In late March 2020—as COVID-19 circulated around the globe—reports emerged of another viral threat, “Zoombombing.” Founded in 2011, the relatively unknown public company, Zoom, entered a crowded and hypercompetitive video-teleconferencing market dominated by the likes of tech powerhouses Google, Skype, and Microsoft (Konrad, 2019). Zoom’s service received widespread acclaim for its videoconferencing quality and reliability, offering few lags and drops that often plagued other established platforms. By 2016, Zoom’s user friendliness, cost effectiveness, and aggressive sales strategy led to it being widely adopted across the education systems (Konrad, 2019). Given its integration into pre-existing education budgets and information technology (IT) departments, Zoom quickly emerged as a preferred platform to replace the in-person classroom as schools and universities were shuttered by COVID-19.

The rapid adoption of Zoom did not go unnoticed on Wall Street and in the business pages of major daily newspapers—the stock valuation of the firm skyrocketed in the early days of the economic shutdown. But the news stories were not all rosy. Soon reports emerged of widespread disruptions of Zoom meetings by uninvited users taking advantage of the videoconferencing’s startlingly weak privacy and security protocols (Cox, 2020; Marczak, Scott-Railton, 2020). Although the company attempted to communicate best practices against Zoombombing to its user base on 20 March in an official blog post (Zoom, 2020), disruptions continued to proliferate, leading users and shareholders alike to organize an online petition (D. Johnson, 2020) and threaten class action (L. T. Johnson, 2020). Finally, Zoombombing gradually began to subside on the videoconferencing platform after the Federal Bureau of Investigation (FBI) issued a statement on 30 March, characterizing it as a cybercrime to be reported to law enforcement agencies (Setera, 2020).

For those organizations, schools and universities that had rapidly come to rely upon Zoom to maintain their everyday operations and educational programming, Zoombombing posed added challenges and uncertainty during a crucial early period of the COVID-19 pandemic. Early press accounts conveyed astonishment over the timing of such disruptions, just as the pandemic was shutting down daily life. Three predominant frames were used by mainstream news media to explain Zoombombing to an already anxious and confused public. First, the more lewd and offensive disruptions on Zoom were characterized as a new type of trolling behavior that disproportionately targeted traditional trolling victims such as women, people of color, religious minorities, and other marginalized groups: “the trolls of the internet are under quarantine, too, and they’re looking for Zooms to disrupt” (Lorenz, 2020).

Corresponding Author: Greg Elmer, Ryerson University, Toronto, ON M5B 2K3, Canada. Email: gelmer@ryerson.ca

1Ryerson University, Canada
2York University, Canada
3Simon Fraser University, Canada

Creative Commons Non Commercial CC BY-NC. This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
extension of other forms of online harassment and hate speech that are often coordinated across various messaging platforms, including Reddit, Discord, and 4chan (Lorenz & Alba, 2020), serving to articulate “another vector for organized harassment” (Glaser et al., 2020). Second, journalists addressed Zoombombing as a security and privacy threat posed by hackers. Such articles subsequently focused on the dissemination of safeguard measures that users could take to protect themselves online (Morris, 2020). This privacy focused framing addressed the relationship of computer insecurity victimization and economic damage through the logic of self-responsibility: “Experts say failing to enable [Zoom] security features not only opens you up to online trolls, [but that] important information can be stolen from your business meetings” (Fan, 2020). A third frame took a more light-hearted approach, highlighting Zoom meetings that were interrupted by jokes and pranks, typically from known individuals such as family members and friends of the Zoom participants (Stern, 2020). Such examples often follow the photobombing theme, reframed into the domestic pandemic space, with the background of a Zoom video used to Zoombomb the roommate or family member.

This article seeks to question the relevance of the aforementioned media framings of Zoombombing, through an empirical study of Zoombombing practices. Do these stories and frames adequately capture the spread and impact of Zoombombing during the global COVID pandemic? What, if anything, do these frames fail to account for? As a novel practice during an exceptional time (global pandemic), Zoombombing emerged out of a wholesale shift from in-person to online learning. This is not to suggest however that Zoomboobing is without precedent or is somehow removed from other toxic, disruptive, and abusive online practices, clearly the abovementioned news reports do help explain aspects of Zoombombing and its spread. But still, we believe that the novelty of the Zoom platform, the widespread displacement of its users from their sites of work and education, and the distinctiveness of the Zoombomb as a mediated object, can offer unique insights on the popular framing and scholarly literature of abusive online practices.

To determine how Zoombombing contributes to—and potentially departs from—pre-existing abusive and disruptive online practices, this article adopts Elmer et al.’s (2012) three-pronged digital method, an approach that posits the development and adoption of online practices as co-constructed between users, media objects (videos, comments, pots, photos, etc.), and online platforms. Given that disruptive and other toxic forms of online behavior often originate and circulate on multiple platforms and online spaces (de Zeeuw & Tuters, 2020) or might migrate from one platform to another to avoid detection, regulation, and deplatforming (Rogers, 2020), our study questions how different platforms afforded the spread of Zoombombing discourses and/or user practices. This first portion of our article focuses on Zoombomb related posts on two popular Internet platforms, Twitter and Reddit, two sites that offer contrasting affordances, practices, and user demographics.

After analyzing how Zoombombing is practiced on Twitter and Reddit, we then move to a more in-depth study of Zoombombs as media objects, the recordings of such online attacks and disruptions, as archived and curated on the YouTube video hosting platform. Again, prior to the pandemic Zoom, the widespread use of virtual teleconferencing was largely limited to geographically remote communities, transnational global firms, government, and some large-scale research initiatives. Zoom’s affordances, interface, and bevy of user settings, as privacy and security-focused reporters noted, were thus all quickly put to the test by a much wider set of users and contexts during the early months of the pandemic. All these platform functions, options, and settings frame our principal object of study, the video itself of the disrupted online meetings, classes, and events. While a “real-time” digital methods study (Back & Puwar, 2012) of Zoombombing could have focused directly on the Zoom platform, our study of recorded Zoombombing videos hosted on YouTube offers the additional benefit of understanding how such seemingly fleeting moments have prolonged the phenomenon in the form of curated YouTube compilations. In other words, the choice of YouTube once again helps us to understand how the affordances of the platform have contributed to the remediation of the Zoombomb as a media object, further qualifying the ongoing disruptive nature of Zoombombing before (online pre-planning of attacks), during (on Zoom) and after the attack itself (Zoom video hosted on YouTube). Finally, supplementing our study of Twitter and Reddit, our YouTube-focused study also qualifies the practice—and targets—of Zoombombers (the users), again through an analysis of their verbal utterances during the mediated attack. It is our ultimate hope that our article’s findings will contribute to the development of policies and solutions that address abusive, racist, and other toxic practices on the Internet and beyond.

Literature Review and Theory

Further delving into the conceptual frameworks offered in our brief review of the mainstream media’s Zoombombing coverage, the article will first turn to a review of the academic literature surrounding disruptive and anti-social behavior online, highlighting the dominant conceptual frameworks such as hacking, cyber abuse, trolling, and pranking. At the conclusion of the literature review, we narrow our focus on visually disruptive user practices, arguing that while Zoombombing takes its name from the rather harmless act of photobombing, it might be better understood alongside other anonymous technology enabled disruptions, namely the intrusive and often abusive practice or “airdropping” photos and images and videos onto personal mobile phones (Knorr, 2019). Such mediated practices thus set the stage for our study of a much more dynamic and interactive
process wherein individual users (or groups of users) disrupt the videoconferencing interface used by many educational institutions, workplaces, and leisure-based organizations.

After the literature review, the article then moves on to introduce the case study, wherein we take a mixed methods approach informed by digital methods, an approach that studies the interplay between user practices, media objects, and platform affordances (Rogers, 2013). Unlike mass media content analysis that typically seeks to empirically determine semantic commonalities (often in mass media texts),

digital methods are designed to trace the rules or practices established over time between users and Internet platforms. Rogers (2004) first described digital methods as an epistemological approach, as “... the means by which the culture of the Web adjudicates” (p. 2). As the web and search engine model gave way to the proliferation of social networking focused platforms, digital methods studies recognized the culture of the web as networked among properties that offered unique or amplified user affordances, services, and interfaces. Our “cross-platform approach” (Elmer & Langlois, 2013; Pearce et al., 2020; Rogers, 2019), bringing together user communication practices and the platform affordances, is anchored by a qualitative coding of Zoombombing focused posts and utterances by users. The coding schema is guided by a-semantic theories, first outlined by Louis Hjelmslev (1961), then later adopted in various forms by scholars interested in hybrid human or machinic communications. Felix Guattari (1992), for one, developed the a-semantic approach to highlight the tangible, material effects of communication as an adjunct to efforts at unearthing the semantic meaning of texts. Elmer (1997) similarly adopted the a-semantic approach to understand how communication through hypertext produced material effects on the Internet (e.g., computer crashes, economic exchanges, the generation of new sites, pages, and so forth).

The a-semantic approach is likewise adopted here to code the posts of users on Twitter and Reddit, and the utterances of Zoombombers on YouTube, not for their opinions, tone, or sentiments, but as a practice of communication that has tangible and material effects. In short, we are concerned with how social media posts enact Zoombombing.

Such an a-semantic coding further amplifies our recognition of Zoombombing as a socially disruptive and toxic socio-technical practice that seemingly stands in direct opposition to phatic forms of communication, interpersonal language that establishes common civil bonds (Miller, 2008, 2015). In theoretical terms then we posit Zoombombing as a mediated, anti-phatic form of communication that disrupts civil forms of social communication. To better position the findings of our study, we next turn to a review of the most common frameworks for understanding disruptive and abusive communication prior to Zoombombing.

**Hacking and Privacy**

The broadest perspective on technological disruptions—in particular, disruptions by users of digital and networked communications technologies—has often focused on the figure of the transgressive hacker. Widely popularized in cinema and other popular media forms, the hacker figure offers important answers to some basic questions about Zoombombing as a disruptive practice. The hacker is posited as a skilled figure, both a user of and contributor to computing infrastructure and programming sectors and industries. The benevolent hacker uses their skill sets to educate others on the limits and often dangers of insecure computer networks and systems (Levy, 2010), though this may involve mocking the underdeveloped skills of others. The destructive “black hat” hacker conversely has made a comeback lately, in large part following claims of international political and economic cyberespionage, election disruption, and information disinformation (Shakarian et al., 2016).

The scholarly literature offers important insights on the role that anonymity plays in the figure and practice of the white or black hat hacker, while also emphasizing the technological motivation of such figures, to both secure or disrupt computer networks (Coleman, 2015). Such a definition harkens back to early conceptualizations of hackers as hobbyists who are mostly motivated by interests in testing the technical limits and social biases of technological objects and apparatuses (Caldwell, 2011). Given the widespread adoption of social media platforms, mobile media, and other consumer media technologies, however, technological expertise has widened among generations, creating a substantial divide between those who have grown up with the Internet and older generations who may possess limited knowledge or interest in using new media technologies (Livingstone, 2006). In other words, the figure of the hacker has been greatly diluted or perhaps increasingly mythologized, lessening its explicative power and conceptual framework for understanding the Zoombombing.

Broadly speaking, the hacking literature’s focus on technological disruptive also does not adequately account for the abusive manner in which individuals and groups are targeted on Zoom.

**Cyber-Abuse, Anonymity, Trolling, and Pranks**

The expansion and use of social media platforms are often cited as reasons for the rise in online forms of abuse and harassment, including widespread misogynist, racist, and homophobic attacks that occur online and extend to the gaming space (Banet-Weiser & Miltnner, 2016; Marwick & Caplan, 2018; Massanari, 2017; Powell & Henry, 2017). This literature is partly grounded in theories of media affordances, which recognizes that social media interfaces (especially vertical threads, tickers, and feeds) create a short attention span and, in turn, consequently abrasive “hot takes,” trolling and flame wars that receive the attention and reposts of users (Bucher & Helmond, 2018; Citton, 2017). Research on the far right or alt-right has also focused on social, political, and economic explanations for online hate
speech, cyber abuse, and harassment (Hawley, 2017; Munn, 2019; Nagle, 2017). While sharing these technological and political concerns, this study of Zoombombing cannot escape its overdetermined historical context, proliferating just as much of the world was coming to terms with a global health pandemic. A study of Zoombombing in other words must also take into consideration the disruption of critical work during an international health crisis.

Accordingly, not all Zoom meeting participants, however, might consider Zoombombing as an attack on—or disruption of—work. Given that early reports of Zoombombing noted their spread in educational settings, it would be remiss not to recognize youth-related explanations for disrupting a classroom or other meeting. “Pranking,” a popular term for playing a practical joke on an unsuspecting party, began to take on more crass and questionable tactics alongside most popular culture with the rise of cable television programming in the 1980s and 1990s. Television programs such as MTV’s Jackass also highlighted the intensely gendered element of prank culture, with young women being the butt of jokes, and a phalanx of events that end with young men being struck in the groin (Wiggins, 2014). The YouTube portion of our study plays a particularly important role in determining the extent to which the utterances of Zoombombing participants indicate playful disruptions or outright abusive practices.

Precursors to Zoombombing: Photobombing and Cyberflashing

While Zoombombing was enabled by a specific set of platform and technology-based affordances and security gaps, there are other like-minded practices—not just conceptual frameworks—that inform our study, and the broader social understanding of the disruptive online practices. As noted earlier, the term Zoombombing derives from “photobombing,” the term used to describe an unwelcome background pose or intrusion into a photo, typically a selfie. The Cambridge Dictionary defines the practice as “appearing . . . behind or in front of someone when their photograph is being taken, usually doing something silly as a joke,” (“Photobomb,” n.d.) highlighting the potential for blending of prankish appeal and disruptive or abusive interruptions. Photobombing is both a practice and an image genre involving a transgressive object or entity that subverts a conventional photographic setting to inject popular humorous appeal (Ibrahim, 2019). The photobomb is a distinctly Web 2.0 practice (Fletcher & Greenhill, 2010) that, as a form of user-generated content, integrates with the social practices of virality across platforms. Notably, the ocular appeal of photobombing and its “aesthetics of transgression” has been attributed to its unexpectedness and subversion of communal norms (Ibrahim, 2019, p. 1112).

Much can be gained from a conceptual comparison of photobombing and Zoombombing since both articulate the “conjoining of the banal and the ludic” (Ibrahim, 2019, p. 1116) in potentially producing a viral spectacle within the Internet economy. Indeed, Zoombombing has emerged out of the simultaneously extraordinary and banal experiences of everyday life during the COVID-19 crisis. As citizens shelter in place and practice social distancing, the “new normal” for students and non-essential workers has become largely integrated with Zoom and other teleconferencing platforms. Zoombombing disrupts the banality of everyday life during the epidemic by transgressing the boundaries of social norms and teleconferencing etiquette that are carried over from the physical practices that Zoom attempts to reproduce. However, the analogy of photobombing is lacking in several respects. Zoombombing is not just an image genre; as we will detail later, Zoombomb attacks can manifest as auditory spectacles, as utterances and exclamations from participants. And as early news reports highlighted (Lorenz, 2020), many Zoombombing attacks included various forms of hate speech and abuse—a stark contrast to the light-hearted and relatively harmless nature of photobombing. Finally, as previously noted Zoombombing does not appear to be a spontaneous practice, but rather involves a high degree of coordination due to the platform’s (albeit easily compromised) security protocols, and as we will detail, its organization, deployment across—and hosting on—a number of Internet platforms and properties.

In comparison to photobombing, we might contrast Zoombombing with the flash mob or flash rob. The term “flash mob” was first used in 2003 to describe a large coordinated crowd performance in Macy’s department store in Manhattan, New York City. The event, a situationist-like prank, saw approximately 100 participants follow a set of instructions shared through blogs and mobile phones. Upon arriving at a predetermined time, the crowd was instructed to surround an expensive rug, and inform the salesperson that the large group “all lived together in a free-love commune and that they wanted to purchase a ‘love rug’” (Nicholson, 2020, p. 6). The flash mob example, later dubbed “smart mobs” by early net culture theorist Howard Rheingold (2003), emphasized the ease through which large groups of users could be organized into coordinated actions. Like Zoombombing, flash mobs often lasted only a matter of minutes, sometimes seconds, with participants scattering quickly at the end of the event. And though seemingly spontaneous and ephemeral as events, flash mobs were well coordinated and often scripted, mobilized by a set or organizers using well-established communication networks and platforms.

By 2011, the rather harmless and amusing art of flash mobs would adopt the same social media enabled tactics to enact so-called “flash robs,” coordinated robberies that drew large crowds to specific targets (Skarda, 2011). While flash robs parallel the antagonistic elements of many Zoombombings, the comparison may be too ham-fisted; while one could argue that people’s time was “stolen” by zoombombers, the economic parallels end there. Rather, a...
more fitting comparison to Zoombombing, might be “cyber-flashing” (Thompson, 2016), the act of sending an abusive photo anonymously to an unsuspecting individual’s cell phone. The practice is most commonly associated with the circulation of pornographic and other jarring photo content shared through the wireless Bluetooth protocol from personal mobile phones. Like Zoom, Bluetooth has its own history of insecurity. Waling and Pym (2019) discuss the practice spreading through Apple’s airdrop protocol, in particular, highlighting the sending of pictures of penises, commonly referred to as “dick pics.” The sharing of similar pornographic images during Zoombombing has raised legal questions about the sharing of pornography, particularly to minors (Thompson, 2016). Cyberflashing therefore highlights how seemingly harmless and amusing events and performances can later turn into overtly abusive practices that target women and people of color.

Finally, while Zoombombing has yet to receive sustained study, our article offers complimentary approaches to Nakamura, Stiverson and Lindsey’s (2021) recently published short monograph entitled Racist Zoombombing. The authors argue that while Zoombombing is new, it is but another example of racist behavior that has plagued the Internet and its many properties, platforms and spaces since their inception. Unlike our study, Racist Zoombombing focuses largely on anti-Black racism, while also drawing on broader trends and explanations for hateful and toxic practices online (and off). The authors’ decision to interview three Black Zoom users adds a deep, rich, and disturbing understanding of the impact and harms of the racist practice of Zoombombing. Our study by contrast focuses more intensely on qualifying the practices and circulation of Zoombombing and not only their racist harms. The harm we seek to address is the framing of such acts are largely technological or somehow juvenile in nature, and not explicitly racist, misogynist, or otherwise socially toxic. To that end, Racist Zoombombing, where the authors indicate that they “. . . analyze artifacts from platforms where these campaigns unfold and draw out conclusions from their own words and actions” (Nakamura et al., 2021, p. 16) This approach is at the heart of our coding of Zoombombing practices on Twitter, Reddit, and YouTube. It is our contention, and our hope, that by distinguishing the different practices, platforms, and media objects produced by Zoombombing, that again, policymakers, educators, and platform regulators might better respond to its different manifestations and locations.

Methods, Data Collection, and Coding

As noted, our study employs a digital methods framework, an approach that seeks to understand not only the development of online cultures and practices, but also their intersection with the affordances of platforms (Rogers, 2013). This study of Zoombombing practices focused on three popular social media platforms: Reddit, Twitter, and YouTube. We anticipated that Zoombombing posts and utterances would take on different characteristics on each of these platforms: Reddit, a community-based platform was chosen because it has a more libertarian or “free speech” set of policies where transgressive and often hateful speech is commonplace; Twitter was thought to provide a more “public” and mainstream platform where messages could easily be reposted and thus go viral; and YouTube provided a stable and easily accessible video hosting site where Zoombombing videos captured from other video apps such as TikTok could be viewed. To capture Zoombombing related content, query-based keyword data collection was used for Twitter and YouTube (Elmer et al., 2012; Rogers, 2019). For example, on Twitter, we used the Twitter Capture and Analysis Toolkit (Borra & Rieder, 2014) to capture tweets containing a string or “basket” of Zoombombing related terms.2 From 28 April to 28 April 2020, we captured 42,104 tweets before using the Python standard library’s random function to collect a random sample of 1,000 tweets for qualitative coding. On YouTube, we queried for “zoombomb,” “zoom bomb,” “zoomattack,” “zoomraid,” “zoom raid,” and “online school trolling” and gathered all videos from the results. We removed news coverage, non-English content, videos with less than 1,000 views, and content that outlined security measures to defend against Zoombombing. We then qualitatively coded the 60 videos that received over 10,000 views.

The structure of Reddit made it easier to collect Zoombombing related content, as a keyword search on the platform revealed that a number of Zoombombing subreddits were created by users. Using a similar keyword query search noted earlier, we assembled a list of Zoombombing focused subreddits. While Reddit’s moderation team was vigilant in banning Zoombombing related subreddits, new subreddits would quickly crop up to replace those deleted. However, all had been shut down by 3 April 2020. We used the Pushshift application programming interface (API)4 to collect all posts and metadata from the following subreddit discussion groups: r/ShareOnlineClassroom, r/zoompranks, r/OnlineClassRaid, r/onlineclaslinks, r/onlineclaslinks2, r/zoombers, r/zoomboming, r/zoomraids, and r/zoomcodes. We used Reddit’s in-house “top” ranking of content to gather a sample of 300 posts from our dataset of 11,944.

Twitter: The Vox Populi?

Arguably, second only to Facebook in terms of media attention and controversy, Twitter’s sparse interface and vertical feed continues to have an outsized impact on social, political, and economic concerns of the day. Of course, Twitter’s standing as social media’s vox pop platform has dramatically worsened and subsequently been drawn into broader debates over free speech, online abuse, and platform censorship by the tweet happy former US president Donald Trump. The company’s decision to mark potentially abusive
and incorrect information posted by Trump (followed by his outright suspension) has only served to heighten attention and debate on the platform. Given the tendency for Twitter to focus on time sensitive matters of concern (Murthy, 2018) and its relative diversity of opinions and voices, we chose to begin our analysis on the microblogging platform. Following the previously noted a-semantic approach, we coded tweets according to their practice, the action that related to Zoombombing. We found five distinct Zoom practices in our sample (see Figure 1): tweets that broadly informed others by sharing news reports (“News Coverage,” 14.9%), sought to entertain or otherwise make light of such attacks (“entertainment,” 14.1%), explicitly targeted an individual or group for harassment and abuse (“targeting,” 15.9%), shared information on how to prevent attacks (“preventive precautions,” 25.6%), and finally, coordinated attacks (“coordination of attacks,” 29.5%). News coverage refers to stories of Zoombombing shared by media outlets or retweeted by users. An example of tweets coded as “entertainment” included, “I just found out ‘zoombombing’ is a thing I laughed really hard.” In contrast, the targeting of specific individuals or groups was evidenced by tweets that name a particular victim for an attack or address the problematic aspects of the targeting rationale; for example, “It’s [an] AA meeting full of drunks tryna [sic] get better everyone join #zoom #zoommeetings #zoomraid.” Some Twitter users disseminated preventive precautions outlined by cybersecurity experts to defend against Zoombombing: “Protect Your Videoconference from the ‘Zoombombing’ Epidemic [URL deleted].” Finally, Twitter also facilitated the coordination of attacks whereby users share Zoom meeting access codes or mobilize an engaged online community to join private channels dedicated to zoombombing: “TIRED OF BORRING [sic] TEACHERS? TAKE REVENGE BY SENDING THERE [sic] ZOOM CODE, AND LET US DO THE REST 😎.” Importantly, this last category does not specify a particular target, but facilitates the distributed practice of Zoombombing across platforms.

Figure 1 captures Zoombombing practices as found in tweets shared between 3 April and 1 May 2020, coded from a sample size of 1,000 randomly selected tweets. Nearly half of the tweets (45.4%) either sought to coordinate Zoombombing, often by sharing Zoom access codes, or explicitly targeted an individual or group. The prevalence of tweets that coordinate attacks is particularly notable given the platform’s reputation as a space for mostly discussion, debate, and the circulation of strong opinions. Nearly 30% of all tweets, the most of all our categories, served to explicitly encourage participation in Zoombomb attacks. That said, while Twitter is a relatively open and public platform for communication, users can still deploy anonymous usernames and profiles. That said, Zoombombers were not dissuaded from organizing in full view of others online. Tweets included the posting of zoom meeting addresses, instructions on how to participate, what meetings were closed, and other logistical posts such as “Tomorrow morning @ around 9am pst I’ll be streaming zoom raids so get rdy to send me your zoom class when I make my tweeeeet.”

Just over 25% of tweets, conversely, sought to place the practice of Zoombombing in the context of other computer and software threats, some posting specific advice on how to better use the Zoom platform, while others posted best practices or suggested other platforms: “Zoombombing: What it is and how you can prevent it in Zoom video chat . . . [URL removed].” Many tweets contained critical comments of the Zoom platform and bemusement about how the platform could be so insecure given the stakes at hand during the early days of the pandemic. Overall though, these tweets tended to be technical in nature and mostly stuck to advice on how to avoid Zoombombing and best secure online meetings. There were no tweets in this category that explicitly sought to prevent or otherwise address specific harms produced by racist or other abusive Zoombombs.

A significant percentage of tweets (15.9%) collected in this study specifically named online targets using Zoom ID codes, including Holocaust memorials, Asian community groups, Alcoholics Anonymous meetings, and various religious services. Thus, while the coordination coded tweets spoke in general terms about how to participate, this selection of tweets tended to be technical in nature and mostly stuck to advice on how to avoid Zoombombing and best secure online meetings. There were no tweets in this category that explicitly sought to prevent or otherwise address specific harms produced by racist or other abusive Zoombombs.
Elmer et al.

Reddit: The Organizational Hub

Billed as the “front page of the internet,” Reddit may be known to lay-users as the place to find cute cat videos, but it is also no stranger to controversy. In contrast to the digital agora of Twitter, where debates happen in full view, Reddit’s siloed sub-forums and threaded discussions foster closed communities among more “digitally literate” Internet users (Burton & Koehorst, 2020). The platform that birthed the #Gamergate coordinated harassment campaign, the infamous r/TheDonald subreddit behind the pizzagate conspiracy theory, and once voted its “jailbait” subreddit the Top Subreddit of the Year—indicating its status as a safe haven for “toxic technocultures” (Massanari, 2017). Reddit also serves as the mainstream end of what Benkler et al. (2018) calls the “propaganda pipeline,” where shocking or offensive content makes its way from the darker corners of the Internet like 4chan onto the relatively visible spaces of Reddit.

The prevalence of subreddits such as “zoompranks” and “OnlineClassRaid” suggested that the platform was largely being used as a staging ground for the Zoombombing of online classes and meetings. An analysis of 300 random posts from Zoombombing subreddits confirmed our suspicions (see Figure 2). Similar to our Twitter study, we categorized subreddit posts into five Zoombombing practices: deleted posts, coordination, targeting, exclamations, and admonishment. The pie chart below shows that nearly 70% of all posts served to coordinate Zoombombing, either by sharing practical advice, zoom meeting ID access codes, or other logistical information. One such post contained the following information: “I've made a discord server please feel free to join and help a brother out with some trolling.” While the vast majority of Reddit posts sought to facilitate Zoombombing, we also found a small percentage (6.69%) that targeted particular groups, including a lesbian, gay, bisexual, transgender (LGBT) social meeting and a breastfeeding support class. Users called upon others to attack their own class or teacher: “My English online class, do your worst :).” Some posts we coded as “exclamations” consist of short affective outbursts or reactions to Zoombombing, (e.g., “yeet,” “yo,” “LOL,” “LMAO”). A final subset of posts (1.7%) sought to admonish Zoombombing and the subreddit communities due to the economic disruption and social harm being caused:

My mother was in an extremely important work conference with hundreds of thousands of dollars on the line, and some dipshits zoombombed her. I get that classroom bombs are funny, but her company is already not doing so good due to the virus, and this may have just ruined her chances of remaining stable.

Like Twitter, Reddit offered limited data to study, often just short bursts of text. There were few full sentences, and even though it is billed as a discussion forum of sorts, we found little in the way of meaningful discussion or debate. Reddit served in short as an index of zoom codes or posts celebrating the online disruptions. But what did these disruptions and attacks actually entail? What did they look and sound like?

YouTube: Compiling Zoombombs

The video-sharing site and early Web 2.0 start-up, YouTube, was founded in 2005 and sold to Google in 2006. As a source of funny, bizarre, amateur, and professional content, it can be easily misconstrued solely in terms of “ephemeral entertainment” (Lange, 2008, p. 87). However, for a subset of participants, the “video vortex” (Lovink & Sabine, 2008) platform is also an imagined community (Anderson, 1991; see also Lange, 2008, p. 88), an interactional space where users comment on videos, subscribe to channels, and even carry out conversations through video (Manovich, 2008, p. 41). Thus, in studying YouTube, it is crucial not to efface its diversity of uses, but rather to consider its convergent affordances as video archive, educational resource, social messaging board, and performer or influencer platform.

Responding to this complexity, scholars have analyzed YouTube through lenses of “participatory culture” (Chau, 2010), “co-creative culture” (Burgess & Green, 2009), “convergence culture” (Jenkins & Deuze, 2008), and “remix culture” (Berry, 2008). In our YouTube study, we certainly observe creative practices in Zoombombing communities, as illustrated by transgressive aesthetics, influencer commentary, and the curatorial work of compilation videos. However, we are not inclined to adopt a creative approach to YouTube, but rather aim to address Zoombombing as a form of harassment and abuse.

Of all the platforms we studied, YouTube offered the most jarring view of Zoombombing, highlighting the popular and
controversial role that the platform played in offering videos of the “funniest moments” in Zoombombing. The large majority of these videos (85%) were roughly 10-minute compilations of multiple clips of zoom-bombs, many of which were initially shared on the popular TikTok platform. The remaining videos, also compilations, include commentaries throughout by YouTube micro-celebrities or influencers, individuals with large numbers of online followers. That said, there are important differences between posted video formats or “media objects.” Figure 3 represents the three distinct types of Zoombomb attacks, videos included an attack by a single user (i.e., a lone wolf), a micro-celebrity, or a mob-like raid in which a Zoom session is chaotically bombarded by multiple users. Our coding of Zoombombing user formats or types helps to further explain how Zoombombing was a coordinated practice. From seemingly random classes or meetings, to specific or sensitive targets, Zoom codes shared from fans to micro-celebrities, or sessions in which students organize a Zoombomb of their own class.

While Zoombombing videos and compilations are rife with laughter, they are hard to watch—many Zoom meeting hosts and participants were confused, irritated, or shocked by the actions and words of zoom-bombers. Teachers of smaller children looked traumatized. In short, we found Zoombombing videos contained a litany of abusive content (see Figure 4). While we found that a few zoom-bombs included light-hearted pranks that bemused some Zoom meeting participants, 86% of YouTube compilations also contained racist, misogynist, homophobic, and other toxic content. Much of this content was directed against female teachers in Zoom classroom meetings. While these categories represent a litany of abusive practices experienced on many other Internet platforms, our “Other” category (representing 14% of our sample), also highlights how Zoombombing specifically targeted health related meetings, for Alcoholics Anonymous (AA) and Narcotics Anonymous (NA).

The abusive content in Zoombombing videos moreover did not disappear after they were criminalized. As previously mentioned, reports of Zoombombing subsided after the FBI’s statement on 30 March, yet the circulation of Zoombombing videos on YouTube proliferated. As Figure 5 shows below within our data sample (videos posted between 26 March and 21 April), we see a clear surge in the number of posted Zoombombing videos on YouTube immediately following the FBI’s statement. This suggests that the notoriety of Zoombombing contributed to grow off the Zoom platform in the form of video content for YouTubers. Two videos posted on 10 April by two affiliated influencers, both of whom are high school aged males, provide commentary on the illegality of the practice after being charged with computer crimes and breach of the peace. Although one influencer, who has a following of over 3 million YouTube subscribers, explains that he is now unable to share new Zoombombing content, he nonetheless provides video commentary on the affair to update and further “entertain” his fanbase. Figure 6 further highlights the substantial growth in views of such videos in the weeks following our formal study, though on a positive side the increase in “dislikes” of these videos may serve as an indicator that the practice’s racist and toxic content is starting to be recognized and rejected by some viewers.

**Conclusion**

While Zoombombing seemingly lives on as a toxic form of YouTube “entertainment,” the phenomenon cannot be
displaced from its timing—just as a deadly global pandemic was taking hold around the world, leading to the closure of workplaces and educational institutions. Yet, as we first detail in our article, abusive behavior is a long-established practice on the Internet, and on other communication technologies that have been quickly and widely adopted by the general public. In this context, we found that Zoombombing does share many of the same characteristics exhibited by hackers, online trolls, pranksters, and abusers. But again, one of the striking differences in the case of Zoombombing is its timing, which may itself partly explain the rise of such online practices, or at least the speed at which it emerged and spread. The widespread disruption of everyday life, and the wholesale migration of education and many other organizational meetings to online platforms such as Zoom unsurprisingly produced a power vacuum, an opportunity to mock and harass. The prevalence of tweets that restated or reposted hacker like discussions of the Zoom’s platform thus served to not only define the issue in technological terms, as an insecure platform, but also to highlight how users sought to actively counter the often hateful and toxic interventions and attacks launched at unsuspecting Zoom participants. The timing of Zoombombing also placed a disproportionate focus on the disruption and spread of toxic and racist language and behavior during everyday work, health, and support meetings and of course classroom settings. Moreover, what our findings suggest with regard to the timing of Zoombombing and Zoom’s insecure platform, is that issues of hate, abuse, and racism were excluded from our Twitter posts. In other words, our research found that racism and abuse was never addressed as a harm by Twitter users who advised on how to mitigate the impact of Zoombombing. In short, we found that the abusive practice of Zoombombing was largely framed as disruptions of meetings, education, or work, enabled by technological insecurities.

Figure 5. Zoombombs over time.

Figure 6. Video Metrics for Zoombombs.
Our article’s sustained evidence of organized and coordinated attacks across all the platforms also qualifies the largely individualistic or memetic framing of Zoombombing as a form of trolling, particularly as an anonymous online practice. The coordination of Zoombombing was surprising prevalent on Twitter, commonly targeted “my classroom” on Reddit, and was more likely to be practiced by “mobs” and not individuals. Moreover, while trolling can often be dismissed as an individual act of attention seeking, we found that Zoombombing commonly targeted named individuals and meetings, often with racist and misogynist slurs. We would therefore likewise concur that the “Racist Zoombombing” conclusions of Nakamura et al. (2021) are much more befitting the practice than the trolling framework that suggests a more banal, everyday attempt to wind up Internet users or otherwise seek to produce a response to outrageous comments.

That said, our study of Zoombombing videos reposted to the YouTube video hosting site, while admittedly missing the “live” Zoom event and some associated sites where the practice was also enacted or reposted (TikTok, Discord, etc.), suggests that Zoombombing has morphed into a commercialized practice, a media object that has been curated and serialized by YouTubers and so-called influencers seeking to attract viewers, likes, and online advertising income. The framing of such videos by YouTubers suggests that at least they found such attacks as potentially income generating, and editorially acceptable content for their streams and accounts, reaffirming to a degree the framing of such attacks as forms of online “entertainment” or pranks, despite the preponderance of racist, sexist, homophobic, and hateful content. The legacy of Zoombombing, then, while exceptional in form and historical context, provides further damning evidence that online platforms, classrooms, and society writ large—including the frameworks deployed to explain online “disruptions”—must continue to question why the targeting of individuals and communities for toxic and racist practices and anti-phatic modes of address, are considered anything other than expressions of hate and abuse.

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is supported by Heritage Canada.

ORCID iDs
Greg Elmer https://orcid.org/0000-0002-5372-3072
Stephen J. Neville https://orcid.org/0000-0001-7731-7418
Anthony Burton https://orcid.org/0000-0001-6474-0313

Notes
1. See McNamara (2005) for an overview of media content analysis.
2. Our query strong included the terms “Zoom attack,” “Zoom bombed,” “Zoom bomber,” “Zoom raid,” “Zoom raids,” “Zoomattack,” “Zoombomb,” “Zoomraider,” “Zoombombed,” “Zoombombers,” “Zoom bombing,” “Zoombomber,” and “Zoombombing.”
3. These choices were made to focus on the more popular videos posted on the YouTube platform. The codebook for all datasets was aligned with our research questions and was conducted by two authors who negotiated and changed any variations in coding choices. Given the qualitative and digital methods goals of the article—that were not guided by questions of empirical reliability but rather cross-platform practice—the authors did not perform a coding reliability study.
4. For the application programming interface (API), see https://github.com/pushshift/api.
5. A study of purely anonymous acts online would make for a helpful follow-up study to determine the extent to which Zoombombers sought to hide their identity.
6. The rise of the so-called alt-right, supported and enabled by former US president Donald Trump is also a significant factor in abusive, racist, and misogynist activity on the Internet.

References
Anderson, B. (1991). Imagined communities. Verso Books.
Back, L., & Puwar, N. (2012). A manifesto for live methods: Provocations and capacities. The Sociological Review, 60(1), 6–17.
Banet-Weiser, S., & Miltnner, K. M. (2016). #MasculinitySoFragile: Culture, structure, and networked misogyny. Feminist Media Studies, 16(1), 171–174.
Benkler, Y., Faris, R., & Roberts, H. (2018). Network propaganda. Oxford University Press.
Berry, D. M. (2008). Copy, rip, burn: The politics of copyleft and open source: The politics of open source. Pluto Press.
Borra, E., & Rieder, B. (2014). Programmed method: Developing a toolset for capturing and analyzing tweets. Aslib Proceedings, 66(3): 262–278.
Bucher, T., & Helmond, A. (2018). The affordances of social media platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), The SAGE handbook of social media (pp. 233–253). SAGE.
Burgess, J., & Green, J. (2009). The entrepreneurial vlogger: Participatory culture beyond the professional/amateur divide. In P. Snickars & P. Vondrau (Eds.), The YouTube reader (pp. 89–107). National Library of Sweden.
Burton, A. G., & Koehorst, D. (2020, September 25). The spread of political misinformation on online subcultural platforms. Harvard Misinformation Review. https://misinforeview.hks.harvard.edu/article/research-note-the-spread-of-political-misinformation-on-online-subcultural-platforms/
Caldwell, T. (2011). Ethical hackers: Putting on the white hat. Network Security, 2011, 10–13.
Chau, C. (2010). YouTube as a participatory culture. New Directions for Youth Development, 2010, 65–74.
Citton, Y. (2017). The ecology of attention. Polity Press.
Coleman, G. (2015). Hacker, hoaxes, whistle-blower, spy: The many faces of anonymity. Verso Books.

Cox, J. (2020). Zoom IOS App Sends Data to Facebook Even If You Don’t Have a Facebook Account. VICE. https://www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-face-\
book-even-if-you-dont-have-a-facebook-account

de Zeeuw, D., & Tuters, M. (2020). The Internet is serious business: On the deep vernacular web and its discontentments. Cultural Politics, 16(2), 214–232.

Elmer, G. (1997). Spaces of surveillance: Indexicality and solicitation on the Internet. Critical Studies in Mass Communication, 14(2), 182–191.

Elmer, G., & Langlois, G. (2013). From networks to traffic tags: The circulation of discrete objects. Information Polity, 18(1), 43–56.

Elmer, G., Langlois, G., & McKeelvey, F. (2012). The permanent campaign: New media, new politics. Peter Lang Press.

Fan, C. (2020). Concerns growing over zoom bombing as hackers interrupt meetings. CBS. https://newyork.cbslocal.\
com/2020/04/03/zoom-bombing-hackers-hijacking/

Fletcher, G., & Greenhill, A. (2010). Photobombing: Mobility, humour and culture. In F. Sudweeks, H. Hrachovec, & C. Ess (Eds.), 2010 proceedings of the seventh international conference on cultural attitudes towards technology and communication, Vancouver, Canada, 15–18 June 2010 (pp. 198–206). School of Information Technology, Murdoch University. http://sammelpunkt.philo.at/2286/

Glaser, A., Kesslen, B., & Solon, O. (2020, March 26). In video chats, familiar forms of online harassment make a comeback. NBC News. https://www.nbcnews.com/tech/security/video-\
chats-familiar-forms-online-harassment-make-comeback-n1168806

Guattari, F. (1992). Chaosmosis. Indiana University Press.

Hawley, G. (2017). Making sense of the all-right. Columbia University Press.

Hjelmslev, L. (1961). Prolegomena to a theory of language. University of Wisconsin Press.

Ibrahim, Y. (2019). The vernacular of photobombing: The aesthetics of transgression. Convergence, 25(5–6), 1111–1122.

Jenkins, H., & Deuze, M. (2008). Editorial: Convergence culture. Convergence, 14(1), 5–12.

Johnson, D. (2020). Demand that Zoom immediately create a solution to protect its users from racist cyber attacks! Organizefor. https://campaigns.organizefor.org/petitions/demand-that-zoom-immediately-create-a-solution-to-protect-its-users-from-racist-cyber-attacks

Johnson, L. T. (2020). Case 5:20-Cv-02376: Class action complaint demand for jury trial. United States District Court Northern District of California.

Knorr, C. (2019). What’s AirDrop and Why are Kids Using it? Common Sense Media. https://www.commonsemsmedia.org/\
blog/whats-airdrop-and-why-are-kids-using-it

Konrad, A. (2019, May 31). Zoom, Zoom, Zoom! The exclusive inside story of the new billionaire behind tech’s hottest IPO. Forbes. https://www.forbes.com/sites/alexkonrad/2019/04/19/zoom-zoom-the-exclusive-inside-story-of-the-new-billionaire-behind-techs-hottest-ipo/

Lange, P. (2008). (Mis)conceptions about YouTube. In G. Lovink & S. Niederer (Eds.), Video vortex reader: Responses to YouTube (pp. 87–100). Institute of Network Cultures.

Levy, S. (2010). Hackers: Heroes of the computer revolution. O’Reilly.

Livingstone, S. (2006). Drawing conclusions from new media research: Reflections and puzzles regarding children’s experience of the Internet. The Information Society, 22(4), 219–230.

Lorenz, T. (2020, March 20). “Zoombombing”: When video conferences go wrong. The New York Times. https://www.nytimes.\
com/2020/03/20/style/zoombombing-zoom-trolling.html

Lorenz, T., & Alba, D. (2020, April 3). “Zoombombing” becomes a dangerous organized effort. The New York Times. https://www.\
ytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

Lovink, G., & Sabine, N. (Eds.). (2008). Video vortex reader: Responses to YouTube. Institute of Network Cultures.

Manovich, L. (2008). The practice of everyday (media) life. In G. Lovink & S. Niederer (Eds.), Video vortex reader: Responses to YouTube (pp. 33–44). Institute of Network Cultures.

Marczak, B., & Scott-Railton, J. (2020, April 3). Move fast and roll your own crypto: A quick look at the confidentiality of Zoom meetings. The Citizen Lab. https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

Marwick, A. E., & Caplan, R. (2018). Drinking male tears: Language, the manosphere, and networked harassment. Feminist Media Studies, 18(4), 543–559.

Massanari, A. (2017). #Gamergate and the fappening: How Reddit’s algorithm, governance, and culture support toxic technocultures. New Media & Society, 19(3), 329–346.

McNamara, J. (2005). Media content analysis: Its uses, benefits and best practice methodology. Asia Pacific Public Relations Journal, 6(1), 1–34.

Miller, V. (2008). New media, networking and phatic culture. Convergence, 14(4), 387–400.

Miller, V. (2015). Phatic culture and the status quo: Reconsidering the purpose of social media activism. Convergence, 23(3), 251–269.

Morris, D. Z. (2020, April 3). How to Stop Hackers from “Zoom Bombing” Your Zoom Video Chats. Fortune. https://fortune.\
com/2020/04/02/zoom-bombing-what-is-meeting-hacked-how-to-prevent-vulnerability-is-zoom-safe-video-chats/

Munn, L. (2019). Alt-right pipeline: Individual journeys to extremism online. First Monday, 24(6), Article 10108.

Murthy, D. (2018). Twitter. Polity Press.

Nagle, A. (2017). Kill all normies: Online culture wars from 4Chan and Tumblr to Trump and the alt-right. John Hunt Publishing.

Nakamura, L., Stiverson, H., & Lindsey, K. (2021). Racist Zoombombing. Routledge.

Nicholson, J. A. (2020). Flash! Mobs in the age of mobile connectivity. The Fibreculture Journal, 6, 1–15. http://six.\
fibreculturejournal.org/fcj-030-flash-mobs-in-the-age-of-mobile-connectivity/

Pearce, W., Ozbekla, S. M., Greene, A. K., Teeling, L., Bansard, J. S., Omena, J. J., & Rabello, E. T. (2020). Visual cross-platform analysis: Digital methods to research social media images. Information, Communication & Society, 23(2), 161–180.

Photobomb. (n.d.). https://dictionary.cambridge.org/dictionary/english/phothobomb

Powell, A., & Henry, N. (2017). Sexual violence: A feminist criminological analysis. In A. Powell & N. Henry (Eds.), Palgrave studies in cybercrime and cybersecurity: Sexual violence in a digital age (pp. 23–47). Palgrave Macmillan.
Rheingold, H. (2003). *Smart mobs: The next social revolution*. Basic Books.
Rogers, R. (2004). *Information politics on the web*. MIT Press.
Rogers, R. (2013). *Digital methods*. MIT Press.
Rogers, R. (2019). *Doing digital methods*. SAGE.
Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication, 35*(3), 213–229.
Setera, K. (2020, March 30). FBI warns of teleconferencing and online classroom hijacking during COVID-19 pandemic—FBI. Press Release. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
Shakarian, J., Gunn, A., & Shakarian, P. (2016). Exploring malicious hacker forums. In S. Jajodia, V. S. Subrahmanian, V. Swarup & C. Wang (Eds.), *Cyber deception: Building the scientific foundation*. Springer.
Skarda, E. (2011). Flash mobs turned criminal: The rise of flash robberies. *Time*. https://newsfeed.time.com/2011/05/12/flash-mobs-turned-criminal-the-rise-of-flash-robberies/
Stern, C. (2020). Husband pranks wife by wearing costumes in her Zoom work calls. *Mail Online*. https://www.dailymail.co.uk/femail/article-8297963/Husband-pranks-wife-wearing-funny-costumes-background-Zoom-calls.html
Thompson, L. (2016, February 3). #DickPics are no joke: Cyber-flashing, misogyny and online dating. *The Conversation*. http://thecconversant.com/dickpics-are-no-joke-cyber-flashing-misogyny-and-online-dating-53843
Waling, A., & Pym, T. (2019). “C’Mon, no one wants a dick pic”: Exploring the cultural framings of the “dick pic” in contemporary online publics. *Journal of Gender Studies, 28*(1), 70–85.
Wiggins, B. A. (2014). The culture industry, new media, and the shift from creation to curation; or, enlightenment as a kick in the nuts. *Television & New Media, 15*(5), 395–412.
Zoom. (2020, March 4). How to keep uninvited guests out of your Zoom event. *Zoom Blog*. https://blog.zoom.us/keep-uninvited-guests-out-of-your-zoom-event/

**Author Biographies**

**Greg Elmer** is Bell Media Research Chair and Director of the Infoscape Research Lab, Ryerson University.

**Stephen J. Neville** is a PhD candidate in the Communication and Culture graduate program, York University.

**Anthony Burton** is a PhD candidate in the Department of Communication, Simon Fraser University.

**Sabrina Ward-Kimola** is an MA student in the Communication and Culture graduate program, Ryerson University.