avri received significant abuse and harassment. In a number of "viral" tweets, Avri has provided screenshots of messages she has received on Twitter from CSAM offenders.[11] These include messages from men claiming that they have previously watched her material, and, in one case, a user who described her daily activities in a fashion that indicated he had been following her. She has also provided screenshots of messages from Twitter users asking for links to her abuse material. On February 27, 2020, she stated:

> I have to live with the knowledge that my abuse will never end, and that every second of every day, someone could be – almost certainly is – watching my torture and abuse. Even once I'm dead, my degradation will continue. I will never be able to escape it. This trauma is infinite.
>
> Child porn is not a victimless crime, and it is the worst form of torture a person can be forced to endure. We must wake up to the

> realities of this pervasive and wide-spread abuse, and push past the discomfort of the topic, because I don't have that privilege. We must hold accountable the people, companies, policies, laws, and cultural beliefs that allow this type of abuse to continue and thrive. We must listen to and defend survivors and put an end to the gaslighting, victim-blaming, and excuses that allow this issue to be ignored.[12]

As Avri's prominence on Twitter grew, she began intersecting with and amplifying existing accounts who identified themselves as "antipedophile"; that is, they proactively sought out and reported CSAM and CSE accounts on Twitter to the platform, as well as to authorities such as the National Center for Missing and Exploited Children.[13] A recent report analyzing CSAM reporting options on popular Web platforms concluded that it is "extremely difficult to report content as CSAM on Twitter" (C3P, 2020b, p. 15). When a user encounters a problematic tweet, Twitter offers four categories of "report" options, including that a tweet is "abusive or harmful." However, subsequent options do not allow users to report CSAM. Instead, users have to search to find a separate online form in order to bring CSAM or a CSE issue to the attention of Twitter moderators.[14] One of the key functions of antipedophile Twitter is to increase awareness of this form and encourage followers to mass report identified CSAM abusers. Faced with the significant concerns raised not only by users but also by agencies such as the Internet Watch Foundation (Wright, 2019) and C3P (2020b) regarding CSAM on the site, Twitter's communications team has stated that "Twitter has zero tolerance for any material that features or promotes child sexual exploitation" (de Gallier, 2020, para. 8).

In October 2020, in the face of sustained pressure (Dodds, 2020), Twitter published a significant revision of its CSE policy that explicitly disallowed efforts to normalize or promote pedophilia as a sexual orientation or identity on the platform. The new policy provided expanded detail on the forms of abusive and exploitative behavior that would be considered a breach of terms of service, including the circulation of drawn or computer-generated abuse images and the sharing of links to abuse material (Twitter, 2020). While this is a positive development, the policy contains no information on resourcing or enforcement. As yet, there are no rigorous reporting and transparency requirements that would oblige Twitter to publicly account for their CSAM problem and proposed solutions.

A recent civil suit against Twitter describes another user who, as a young person, struggled to have his abuse material removed from the platform. In the suit, the now 17-year-old complainant alleges that Twitter failed to remove abuse videos of him as a 13 year old boy after he repeatedly notified them of the content. The suit alleges that Twitter only removed the content, five weeks after the first report, once it was escalated by law enforcement (Fonrouge, 2021). It appears that, in the absence of adequate efforts from Twitter, CSAM regulation has become the province of users and, in some cases, victims and survivors themselves. As they identify and report CSAM on Twitter and elsewhere, Avri and other antiabuse activists expose themselves to significant trauma and other risks:

vitriol and attacks from pedophiles and other users on the site, as well as exposure to sexually abusive imagery that carries with it a high likelihood of traumatization. From late 2020, Avri became the subject of a concerted online campaign which attempted to attack her credibility in various ways, including the claim that her narrative had been invented as part of a religiously motivated "antipornography" campaign. This claim was advanced despite Avri's public statements in support of sex workers, in which she made clear distinctions between CSAM and consensual adult content.[15] However, as momentum for online regulation and harm reduction builds apace, due in part to an increasingly vocal CSAM survivor contingent, it is triggering backlash by libertarian activists and coalitions for whom a regulated internet is a censorious one.

Analysis and Reflection

The rhetoric of cyberlibertarianism has powerfully shaped the landscape of the internet, justifying the regulatory stance of technology companies and states in which corporate discretion has been prioritized over user safety. This strategy owes its success to a confluence of factors including the correspondence and mutually reinforcing relationship between cyberlibertarianism and entrenched free-market neoliberalism as well as with some forms of "progressive" identity politics, in which the online proliferation of sexual freedom and self-expression is considered a *prima facie* public good. Nagle (2017) observes the naivete of optimistic academic and media accounts of online transgression as politically emancipatory, pointing to the deeply amoral and nihilistic strains of internet culture that have been facilitated by cyberlibertarianism. However, the catastrophic consequences of cyberlibertarianism for children have been obscured by its often self-interested narration as a bearer of straightforward "goods" such as "freedom of speech," "connection," and "opportunity," and effective use of vagaries and platitudes to hide its contradictions and distasteful aspects. The cyberlibertarian narrative of maximal online freedom with minimal state regulation does not, and cannot, accommodate the categorical differences in vulnerability between children and adults, the moral prerogatives of child protection, or children's internationally recognized and acclaimed human rights. Hence, children, similar to other groups socially marginalized by racism, sexism, homophobia, and other oppressions, are simply *not taken into account* by cyberlibertarianism. During the formative decades of the internet, the core principle of cyberlibertarianism was that it is, by default, the right thing to maximize "online freedom," defined as "freedom from interference" for corporations and individuals alike. The myopic focus on maximal freedom from regulation and oversight was an appealing alternative to the demanding and messy work of adjudicating a plurality of competing interests and even competing freedoms, all of which need to be carefully considered and weighted to achieve a fair and transparent system in which the most egregious harms are prevented.

Few would deny that CSAM survivors' rights to privacy and dignity are violated where images of their abuse are shared online, or where the men who

have viewed those images stalk and harass them. However, their assertion of their right to privacy *from other social media users* and *criminal abusers* is considerably broader than the narrow formulation championed by cyberlibertarians, understood solely in terms of freedom from interference from the state. Having lost faith in the willingness of social media platforms to protect them, CSAM survivors and other users instead publicly "name and shame" the platforms who host images and videos of their abuse. They seek external intervention in order to secure their privacy and other basic human rights from the Web 2.0 business model in which abusive and illegal content circulates with de facto impunity. Civil and cyberlibertarians have responded to the prospect of increased state intervention in social media and online content by pointing to the (very real) potential for state and police overreach in the name of child protection; however, they are persistently unwilling or unable to take into account the broader claims to privacy asserted by self-identified CSAM survivors like Avri and others like her. Indeed, the narrow formulation of "online privacy" advanced under cyberlibertarianism continues to justify measures that are in direct conflict with the rights and interests of CSAM victims and survivors. For example, Facebook and Twitter are currently seeking to implement end-to-end encryption on their messenger functions, which would necessarily facilitate CSAM distribution and protect CSAM offenders. It is estimated that Facebook's encryption plans would reduce reports of online CSE in the United States by two-thirds (Valentino-DeVries & Dance, 2019) and reduce arrests for online CSE in the United Kingdom by up to 2,500 per year (Murgia, 2019). Despite ongoing and high-level resistance to Facebook's plans, due to their serious implications for global child protection efforts, Twitter's Head of Product Kayvon Beykpour has stated emphatically that Twitter is also seeking to encrypt its Direct Message (DM) function (Marino, 2019). In this example, the libertarian formulation of privacy in terms of the capability of users to share content (including CSAM) without consequence is prioritized by technology companies over the human rights of CSAM survivors to privacy, dignity, and safety. By (either explicitly or implicitly) adopting the cyberlibertarian narrative, industry, governments, and individuals have effectively given themselves license to see online harms, including child abuse and exploitation, as inevitable "necessary evils" that should be tolerated or ignored given the necessity of "online freedom." This position dovetails with the general societal discomfort with anti-CSAM activists like Avri name, enabling people to remain within their comfort zone, not seeing or recognizing what should be shocking and attention-grabbing levels of child abuse. While the need for greater regulation has been recognized by some governments and other principles for the online environment are now being delineated and asserted, progress, where it happens, is slow (particularly in contrast to the fast speed of innovation for profit), and decisions continue to be made by corporations and states that flow from cyberlibertarianism's fundamentally unethical premises. For example, some technology companies choose not to screen for known CSAM, arguing that this would constitute an invasion of privacy (IICSA, 2020, p. 48), despite their very business model being based around surveillance and the invasion of privacy (Zuboff, 2019). Hypocrite and contradiction loom large, yet are hidden through sleights of hand

and platitudes that remain largely unchallenged. While governments and their inquiries have started to ask pressing questions about the persistent and growing problem of online child abuse, regulation is still seen as a last resort, a regrettable alternative to the supposedly higher plane of "collaboration" with industry. Too often the questions asked are not ambitious enough, they work within, rather than identify and challenge, the overarching cyberlibertarian construction of "online freedom," without critically examining whose "freedom" it is that we are talking about. One consequence of all of this is a situation in which mainstream platforms are beset with CSAM, and users, too often children and/or survivors, are those tasked with its identification and attempts at its removal.

As noted, reports indicating that survivors and other internet users are frequently finding and taking action against CSAM, grooming, and other online pedophilic activity challenges the notions that regulation is unwarranted, unwanted, or unworkable – as well as the alternative argument that adequate safeguards are already in place. While the determination and resourcefulness of these individuals is to be applauded, their efforts should never have been necessary, and the fact that they are points to a deeply troubling state of affairs. The role they are compelled to undertake in the absence of corporate and government action carries numerous personal costs and risks. There is the traumatizing impact of exposure to illegal material, including, in some cases, images of their own abuse, alongside the legal risks involved in following the pathways to it. There is also the risk that speaking out leads to harassment and further abuse of oneself or others, and in particular for survivors, there can be the distressing impact of societal invalidation. Invalidation can be one of the hardest aspects of child sexual abuse to deal with: the message conveyed through the words and actions of the offender(s) that the child's self, agency, and feelings are unimportant (Salter, 2012). When technology companies fail to prevent survivors' CSAM circulating or fail to robustly act when it is brought to their attention (or in other ways fail to take a survivor's abuse seriously), the invalidating message of the original abuse is echoed by "the system." For some survivors, the impact of wider society falling in step with their abuser can be catastrophic, confirming deep-rooted fears about their lack of self-worth and effectively sending them into free fall. It can be the shattering of fragile hopes that the offender(s)' stance toward them did not reflect the truth.

Ways Forward

Continuing technological innovations designed to detect online child abuse, together with recent actions and positions taken by governments, are promising, while the hegemony of cyberlibertarianism has been destabilized and its self-serving rhetoric exposed by multiple colliding world events. Many of the supposed democratic benefits of social media and the internet have been found wanting, and cascading developments have corroded public trust in the technology industry, including the monopolization of the internet by a few mammoth companies, the manipulation of social media to spread disinformation and conspiracy theories, privacy breaches including the Cambridge Analytica scandal,

and the use of social media as a surveillance tool by private sector, governments, and police. As conflicts between the public good and the private interests of the technology industries come into focus, civil society and some governments are starting to articulate new, more ethical paradigms of online freedoms that include a duty of care, children's rights, social justice, and an orientation toward human rather than capital ends. These paradigms move beyond libertarian scaremongering in which online privacy is an all-or-nothing proposition, either total freedom from regulation and censorship, or a Big Brother style panopticon of state censorship. Instead, a range of stakeholders are situating online harms within a critique of the ways in which online architecture and administration constitutes its own mode of regulation, albeit one designed for capital rather than public interests.

In many regards, these shifts can be tied toward wider moves toward "progressive capitalism" (Stiglitz, 2019) that seeks to reembed markets within government control and social responsibility. It is undoubtedly the case that a coherent, ethical, and accessible philosophical framework is a necessary basis from which to ask the right questions about online child safety and protection and then set about answering them, and this will surely lead to progress, although it is unclear whether notions of "progressive capitalism" ultimately are up to the task. For example, legislating a statutory "duty of care" may turn corporate attention toward the minimization of potential harms embedded in online services and products but does not directly address the cause of those harms. The current formulation of social media business models generates enabling conditions for abuse and exploitation, structuring user incentives in a way that creates competitive and often alienating hierarchies in an effort to maximize engagement and advertising revenue while harvesting user data (Salter, 2017). In other words, social media companies are invested in maintaining online environments that are conducive to abuse. There is a continuity between an increasingly outmoded cyberlibertarianism and the friendlier face of a "progressive capitalism," in that they both legitimize the exploitation of users (including children) in the interests of profit, albeit the former proposes that such exploitation is natural and inevitable, while the latter seeks to build in basic safeguards. It should, therefore, not be a surprise if sexual exploitation persists on platforms built for user exploitation, regardless of the stipulated corporate philosophy of the platform itself. A more fundamental question is: What would an internet built in the interests of children and other users look like? This is the truly ethical question we need to begin with, journey on from, and keep bringing ourselves back to.

Notes

1. The Twitter account of Avri Sapir remains limited to followers; however, this tweet was made on May 1st at 11.47 a.m. At the time of publication of this book, as with most tweets, no allegation made by Avri has been proven in court.
2. The Technology Coalition has recently announced a "Plan to Combat Online Child Abuse" that includes research and development funds for "technological tools" to prevent online child sexual exploitation (CSE) and the publication of an

annual progress report charting industry efforts, see https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/.

3. Media reports indicate that reliance on human content moderators has been reduced in the context of COVID-19 (Dwoskin, 2020).
4. For example, see Project Arachnid (https://projectarachnid.ca/en/).
5. For example, see Five Country Ministerial. (n.d.). *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*. Retrieved from https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5e6123b6cfea6860596132af/1583424438930/111Voluntary1principles1-1one1page1-1Final.pdf.
6. While we have done our best to reflect changes in this rapidly evolving policy environment, the realities of publication mean that more recent changes may not be incorporated in this chapter.
7. See MattsWhatItIs. (2019, February 17). *Youtube is Facilitating the Sexual Exploitation of Children, and it's Being Monetized (2019)* [Video]. YouTube. Retrieved from https://www.youtube.com/watch?v5O13G5A5w5P0&t55s.
8. See MattsWhatItIs. (2019, February 17). *Youtube is Facilitating the Sexual Exploitation of Children, and it's Being Monetized (2019)* [Video]. YouTube. Retrieved from https://www.youtube.com/watch?v5O13G5A5w5P0&t55s.
9. For example, see Lin, Y. (2019, November 30). 10 Twitter Statistics Every Marketer Should Know in 2020 [Infographic] [Blog post]. Retrieved from https://www.oberlo.com/blog/twitter-statistics.
10. Some of the content of the following section is based on Twitter postings made on a public account @AvriSapir, which is private at the time of publication. Republication of these Twitter postings has been made with the consent of the owner of @AvriSapir.
11. Sapir, A. [@AvriSapir] (2020, 27 February 6.45 a.m.). "This is what it's like to be a survivor of child pornography that was commercially sold, traded, and shared all over the internet" [Tweet].
12. Sapir, A. [@AvriSapir] (2020, 27 February 6.45 a.m.).
13. For example, see this tweet in which Avri requests her followers to report a Twitter account allegedly sharing child sexual abuse material (CSAM) on the platform. Sapir, A. [@AvriSapr] (2020, April 25, 5.35 p.m.) "everyone do me a favor and report (redacted) using Twitter's CSE form do NOT scroll through the account, just report it please" [Tweet].
14. For example, see Twitter. (n.d.). *Report a child sexual exploitation issue* [Online form]. Retrieved from https://help.twitter.com/forms/cse.
15. For example, Avri has publicly objected to policy developments that she feels appropriate notions of "trafficking" to justify the banning of adult pornography or the harmful regulation of adult sex work. Sapir, A. [@AvriSapir] (2021, January 1, 55 a.m.). "If people actually listened to survivors, nonsense like SISEA wouldn't happen. They're not listening to survivors, because this isn't about trafficking – it's about banning pornography under the guise of victim protection. It's offensive" [Tweet].

References

Alexander, J. (2019, February 19). YouTube still can't stop child predators in its comments. *The Verge*. Retrieved from https://www.theverge.com/2019/2/19/18229938/youtube-child-exploitation-recommendation-algorithm-predators

BBC. (2018, November 20). Tumblr removed from Apple app store over abuse images. Retrieved from https://www.bbc.co.uk/news/technology-46275138

BBC. (2019, November 6). Police concerns over rise of 'paedophile hunters'. *BBC*. Retrieved from https://www.bbc.com/news/uk-england-50302912

BBC News. (2020, November 2). TikTok failed to ban flagged 'child predator'. *BBC News*. Retrieved from https://www.bbc.com/news/technology-54773257

Bloomberg. (2020, February 17). Facebook needs, wants, must have regulation, Zuckerberg says. *Los Angeles Times*. Retrieved from https://www.latimes.com/business/technology/story/2020-02-17/facebook-needs-regulation-zuckerberg

Briggs, L. (2018). *Report of the statutory review of the enhancing online safety act 2015 and the review of schedules 5 and 7 to the broadcasting services act 1992 (online content scheme)*. Canberra. Retrieved from https://www.communications.gov.au/publications/report-statutory-review-enhancing-onlinesafety-act-2015-and-review-schedules-5-and-7-broadcasting

Broderick, R. (2019, June 24). TikTok has a predator problem. A network of young women is fighting back. *Buzzfeed*. Retrieved from https://www.buzzfeednews.com/article/ryanhatesthis/tiktok-has-a-predator-problem-young-women-are-fighting-back

Bursztein, E., Clarke, E., DeLaune, M., Elifff, D. M., Hsu, N., Olson, L., … Bright, T. (2019, May 13–17). Rethinking the detection of child sexual abuse imagery on the internet. In Proceedings of the 2019 world wide web conference, WWW '19, San Francisco, CA.

C3P. (2017). *Survivor's survey preliminary report*. Winnipeg, MB: Canadian Centre for Child Protection.

C3P. (2020a). *How we are failing children: Changing the paradigm*. Winnipeg, MB: Canadian Centre for Child Protection. Retrieved from https://www.protectchildren.ca/en/resources-research/child-rights-framework/

C3P. (2020b). *Reviewing child sexual abuse material reporting functions on popular platforms*. Winnipeg, MB: Canadian Centre for Child Protection. Retrieved from https://www.protectchildren.ca/pdfs/C3P_ReviewingCSAMMaterialReporting_en.pdf

Carr, M. (2015). Power plays in global internet governance. *Millennium*, 43(2), 640–659.

CBC News. (2018, August 29). After their child sexual abuse was recorded and spread online, survivors call on governments to take action. *CBC News*. Retrieved from https://www.cbc.ca/news/canada/manitoba/phoenix-11-child-sex-abuse-images-1.4802132

Common Sense Media. (2021). Parents' ultimate guide to TikTok. Retrieved from https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-tiktok

Cox, J. (2018, December 6). TikTok, the app super popular with kids, has a nudes problem. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/j5zbmx/tiktok-the-app-super-popular-with-kids-has-a-nudes-problem?utm_source5mbtwitter

Dahlberg, L. (2010). Cyber-libertarianism 2.0: A discourse theory/critical political economy examination. *Cultural Politics*, 6(3), 331–356.

Dance, G., & Keller, M. H. (2020, February 7). Tech companies detect a surge in online videos of child sexual abuse. *New York Times*. Retrieved from https://www.nytimes.com/2020/2002/2007/us/online-child-sexual-abuse.html

Dodds, L. (2020, January 9). Twitter accused of aiding child abuse by allowing 'explosion' of online paedophile communities. *Telegraph*. Retrieved from https://www.telegraph.co.uk/technology/2020/2001/2009/twitter-accused-aiding-child-abuse-allowing-explosion-online/

Dwoskin, E. (2020, March 24). Stay-home orders test the future of policing online content. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/

ECPAT. (2018). *Trends in online child sexual abuse material*. Bangkok: Author.

Farid, H. (2017, September 19). Technology sector should not be shielding sex traffickers online. *The Hill*. Retrieved from https://thehill.com/opinion/technology/351315-technology-sector-should-not-be-shielding-sex-traffickers-online

Fight Online Sex Trafficking Act (FOSTA). (2017). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/1865/text

Fisher, M., & Taub, A. (2019, June 3). On YouTube's digital playground, an open gate for paedophiles. *New York Times*. Retrieved from https://www.nytimes.com/2019/2006/2003/world/americas/youtube-paedophiles.html

Fonrouge, G. (2021, January 21). Twitter refused to remove child porn because it didn't 'violate policies': Lawsuit. *New York Post*. Retrieved from https://nypost.com/2021/01/21/twitter-sued-for-allegedly-refusing-to-remove-child-porn/

de Gallier, T. (2020, April 7). I make over £20k a month selling nudes online. *BBC*. Retrieved from https://www.bbc.co.uk/bbcthree/article/5e7dad06-c48d-4509-b3e4-6a7a2783ce30

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. New Haven, CT: Yale University Press.

Gorman, G. (2020, December 9). Child abuse victim says porn website Pornhub profited from her child rape. *News.com.au*. Retrieved from https://www.news.com.au/life-style/real-life/news-life/child-abuse-victim-saysporn-website-pornhub-profited-from-her-child-rape/news-story/7e3880aa4a94504acea7675bb8112cff

Hadjimatheou, K. (2019). Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters. *Criminology & Criminal Justice*. Forthcoming.

Halliday, J. (2012, March 22). Twitter's Tony Wang: 'We are the free speech wing of the free speech party'. *Guardian*. Retrieved from https://www.theguardian.com/media/2012/mar/2022/twitter-tony-wang-free-speech

Hamilton-Giachritsis, C., Hanson, E., Whittle, H., & Beech, A. (2017). *Everyone deserves to be happy and safe. A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it*. London: NSPCC.

Hanson, E. (2019). 'Losing track of morality': Understanding online forces and dynamics conducive to child sexual exploitation. In J. Pearce (Ed.), *Child sexual exploitation: Why theory matters* (pp. 87–116). Bristol: Policy Press.

Hemphill, T. A. (2019). 'Techlash', responsible innovation, and the self-regulatory organization. *Journal of Responsible Innovation*, 6, 240–247.

HM Government. (2019). *Online harms white paper*. London: Author.

IICSA. (2020). *The internet: Investigation report*. London: Independent Inquiry into Child Sexual Abuse.

Interpol. (2020, September 7). *INTERPOL report highlights impact of COVID-19 on child sexual abuse*. Lyon: Author. Retrieved from https://www.interpol.int/en/

News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

Itzin, C. (2001). Incest, paedophilia, pornography and prostitution: Making familial abusers more visible as the abusers. *Child Abuse Review*, 10, 35–48.

Jenkins, P. (2001). *Beyond tolerance: Child pornography on the internet*. New York, NY: New York University Press.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2013). Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010). *Psychology of Violence*, 3(1), 53–69.

Kaiser, J., & Rauchfleisch, A. (2019). The implications of venturing down the rabbit hole. *Internet Policy Review*, 8(2), 1–22.

Keller, M. H. (2020, March 5). Bill would make tech firms accountable for child sex abuse imagery. *New York Times*. Retrieved from https://www.nytimes.com/2020/2003/2005/us/child-sexual-abuse-legislation.html

Leskin, P. (2019, December 21). A year after Tumblr's porn ban, some users are still struggling to rebuild their communities and sense of belonging. *Business Insider*. Retrieved from https://www.businessinsider.com.au/tumblr-porn-ban-nsfw-flagged-reactions-fandom-art-erotica-communities-2019-2018?r5US&IR5T

Liao, S. (2018, December 3). Tumblr will ban all adult content on December 17th. *Verge*. Retrieved from https://www.theverge.com/2018/2012/2013/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode

Maack, M. (2019, July 24). 'YouTube recommendations are toxic,' says dev who worked on the algorithm. *Next Web*. Retrieved from https://thenextweb.com/google/2019/06/14/youtube-recommendations-toxicalgorithm-google-ai/

Marino, A. (2019, October 15). Twitter is thinking about how tweets can become more ephemeral. *Verge*. Retrieved from https://www.theverge.com/2019/2010/2015/20913994/podcast-twitter-head-of-product-kayvon-beykpour-interview-auto-delete-tweets-vergecast

Murgia, M. (2019, October 18). Facebook looks to improve child protection over fears encryption will raise risks. *Financial Times*. Retrieved from https://www.ft.com/content/b5480746-f01f-11e9-bfa4-b25f11f42901

Nagle, A. (2017). *Kill all normies: Online culture wars from 4chan and Tumblr to Trump and the alt-right*. Winchester: Zero Books.

Orphanides, K. G. (2019, February 20). On YouTube, a network of paedophiles is hiding in plain site. *Wired*. Retrieved from https://www.wired.co.uk/article/youtube-pedophile-videos-advertising

Pauls, K., & MacIntosh, C. (2020, December 1). Women who spent years scrubbing explicit video from internet urges tech firms to make it easier to remove. *CBC News*. Retrieved from https://www.cbc.ca/news/canada/manitoba/canada-internet-children-abuse-pornography-1.5822042

Peters, T. (2021, January 13). TikTok reveals new privacy settings for kids: What parents should know. *Today*. Retrieved from https://www.today.com/parents/tiktok-changes-privacy-settings-kids-under-18-t205733

Salter, M. (2012). Invalidation: A neglected dimensions of gender-based violence and inequality. *International Journal for Crime, Justice and Social Democracy*, 1(1), 3–13.

Salter, M. (2013). *Organised sexual abuse*. London: Glasshouse/Routledge.

Salter, M. (2017). *Crime, justice and social media*. London; New York, NY: Routledge.

Salter, M. (2018). From geek masculinity to Gamergate: The technological rationality of online abuse. *Crime, Media, Culture*, 14(2), 247–264.

Seto, M., Buckman, C., Dwyer, R., & Quayle, E. (2018). *Production and active trading of child sexual exploitation images depicting identified victims: NCMEC/Thorn research report*. Alexandria, VA: NCMEC.

Silverstein, J. (2018, November 20). Tumblr app disappears from Apple's App Store because of child porn. *CBS News*. Retrieved from https://www.cbsnews.com/news/tumblr-app-disappears-from-apple-app-storebecause-of-child-porn/

Solon, O. (2020, April 23). Child sexual abuse images and online exploitation surge during pandemic. *NBC News*. Retrieved from https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506

Stiglitz, J. (2019). *People, power, and profits: Progressive capitalism for an age of discontent*. London: Penguin Books.

Taylor, J. (2020, March 2). TikTok removes Australian account purporting to hunt paedophiles. *Guardian*. Retrieved from https://www.theguardian.com/technology/2020/mar/2002/tiktok-removes-australian-account-purporting-to-hunt-paedophiles

Tufekci, Z. (2018, March 10). YouTube, the great radicalizer. *New York Times*. Retrieved from https://www.nytimes.com/2018/2003/2010/opinion/sunday/you-tube-politics-radical.html

Turner, F. (2010). *From counterculture to cyberculture: Stewart Brand, the whole earth network, and the rise of digital utopianism*. Chicago, IL: University of Chicago Press.

Twitter. (2020). Child sexual exploitation policy. Retrieved from https://help.-twitter.com/en/rules-and-policies/sexual-exploitation-policy

US Attorney General. (1986). *Attorney general's commission on pornography: Final report*. Washington, DC: U.S. Department of Justice.

Valentino-DeVries, J., & Dance, G. (2019, October 2). Facebook encryption eyed in fight against online child sex abuse. *New York Times*. Retrieved from https://www.nyti-mes.com/2019/2010/2002/technology/encryption-online-child-sex-abuse.html

Wakabayashi, D., & Maheshwari, S. (2019, February 21). Advertisers boycott YouTube After pedophiles swarm comments on videos of children. *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/20/technology/youtube-pedophiles.html

Warzel, C. (2017, November 22). YouTube is addressing its massive child exploitation problem. *Buzzfeed*. Retrieved from https://www.buzzfeednews.com/article/charlie-warzel/youtube-is-addressing-its-massive-child-exploitation-problem

Wright, M. (2019, November 11). Twitter responsible for half of child abuse material UK investigators found on web platforms. *Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2019/11/10/twitter-responsible-half-child-abuse-mate-rial-uk-investigators/

YouTube. (2019). An update on our efforts to protect minors and families. Retrieved from https://blog.youtube/news-and-events/an-update-on-our-efforts-to-protect

YouTube. (2020). *Transparency report featured policies: Child safety*. Retrieved from https://transparencyreport.google.com/youtube-policy/featured-policies/child-safety?hl=en&policy_removals=period:2020Q4&lu=policy_removals

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.