American Behavioral Scientist
1–22


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/00027642231155367
journals.sagepub.com/home/abs


Why Zoom Is Not Doomed Yet: Privacy and Security Crisis Response in the COVID-19 Pandemic

Wenhong Chen[1] and Yuan Zou[2]

Abstract

The COVID-19 pandemic not only fueled the explosive growth of Zoom but also led to a major privacy and security crisis in March 2020. This research examines Zoom's response to this privacy and security crisis with the aid of a producer's perspective that aims to direct attention to institutional and organizational actors and draws on theories of privacy management and organizational crisis communication. We primarily use data from 14 weekly *Ask Eric Anything* webinars from April 8 to July 15, 2020, to illustrate the strategies of Zoom's crisis response, especially organizational representation, the contours of its analytic account acknowledging and minimizing responsibility, and patterns of corrective and preventive action for user education and product improvement. Results demonstrate the usefulness of the producer's perspective that sheds light on how Zoom navigated the privacy and security crisis. Special attention is paid to the mobilization of networks of executives, advisors, consultants, and clients for expertise, endorsement, and collaboration. It is argued that Zoom's response strategies have contributed to Zoom's organizational mission and culture and reframed the crisis from a growing pain to a growth opportunity relating to privacy and security. Zoom's nimble, reasonable, collaborative, interactive yet curated organizational response to the privacy and security crisis can be seen as an unintended consequence of its sudden rise amid a global pandemic. It offers a useful model for tech firms' crisis response at a crucial moment for the tech industry around the world.

[1]Department of Radio-Television-Film, School of Journalism and Media, Department of Sociology, University of Texas at Austin, Austin, TX, USA
[2]School of Public Policy and Management, Heinz College, Carnegie Mellon University, Pittsburgh, PA, USA

Corresponding Author:
Wenhong Chen, Department of Radio-Television-Film, School of Journalism and Media, Department of Sociology, University of Texas at Austin, Austin, TX 78712-1139, USA.
Email: wenhong.chen@austin.utexas.edu

Keywords
privacy, security, organizational crisis communication, Zoom, COVID-19

The COVID-19 pandemic made Zoom Video Communications (hereafter Zoom) a verb as it became a popular video conferencing choice for remote work and learning, as well as happy hours, parties, weddings, holiday celebrations, live performance, or political campaigns. The explosive growth brought great scrutiny on Zoom's real or perceived privacy and security vulnerabilities and violations (Warren, 2020a). By the end of March 2020, Zoom was besieged by harsh criticism on its various privacy and security practices and growing competition from deep-pocket competitors such as Microsoft Teams, Google Meet, and Cisco WebEx. Analyzing Zoom's response to its privacy and security crisis during the COVID-19 pandemic advances the understanding of the socioeconomic and technical consequences of the pandemic.

Privacy and security issues can create serious risk and damage to governments, organizations, and individuals in the digital age. However, few studies have examined how organizations respond to privacy and security crises (see an exception in Kim & Lee, 2018), let alone during a global public health crisis when organizations are forced to adapt to an already fluid situation. This research advances a producer's perspective by directing attention to institutional and organization actors. It draws on theories of privacy management and organizational crisis communication to examine Zoom's response to its privacy and security crisis. We primarily drew data from 14 weekly *Ask Eric Anything* webinars from April 8 to July 15, 2020, complemented by Zoom corporate documents, press releases, public conference calls, corporate blog posts, and social media. We first trace the arc of Zoom's crisis response strategies, especially the contours of its analytic account acknowledging and reducing responsibility, and then identify patterns of its corrective and preventive action for user education and product improvement. Results show that Zoom navigated the privacy and security crisis through mobilizing networks of executives, advisors, consultants, and clients for expertise, endorsement, and collaboration. Moreover, its response strategies have built on and contributed to Zoom's organizational mission and culture, reframing the crisis as a growth opportunity for embedding privacy and security into its long-term goals rather than mere growing pains.

Background

The COVID-19 pandemic not only made Zoom popular but also tossed it into a major privacy and security crisis, leaving people wondering if it could survive. A wide range of criticisms and accusations were leveled against Zoom's privacy and security practices in March and April 2020, including misleading encryption claims, unnecessary data disclosure to Facebook and LinkedIn, possible remote control and attack through Zoom's macOS installer, and leaked Zoom usernames and passwords for sale on the dark web (Singer & Perlroth, 2020; Somers, 2020). Zoom was also criticized for traffic routing through data centers in China and business ties to China, which

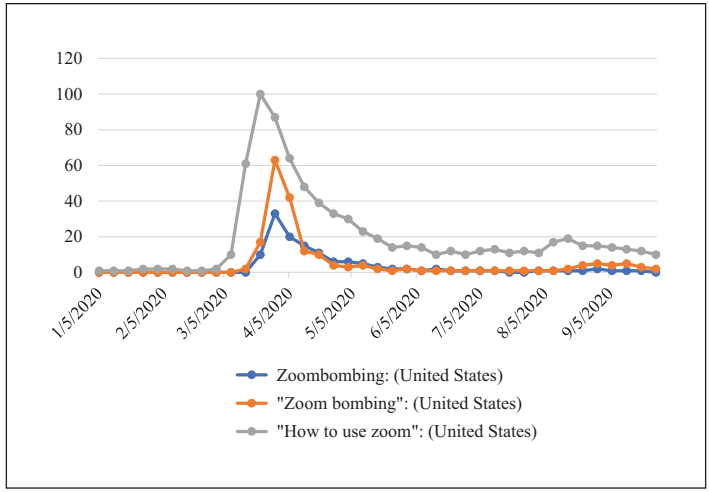

Figure 1. Google searches of "Zoom" and "Zoom bombing."

involved geopolitics and national security concerns (Chen, 2022). While some of these vulnerabilities required a sophisticated level of technical expertise to exploit, other tactics such as Zoombombing did not. Zoombombing refers to incidents when uninvited participants join a Zoom meeting and share offensive content such as hate speech, pornographic images, or violent threats.

As shown in Figure 1, Google searches in the United States for "how to use Zoom" peaked around March 22, 2020, and searches for "Zoom bombing" or "Zoombombing" peaked a week later, illustrating the public panic after many educational institutions adopted Zoom for remote learning after the spring break (Lorenz, 2020). In response, the Federal Bureau of Investigation in Boston issued a public warning about Zoombombing. The Department of Education of New York City, supervising one of the largest school districts in the nation, even asked its schools to stop using Zoom (Strauss, 2020).

In addition to Zoombombing, several lawsuits were filed accusing Zoom of misleading users or investors on the nature of its encryption or unlawfully sharing user data with third parties. Zoom's competitors in the video conferencing market such as Facebook, Google, and Microsoft, despite their own past privacy and security issues, restricted their employees' Zoom use, citing security concerns (Dixit, 2020). Moreover, they highlighted offering better privacy and security features than Zoom in their advertisements or press releases (Warren, 2020b).

Theoretical Framework: Privacy and Security Crisis Response

Like environmental, financial, or public health crises, privacy and security crises have become a latent side effect of modern societies, with critical social, political,

and economic ramifications in the digital age. Lockdowns caused by the COVID-19 outbreak have exacerbated this issue as they dramatically accelerated remote work and learning. Privacy and security breaches are rampant across industries (Chen et al., 2018). Many tech firms have reported major data breaches or have been exposed for dubious privacy practices such as collecting, analyzing, or sharing personally identifiable information for millions of users with third parties. In the United States, 35% of broadband households experienced identity theft, data theft, or a virus/spyware infection in the past 12 months (Parks Associates, 2019).

Aiming to develop the producer's perspective of privacy and security, our theoretical framework utilizes privacy literature and organizational crisis responses to analyze Zoom's response to the privacy and security crisis it experienced due to its rapid rise during the pandemic. We start with the privacy literature and highlight the necessity of moving the analysis beyond the level of individual users to organizational and institutional actors. We then draw on organization crisis communication literature, which while not centering on privacy and security crises still offers a useful framework to benchmark the patterns and strategies of Zoom's response.

A growing subset of privacy literature has been dedicated to the patterns, causes, and consequences of individual users' privacy concerns, motivations, skills, and behaviors, drawing on privacy management theory (Metzger, 2007; Petronio, 2013), privacy calculus theories, or digital inequality theories (Chen & Chen, 2015; Huang et al., 2018; Li et al., 2018; Park, 2013). By contrast, a producer's perspective examines the issue from the standpoint of industrial and institutional actors such as governments, corporations, media, advocacy groups, and user communities shaping privacy and security issues (Chen et al., 2018). A producer's perspective thus can shed light on the networks involved in the production and development of privacy and security practices.

First, privacy and security violations have become baked into the business model of digital platforms, especially those reliant on mining user data for advertising dollars (Pasquale, 2015). Apple CEO Tim Cook pointed out in 2015 that "Some of the most prominent and successful companies [in Silicon Valley] have built their businesses by lulling their customers into complacency about their personal information." Information and power asymmetry keep users from fully understanding what happens to their personal data shared on or collected by digital platforms. When using a digital product and service, users must "agree" or "accept" privacy policies that are often deliberately written in a tedious, obscure manner (Radin, 2015). Tech firms respond to this critique by hiding behind the privacy paradox narrative, arguing that users do not care about privacy, or cite the privacy tradeoff, claiming that users rationally give up privacy in exchange for a free service (Scoble & Israel, 2013). Interviews with 45 tech startups in the United States show that many entrepreneurs lacked the awareness, bandwidth, or capacity to treat privacy as a core business strategy or a top concern. Instead, most entrepreneurs adopt a build-the-plane-while-flying-it approach, adapting privacy policies and practices as the environment changes (Chen et al., 2018).

Second, problematic privacy and security practices can create organizational crises that undermine corporate reputation, customer loyalty, and public trust. Government

hearings, investigations, and regulations have emerged and intensified in the wake of recent scandals, although these efforts are often left behind by fast-moving technological innovations. In response, tech firms develop delay, denial, or deflection strategies to handle privacy and security crises (Frenkel et al., 2018). Reporting data breaches is often delayed, for example, it took an average of 280 days to identify a breach in 2020 (IBM Ponemon Institute Research, 2020). An "organized irresponsibility" (Beck, 1992, p. 155) spreads as the magnitude of direct loss is hard to assess. Yet, as Zoom noted in its 2019 U.S. Securities and Exchange Commission (SEC) filing, tech firms understand the security compromises "by our competitors, by our customers or by us may lead to public disclosures."

Crisis communication literature provides valuable insights on how organizations should respond during a crisis to restore their image in terms of representation and apology strategies, (Benoit, 1997; Coombs, 2012). First, organizational representation matters. The visibility and actions of a firm's CEO are crucial to the effectiveness of its crisis response, as the reputation and credibility of an organization and its leader are closely intertwined (Kim & Lee, 2018). A meta-analysis of more than 30 organizational crises suggests that the CEO must step up at the beginning of a crisis, particularly when organizational integrity is on the line (Lucero et al., 2009). Second, in restoring a tarnished image, organizations can respond with various strategies but apology seems more effective than others (Kim et al., 2009). Benoit (1997) describes five strategies of crisis response: denial, evasion of responsibility, reduction of offensiveness, corrective action, and mortification. The situational crisis communication theory (Coombs, 2012) consolidates response strategies into denial, diminishment, and rebuilding. The effectiveness of each strategy may vary by the crisis severity, the attribution of responsibility, public perception, cultural differences, and past record. An experiment reveals that stakeholders prefer apology to compensation when there is high attribution of crisis responsibility and public anger (Kiambi & Shafer, 2016).

Third, an apology is more than just saying sorry. Comparing official statements of 108 American and South Korean firms that experienced cybersecurity breaches, Kim and Lee (2018) identify that four major components of an apology include accepting responsibility based on analytic account (i.e., what has happened and why), expressing emotion toward stakeholders, reassuring the prevention of future failure, and offering corrections. Among these components, the analytic account is critical to the attribution of responsibility. Organizations can deny responsibility, claiming the crisis as an accidental, unintended consequence of benevolent action, defeasibility (lack of control), or victimization due to other actors' wrongdoing (Coombs, 2017). However, stakeholders may perceive denials of "intention, volition, and agency" as unjustified and develop greater distrust (Marcus & Goodman, 1991, p. 291). In addition, emotional signals such as shame, guilt, or compassion help to increase stakeholders' account acceptance and mitigate public anger (Kim & Lee, 2018). Last but not least, crisis communication must be backed up by corrective and preventive action that rectify or improve process, product, policy, or employee behavior (Marcus & Goodman, 1991). A fictitious case of a hotel facing a racially charged crisis shows that corrective action generates greater online engagement compared to other strategies (Triantafillidou & Yannas, 2020).

More recently, research has explored two emerging topics with growing importance: first, the use of digital media platforms in crisis communication, and second, the interaction between crisis response and organizational identity. On one hand, social media have broken the monopoly of mass media in crisis communication, allowing organizations to directly engage with stakeholders. On the other hand, the effectiveness of using social media for crisis response remains unclear. A case study of Lowe's apology after pulling ads from TLC's All-American Muslim suggests that Facebook might not be the best venue for crisis communication (Kinsky et al., 2014). In comparison, Twitter was found to be more useful than Facebook or Instagram on post-crisis reputation evaluation, positive social media engagement, and offline behavioral intention (Triantafillidou & Yannas, 2020). Just as importantly, an organization's crisis response that builds on its organizational mission and culture can contribute to its corporate identity (Cornelissen, 2004). A crisis can become an opportunity if organization leaders can mobilize resources in a timely, reasonable manner to implement immediate short- and long-term plans in line with their organizational identity.

2020 was not the first time Zoom faced privacy and security criticisms. In 2018, Zoom had a relatively slow overhaul of its security problem even after being notified and pushed by its client Dropbox (Singer & Perlroth, 2020). By contrast, the stakes in 2020 were much higher as the number of Zoom's users grew exponentially and the competition with established tech giants intensified during a global pandemic. It was crucial for Zoom to swiftly restore public trust and avoid the loss of newly gained users. Based on the theoretical framework at the intersection of the producer's perspective and organizational crisis communication, the research questions center on Zoom's crisis response strategies. More specifically, drawing on crisis communication literature, we investigate organizational representation, analytic account, corrective and preventive action, as well as the use of digital media platforms and their relations with organizational identity. Building on the producer's perspective, we are particularly interested in the network of organizational actors, both internal and external, involved in the response to the privacy and security response.

Data and Methods

This study primarily drew on text and video data of 14 weekly *Ask Eric Anything* webinars via Zoom and livestreamed on Zoom's YouTube channel on Wednesdays from April 8 to July 15, 2020, which Zoom used as a major venue to address its privacy and security crisis. The weekly webinar became monthly after July 15, 2020. The two authors participated in the webinars, watched the 15 hours of webinar recordings multiple times, and analyzed the transcripts. Table 1 shows the data source, duration, number of views, comments, likes, and dislikes for each webinar as indicated by YouTube. We assigned a number to each webinar based on chronological order for better reference. We used additional data to corroborate this information, including Zoom corporate documents such as quarterly and annual reports, SEC filings, corporate press releases, public conference calls, corporate blog and social media, as well as public interviews.

Table 1. Ask Eric Anything Webinars.

#	Citation	Length	Views	Comments	Like	Dislike
AEA1	Zoom. (2020, April 8). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=TeohYK-hsO4	43:27	34,110	58	254	29
AEA2	Zoom. (2020, April 15). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=VNVhDiWACwM	1:03:06	22,226	37	178	28
AEA3	Zoom. (2020, April 22). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=OGQpawfDRcA	1:00:57	19,520	26	147	21
AEA4	Zoom. (2020, April 29). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=tlC-sEdqY48	57:27	22,684	25	164	20
AEA5	Zoom. (2020, May 6). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=moN7tYbdhG0	58:15	18,083	41	133	24
AEA6	Zoom. (2020, May 13). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=OL_QyUhgySM	54:15	13,476	14	116	16
AEA7	Zoom. (2020, May 20). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=YRbZ9jOPB5g	59:39	13,777	35	122	24
AEA8	Zoom. (2020, May 27). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=deu07TL8mhc	59:25	14,603	28	116	24
AEA9	Zoom. (2020, June 3). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=-ZyYU81IaaM	57:43	16,743	30	123	21
AEA10	Zoom. (2020, June 10). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=-UGc9_-QANw	59:04	15,678	34	149	26
AEA11	Zoom. (2020, June 17). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=R4cn4qb_FoE	57:31	17,351	39	165	32
AEA12	Zoom. (2020, June 24). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=2bmvRATTMP8	57:56	12,796	25	110	19
AEA13	Zoom. (2020, July 1). *Ask Eric Anything* [Video file]. YouTube. https://www.youtube.com/watch?v=09Bb43Q6aZI	57:41	11,981	23	115	18
AEA14	Zoom. (2020, July 15). *Exclusive Chat with Zoom CEO* [Video file]. YouTube. https://www.youtube.com/watch?v=ar0ay7Spm-I	59:30	15,088	18	120	19
Total		887	24,8116	433	2,012	321

Table 2. The Panelists on the *Ask Eric Anything* Webinars.

Name	Title	Frequency	First appearance
Eric Yuan	Zoom Founder and CEO	14	April 8, 2020
Janelle Raney	Zoom Head of Product Marketing	13	April 15, 2020
Oded Gal	Zoom Chief Product Officer	13	April 15,2020
Brendan Ittelson	Zoom Chief Technology Officer	9	April 15,2020
Lynn Haaland	Zoom Deputy General Counsel, Chief Compliance and Ethics Officer, Chief Privacy Officer, former assistant United States attorney, started in January 2020	6	May 6, 2020
Max Krohn	Zoom Head of Security Engineering	4	May 13, 2020
Alex Stamos	Director, Stanford Internet Observatory, Hoover Institute visiting scholar, Zoom's outside security advisor, recruited in late March 2020, former CSO at Facebook and Yahoo	3	April 15, 2020
Gary Sorrentino	Zoom Global Deputy CIO, leader of Zoom's CISO Council, former managing director at J. P. Morgan Asset and Wealth Management	3	April 29, 2020
Lea Kissner	Outside Security and Privacy Consultant, former Global Lead of Privacy Technology at Google	2	April 22, 2020
Kristen Klein	Zoom Manager, Customer Marketing	1	April 8, 2020
Katie Moussouris	Founder, Luta Security, bug bounty program pioneer	1	May 20, 2020
Randolph Barr	Zoom Head of Product Security	1	June 24, 2020
Velchamy Sankarlingam	Zoom President of Product and Engineering, joined in late May	1	June 24, 2020
Aparna Bawa	Zoom Chief Operating Officer	1	July 1, 2020
Jason Lee	Zoom Chief Information Security Officer, former founder/CEO of Keybase	1	July 1, 2020
Cy Fenton	Chief Security Officer, Chief Privacy Officer and Senior Vice President, Global Infrastructure at Ralph Lauren	1	July 1, 2020
James Shira	Global and US Chief Information Technology Officer at PwC	1	July 1, 2020

Results

Except for the first webinar, the webinars followed a consistent format. All webinars were hosted by Zoom founder and CEO Yuan, moderated by Zoom's Head of Product Marketing Janelle Raney, and included Zoom executives, advisors, consultants, and clients as panelists. The webinars had a combined total of about a quarter of a million

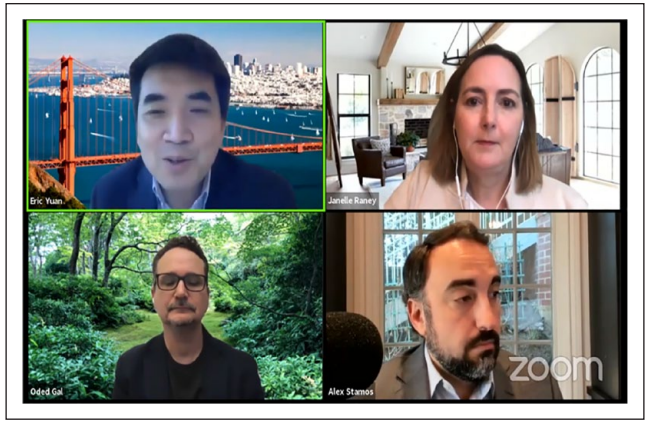

Figure 2. A screenshot of the *Ask Eric Anything* Webinar (April 15, 2020).

views, 433 comments, 2,012 likes, and 321 dislikes as of December 2020. To contextualize these numbers, few of Zoom's recent Facebook posts or Tweets received similar levels of public engagement. On the other hand, several "How to Zoom" tutorials on the firm's YouTube channel boast of millions of views.

While the main purpose was to present Zoom's key initiative for privacy and security fixes and updates for "user education," Zoom used the webinars to engage and cultivate its user communities: introducing top recruits in privacy and security, calling participants to recommend experts to Zoom, or sharing "your stories of how you're using Zoom both personally and for work, education, business, government, [and] health care" (Raney, AEA12). Table 2 shows the names and titles of the 17 Zoom executives, advisors, consultants, or clients that appeared in the webinars, their frequency of participation, and the date of their first webinar appearance. The projected openness, the focus on privacy and security, and the presence of Yuan and his top lieutenants were the central feature of each webinar from April to July 2020 (Figure 2).

On the one hand, media are used to serve as the major domain for the construction, contestation, and criticism of risk and crisis, on the other hand, organizations increasingly use social media to advance their narratives and influence public opinion. Media events used to be spectacles broadcast live through television to a national or international audience and served as "mediatized rituals" that created and mobilized collective sentiments and identity (Cottle, 2006). The *Ask Eric Anything* webinars constructed "mediatized" routines to perform and reinvent Zoom's organizational identity through executive representation and reassurance, advance the firm's framing of its privacy and security practices during, before and beyond the crisis, and ultimately restoring public trust.

Organizational Representation and Reassurance

Privacy and security lapses and halfhearted, slow responses are commonplace in the tech industry, which gives Zoom some cover and partially mutes its competitors'

criticisms. Compared to the tech industry's common tactics, Yuan's post *A Message to Our Users*, published to Zoom's website on April 1, 2020, offers not only a quick apology but also a plan of action. In the apologetic blog, Yuan wrote that "we recognize that we have fallen short of the community's—and our own—privacy and security expectations. For that, I am deeply sorry, and I want to share what we are doing about it." He said Zoom would devote all its engineering resources to a 90-day campaign to "better identify, address, and fix issues proactively," and a weekly *Ask Eric Anything* webinar open to the public "for a candid conversation with Eric" with a moderated live Q&A starting on April 8 (Yuan, 2020a).

In the first *Ask Eric Anything* webinar, Yuan promised "laser focus on privacy and security" from the "entire team" during the self-imposed 90-day feature freeze. Yuan and his executives promised throughout the 14 webinars that Zoom would be open, transparent, and honest, and "do what it takes to maintain your trust" (Yuan, AEA3). Yuan's down-to-earth, matter-of-fact, earnest, and accessible demeanor telegraphed sympathy toward users to decrease their concerns, while also presenting Zoom's analytic account and explaining how the company was utilizing its resources to improve their product. Yuan was echoed by his executives and consultants throughout the 14 webinars through phrases such as "privacy [and] security first," privacy and security as the "one thing," "very committed," "high confidence," or "we really understand that privacy is very important." Such a swift and straightforward response to privacy and security issues is rare in the tech industry. Alex Stamos, highly respected for his candid criticism of tech giants' privacy and security practices when he served as Facebook's Chief Security Officer and in similar roles, was brought in by Zoom as an outside advisor in late March. He compared Yuan favorably to other CEOs in the second webinar: "Eric has been incredibly dedicated to this issue and all of the executives at Zoom have made security and safety and the trust of their users their number one priority" (AEA2).

Analytic Account

The attribution of responsibility is based on an analytic account, which is the critical step that sets the tone for the rest of the crisis responses. Zoom's analytic account included an acknowledgement and minimization of responsibility, while also explaining what happened and humblebragging about its record and achievements. For example, in the first webinar, Yuan reiterated Zoom's privacy and security flaws as "missteps" due to "our urgency to help" new users, who flocked to the Zoom platform after the pandemic created an unprecedented need for remote work and learning. In this narrative, Zoom's privacy issues were the unintended consequence of a benevolent action—providing an essential service for free to millions of workers and students forced online by the pandemic. This framing was further reinforced in Yuan's apologetic blog (2020a), where he carefully separated "areas where we are strengthening our platform and areas where users can take steps of their own to best use and protect themselves on the platform."

Yuan and his executives also reminded the public that Zoom's platform was not originally designed for individual consumers, but rather for enterprise clients ranging from "the world's largest financial services companies to leading telecommunications

providers, government agencies, universities, healthcare organizations, and telemedicine practices" (AEA4). Zoom offered built-in, preconfigured security features and trainings to the in-house IT teams of these enterprise clients, who, for their part, had "done exhaustive security reviews of our user, network, and data center layers and confidently selected Zoom for complete deployment" (Yuan, AEA4, see also AEA7). This account showcased both the background of Zoom's product development and its strong track record. Just as importantly, the focus on enterprise clients allowed Zoom to differentiate itself from the prevailing business model of tech firms. As declared in Yuan's apology blog and subsequent webinars, Zoom was not in the business of selling user data. Lynn Haaland, Zoom's Chief Privacy Officer, assured webinar participants that "we do not sell your data in any way; we never have and we have no intention of doing so in the future" (AEA8). She explained that "the Zoom platform is our product, you are not our product" and "we would like to sell the Zoom platform and provide the service to you" (AEA9). Not surprisingly, Yuan invited webinar participants to compare Zoom's privacy and security record with its competitors, asking "Is Zoom safe compared to peers?" and answered his own question immediately with a confident "yes" (AEA1).

In addition, Yuan attributed a large share of Zoom's privacy and security issues to the vast amount of "brand new consumer use cases" (AEA1), a message reinforced multiple times at multiple webinars. These new users were "utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived . . . ." (Yuan, 2020a).

Zoom executives and supporters took the opportunity during the webinars to point out Zoom's popularity in a highly competitive market and humbly hinted that the platform became a victim of its own success. Zoom was free for meetings shorter than 40 minutes. As a stand-alone, sole-purpose service, it did not require casual users to sign in. It was scalable for large group meetings and allowed third-party app compatibility. Zoom had better functionality and features than its competitors, such as breakout rooms or virtual backgrounds. The ease of use was "the platform's trademark" (Max Krohn, AEA8) and Zoom was "one of the easiest platforms to use of any kind" (Cy Fenton, AEA13). For instance, Janelle Raney read glowing praise posed as a question from one webinar participant, who said that "Zoom has long been known for its ease of use. The term 'It just works' has become synonymous with how customers felt about Zoom" (AEA6). However, because people could use Zoom with no or minimal training, Yuan said, many overlooked or ignored privacy protection features such as locking the meeting or enabling the waiting room (AEA3). Even users who supposedly had advanced privacy knowledge and skills could make mistakes. The British Prime Minister posted screenshots to Twitter of a Zoom call with government ministers that had a visible meeting ID (Lillington, 2020).

Corrective and Preventive Action: User Education and Product Changes

Zoom's Chief Product Officer Oded Gal said the analytic account guided Zoom's two-pronged approach to addressing privacy and security flaws: user education and

product changes (AEA12). In the first webinar on April 8, Zoom acknowledged not being "thoughtful enough about educating new users" (Yuan, AEA1). The analytic account said that individual users lacked knowledge about privacy awareness or protection, which led to Zoom's user education efforts during the webinars and beyond. Examples of these efforts included introducing privacy and security features, asking users to check Zoom's privacy and security webpages, and urging them to adopt privacy protection behaviors. Zoom simplified its privacy policy "so everyone can understand" (Yuan, AEA1) and added details to its website "about our policies, how we handle privacy and all the rights under [the General Data Protection Regulation]" (Ittelson, AEA3). Yuan instructed webinar participants to "have a password right now," while Brendan Ittelson, Zoom's Chief Technology Officer, encouraged them to adopt longer passwords (AEA4) and Alex Stamos suggested they "use a password manager" (AEA5). Lynn Haaland encouraged participants almost in every webinar she appeared in to "take a look at our privacy policy" (AEA4) and invited them to "go early and often and check out the privacy and security webpages" as Zoom would "try to post as many useful resources as we can" (AEA9). Indeed, beside the webinars, Zoom had workshops, video tutorials, and webpages to equip users with better skills, including but not limited to privacy and security skills. Given the sensitivity of educational data, Zoom rolled out a dedicated K-12 privacy policy and guidelines for K-12 users on setting up secure virtual classrooms through waiting rooms and restricted content sharing.

Even before Yuan's apologetic blog and the webinars, Zoom started to improve its privacy and security features. Yet, the webinars provided a weekly venue during the 90-day campaign to showcase over 100 of Zoom's new or improved privacy and security features and user interface refinements, according to Aparna Bawa, Zoom's Chief Operating Officer who oversaw the company's security efforts (AEA13). To address privacy and security accusations, major product changes included giving users more privacy and security controls, easing user concerns about data surveillance, and upgrading to industry-standard end-to-end encryption (E2EE).

Zoombombing was perhaps the most urgent privacy and security issue that landed Zoom in the negative spotlight, because Zoom's previous default settings allowed meeting participation without password requirements and screensharing by any participant. New features were added to give users greater and easier privacy and security control such as default security settings, required passwords, the waiting room, the "report a user" feature for reporting inappropriate or offensive behavior, and host control of muting, screen sharing, or chat (Yuan, AEA9). Zoom also tried to quiet users' concerns about data surveillance. Zoom removed the controversial attendee attention tracker feature originally designed to monitor corporate meeting participants, and Brendan Ittelson assured participants that Zoom meetings were only recorded when explicitly requested by the host. Max Krohn, Zoom's Head of Security Engineering, pledged that Zoom had no backdoor or "ability to monitor meetings" (AEA4). Zoom's misrepresentation of its E2EE capability created a false impression that it offered better data protection than it actually did. Although most users might not understand the technical details, the revelation damaged Zoom's organizational integrity and public

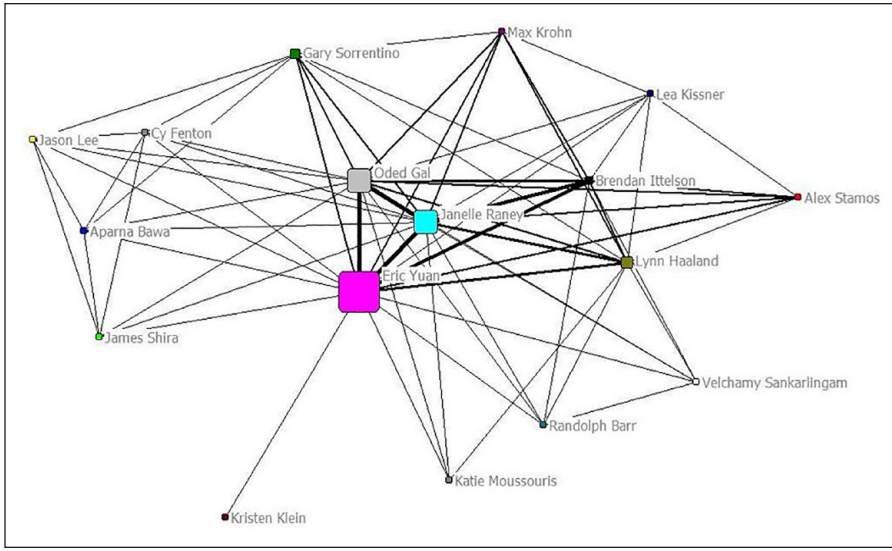

Figure 3. The coappearance network of the *Ask Eric Anything* webinar panelists.

trust. While Yuan (2020a) described it as a "confusion" in his apologetic blog, Oded Gal (2020) acknowledged "a discrepancy between the commonly accepted definition of E2EE and how we were using it" in an apology posted the same day. Zoom upgraded its E2EE to the common industry standard in May 2020 and celebrated it as a key milestone, given the large size of meeting participants Zoom allowed (Stamos, AEA7).

Collaboration Networks of Privacy and Security

Besides the strategies illustrated through the lens of organizational crisis communication, a producer's perspective of privacy management helps to shed light on how privacy and security practices involve a network of stakeholders. Tech startups often rely on professional and organizational networks to learn how to develop privacy policies and practices (Chen et al., 2018). It was thus interesting to observe how Zoom promptly developed and showcased a collaborative network of privacy and security experts stocked with newly hired top executives, consultants, and clients with global name recognition. Zoom hired A-list privacy and security heavyweights, such as executives or outside consultants who had worked for or with global tech giants such as Facebook, Microsoft, or Google, to "review and make enhancements to our products, practices, and policies" (Yuan, 2020a). They were introduced and displayed in the webinars together with Zoom's top clients (see a list in Table 2). Figure 3 illustrates the appearances of 17 Zoom executives, consultants, and clients in the 14 webinars. Yuan, as Zoom's CEO and the host of the webinars, had the top betweenness centrality score, an indicator of his centrality in linking different clusters of executives, consultants, and clients together, followed by Janelle Raney, the moderator of the webinars, Oded

Gal, CPO, Lynn Haaland, Deputy General Counsel, and Gary Sorrentino, Global Deputy CIO.

Among the hired guns, Yuan announced in the first webinar that Alex Stamos would help Zoom conduct a comprehensive security review as an outside advisor. Serving as the director of the Stanford Internet Observatory and a visiting scholar at the Hoover Institution, Stamos is well known and respected for his candidness and outspokenness about big tech's privacy and security practices. Stamos introduced himself in the second webinar and described his career in cybersecurity:

> I did a lot of work with big companies helping them fix their security issues as well as responding to crises . . . I joined Yahoo as their Chief Information Security Officer and then moved to Facebook as the CSO where I spent a little over three years.

Lea Kissner was recruited as a consultant in April and introduced in the third webinar as an expert who spent "many years at Google working to build respect for users into products and systems through product design, privacy enhancement, enhancing infrastructure application, security and novel research into both theoretical and practical aspects of privacy" (AEA3). Among top executives recruited since April 2020, Max Krohn became Zoom's Head of Security Engineering in May after Keybase, a security and encryption firm he founded, was acquired by Zoom (Yuan, AEA9). Jason Lee, a 20-year security expertise veteran who spent time at firms such as Microsoft or Salesforce, joined Zoom as its Chief Information Security Officer (CISO) in June 2020 (AEA13). Beneath the top executives, Zoom also built and kept expanding an offensive security team (AEA4). In addition, Ginny Lee, Associate General Counsel for Privacy, Mara Davis, Associate General Counsel for Compliance and Ethics, Andy Grant, Head of Offensive Security, and a new Head of Vulnerability and Bug Bounty were recruited in July (Yuan, 2020b).

Besides hiring superstars in the privacy and security space and basking in their glow, Zoom formed a CISO Advisory Council to lead the comprehensive review and initiated a bug bounty program. The advisory board consisted of "security leaders from VMware, Netflix, Uber, Electronic Arts, and others" (Yuan, 2020c). Gary Sorrentino, Zoom's Global Deputy CIO, led a CISO Council comprising "39 of the leading security experts across many various industries such as technology, financial services, retail, professional services, government, education, health care, manufacturing, communication, biotech, pharma agriculture and other agriculture industries and they include some very well-known security experts . . ." (AEA1, see also AEA11). The bug bounty program was handled by Katie Moussouris, recruited as Zoom's Security Advisor, and her company Luta Security, in May 2020 (AEA3). Moussouris pioneered the bug bounty program at Microsoft and the U.S. Department of Defense. The bug bounty program called for outside security researchers and hackers to discover Zoom's security flaws and vulnerabilities (Stamos, AEA3). Randolph Barr, Zoom's Head of Product Security, urged hackers to "submit their research over to security" (AEA4). Furthermore, Zoom hired respected third-party security firms such as Trail of Bits, NCC Group, and Bishop Fox (Yuan, 2020c) to review its platform

including its use of public and colocated data centers, cloud configuration, external IP space, internal production network, web application, and corporate network (see also Bawa, AEA14). In the 13th webinar celebrating the successful completion of the 90-day privacy and security improvement campaign, Yuan thanked a long list of the CISO Council, industry partners, third-party researchers, and advocacy organizations (AEA13). In return, council members gave Zoom rave reviews. For instance, Cy Fenton, Ralph Lauren's top privacy and security officer, lauded Zoom that "your ears really are perking up when we start talking" (AEA13).

The namedropping, the display of the variety of industries in which Zoom's clients operate, the invitation to the bug bounty program, and the third-party review were just some of Zoom's response strategies to project expertise, credibility, and trustworthiness in its privacy and security practices. Moreover, these connections and collaborations gave Zoom access to expertise, influence, and a layer of protection when attacked or criticized. For instance, Zoom initially announced the full E2EE service as a premium for paid but not for free users. Criticized by advocacy groups, Zoom explained that the intention of leaving its free service unencrypted was to balance user privacy "with the safety of vulnerable groups," a decision informed by input from "civil liberties organizations and our CISO Council, child safety advocates, inclusion experts and government representatives and also our own users and also others as well to gather their feedback on this feature" (Yuan, AEA9). Zoom eventually offered E2EE protection to all users (Yuan, AEA11).

Mission, Culture and Identity: "DNA" and a "Journey"

Another issue not fully addressed in the crisis communication literature is the relationship between crisis response and organizational identity. The analytic account and corrective and preventive action developed during a crisis response coevolve with the organizational mission and culture, which can be revised retrospectively or added ad-hoc (Weick & Browning, 1986). Zoom changed its official mission from "Make communications frictionless" to "Make video communications frictionless and secure" since the crisis response to privacy and security. Executives emphasized that "protecting users' privacy has always been a part of the mission and Eric's vision" (Haaland, AEA9). The newfound commitment to privacy and security was elevated—if in retrospect—as an integral part of Zoom's "DNA" and corporate culture of "delivering happiness" (Yuan, AEA10, see also AEA13, AEA14). Privacy and security were purposely embedded into Zoom's company culture as "pillars" that made Zoom unique, joining the other pillars of availability, agility, and cost, according to Velchamy Sankarlingam, President of Product and Engineering (AEA12). In other words, the privacy and security DNA must be built "into the fabric of how you work" and "the security agenda has to be married to the overall agenda, technical agenda, and strategic agenda" (Cy Fenton, AEA13).

Over time, Yuan's rhetoric of balancing ease of use with security gradually moved to "privacy and security are always more important than usability" (AEA6, see also AEA3). In the July 1 webinar, Zoom announced the 90-day campaign successfully

completed and declared that privacy and security had been adopted as a top priority for product design (AEA13, see also AEA11). Zoom said that mechanisms had been put in place to prioritize privacy and security "in each phase of our product and feature development" (Yuan, 2020c) from the designing, building, and testing stages to production (see also Oded Gal, AEA14). Moreover, Zoom's privacy and security crisis was reinterpreted from a growing pain into a growth opportunity allowing Zoom to become an industry leader and standard-bearer through collaboration with partners, clients, and users, and helping the firm "transform our brand to be a security first and a frictionless collaboration service" (Yuan AEA3, see also AEA4, AEA6). Heralding Zoom's E2EE upgrade, Yuan positioned Zoom as "an industry leader with regards to encryption security for open and interoperable video communications at a scale" (AEA9).

A journey is the other metaphor used by Zoom executives during the privacy and security crisis response, particularly to represent the company's long-term commitment to the practices it was implementing. Although merely 5 weeks into Zoom's 90-day campaign, Janelle Raney stated that "security issues are few and far between" (AEA5), and Yuan and other Zoom executives pledged to "[double] down on privacy and security" as part of the "focus on customer experience" (AEA4, see also AEA6, AEA9, AEA10, AEA13). Aparna Bawa confirmed that the end of the 90-day campaign was "really just the beginning. Our work on privacy and security is never done" (AEA13). The journey metaphor also referred to the companionship and camaraderie with fellow travelers on their way to a shared destination, a community effort, and "a team sport" (Fenton AEA13). Yuan saw privacy and security as a way to "keep this open dialogue with our users' community" (AEA9). Jason Lee used both the DNA and journey metaphors when he declared his goal as Zoom's CISO was "to partner on the product roadmap and really instill that security DNA into our products" (AEA13).

Discussions and Conclusions

Zoom's privacy and security journey is not finished yet. In November 2020, the FTC (2020) and Zoom settled for a Consent Agreement on Zoom's security misrepresentation dating back to 2016 and required implementation of better security measures. Nonetheless, Zoom's crisis response seemed to be well-received. Zoom remains popular as various stakeholders from the government, media, and users have given it a second chance. Eric Yuan was chosen as Time Magazine's Business Person of the Year. Zoom's explosive growth may have peaked as vaccinations help more people return to the workplace and school and Zoom's ease of use, scalability, and functionality advantages shrink as major competitors add similar features. Zoom's lack of business or social networking makes it difficult to create network effects among its users. Both these achievements and challenges suggest the critical significance of Zoom's 90-day crisis response in 2020.

Our analysis centers on how Zoom, a young tech firm that rapidly evolved from a small enterprise service provider into a household name as a consequence of the COVID-19 pandemic, responded to a major privacy and security crisis. The topic is

highly relevant and significant to the understanding of the socio-technical and economic consequences of this still-ongoing global pandemic. Our theoretical framework is innovative, integrating organizational crisis responses and the producer's perspective on privacy and security management. Besides the strategies illustrated through the lens of organizational crisis communication, a producer's perspective of privacy management also helps shed light on how privacy and security practices involve a network of stakeholders.

Using data from 14 weekly webinars between April and July of 2020, and drawing on the producer's perspective of privacy management and the crisis communication literature, our research into Zoom's crisis response strategies produced the following findings. First, in line with the crisis communication literature, we identify Zoom's organizational representation, the contours of its analytic account, and the corrective and preventive actions taken by the company. The extent and manner in which top leaders, principally the CEO, engaged in crisis response directly affected response outcomes. Different from the tech industry's common tactics of delay or distraction, Zoom's CEO Eric Yuan swiftly issued an apologetic blog to repair Zoom's reputation and to increase public confidence. Zoom's analytic account included both acknowledging and reducing responsibility, pointing out that (a) Zoom was originally designed for enterprise clients with in-house IT support and (b) many privacy and security issues Zoom was criticized for, especially Zoombombing that stirred public panic, came from the sudden influx of new customer users who rushed to the platform for its ease to use but often ignored or were unfamiliar with its privacy and security features. The attribution of responsibility set the tone for corrective and preventive action. Zoom made a great effort to educate users on new and improved privacy and security features through webinars, tutorials, and other venues. The company also quickly fixed many of its problematic privacy and security flaws to deal with Zoombombing and other vulnerabilities. Acknowledging its early claim of offering clients E2EE as confusion rather than deception, Zoom eventually provided industry-standard encryption service to both paid and free users.

Second, the producer's perspective of privacy management helps shed light on the interrelations and interactions of multiple stakeholders that shaped Zoom's responses to the privacy and security crisis. Zoom promptly expanded its organizational networks through (a) recruiting privacy and security heavyweights as executives, advisors, and consultants and (b) rallying clients and third-party experts to conduct a comprehensive review of its platform and revamp its bug bounty program to fix security weaknesses. Endorsements from clients and influencers lent Zoom credit and allowed it to claim transparency, accountability, and competence.

Third, while crisis communication literature has examined the patterns and effectiveness of crisis response in terms of messaging and action, our findings foreground the importance of organizational identity. Zoom's crisis response strategies built on and contributed to its organizational mission and culture, reframing the crisis as a growth opportunity to build its brand as a reliable, trustworthy platform and its position as an industry standard-bearer. Zoom shifted from balancing usability and security to putting privacy and security first. Adding "secure" to its organizational mission,

Zoom claimed to implement a mechanism at each stage of its product cycle to embed privacy and security into its DNA and continue its privacy and security journey through open dialogues with its clients and users.

Last but not least, using social media platforms allowed Zoom to engage its users in a direct, interactive, and curated manner. Zoom used the *Ask Eric Anything* webinars as a mediatized routine to perform its organizational identity through executive representation and reassurance, advance the firm's framing of its privacy and security practices during, before, and beyond its privacy and security crisis, cultivate a user community, and ultimately restore public trust. As one of Zoom's clients told webinar participants, if privacy and security was a journey, "what happened with Zoom is to have that journey occur in the public square like worldwide, real-time" (James Shira, AEA13).

This research makes several contributions. Theoretically, a producer's perspective points to the necessity of examining institutional and organizational actors that shape the construction and production of privacy policies and practices, along with other structural drivers such as the prevalent business model of the digital economy, the catch-up nature of privacy laws and regulations, and the asymmetrical cost and benefit of noncompliance. Zoom's privacy and security crisis response offers an illustrative case on the limitations of individual-level analysis if structural forces such as regulatory and industry factors set the parameters of privacy and security practices within which individual users choose from a finite number of options. Our work also enriches the crisis communication literature, which has not paid enough attention to how organizations develop and mobilize networks of executives, advisors, consultants, clients, and third-party experts to navigate a crisis, or how organizations must engage with a web of stakeholders for an effective response to mitigate negative outcomes such as damaged reputation and user exodus. Methodologically, the crisis communication literature tends to employ experiments using vignettes for fictitious cases or content analysis of a corporate statement. By innovatively analyzing 14 webinars, this study suggests that digital media platforms have become a critical venue for crisis response strategies and studies.

The limitations of this study call for future research through comparative cases of privacy and security crisis responses in different legal and regulatory settings, or organizational responses to other types of crises such as environmental disasters, collapsed buildings, or leadership failures amid an ongoing global pandemic. The time period of our research centers around Zoom's 90-day campaign of addressing its privacy and security issues. Future research may consider a longitudinal approach to investigate the sustainability of corrective and preventative actions, the evolution of collaborative networks, as well as the extent to which privacy and security have been prioritized or become part of the organizational mission. As our analysis here focuses on crisis response strategies based on the *Ask Eric Anything* webinars, future research might be interested in content analysis such as the use of specific words and tones.

Regulators and the public have become increasingly impatient with the tech industry's often halfhearted, condescending, and misleading responses to privacy and security issues, whose significance has been further magnified by the pandemic as digital

platforms prove essential for work, education, and daily life. Zoom's nimble, reasonable, collaborative, interactive, and curated organizational response to its privacy and security crisis offers a useful model for tech firms' crisis responses at a crucial moment for the tech industry around the world. Our findings provide evidence-based practical insights. Existing and emerging government cases against tech firms such as Facebook, Google, and others in the United States, Europe, and beyond show that regulatory scrutiny has intensified and accumulated public resentment can cloud the future of the tech industry. Addressing a major crisis during the global pandemic, firms need to rapidly analyze the situation, design and craft messages delivered by calm, confident, and compassionate leaders who convey transparency and competency, and provide analytic accounts on what happened and evaluate its options. While there is no one-size-fits-all crisis strategy and firms have different values and resources, Zoom's crisis response offers insights on the importance of a timely apology, reasonable accreditation of responsibility based on a persuasive analytic account, and mobilizing networks for expertise and endorsement that legitimize and optimize corrective and preventative actions informed by and that contribute to the organizational mission and culture. We hope this exploratory study will inspire more research employing the producer's perspective to understand organizational crisis responses to privacy and security issues and beyond.

Acknowledgments

The authors are thankful to the Woodrow Wilson Center for International Scholars. The first author was a visiting fellow with the Kissinger Institute on China and the United States as well as the Science and Technology Innovation Program and the second author was an intern at the Wilson Center in 2020.

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: The first author also thanks the support from the Chiang Ching-kuo Foundation. The views and opinions expressed here are solely those of the authors.

References

Beck, U. (1992). *Risk society: Towards a new modernity* (*Vol. 17*). Sage.

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review*, *23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0

Chen, W. (2022). Zoom in and zoom out the glocalized network: When transnationalism meets geopolitics and technopolitics. *Information, Communication & Society*, *25*(16), 2381–2396. https://doi.org/10.1080/1369118X.2022.2118545

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Chen, W., Huang, G., Miller, J., Lee, K. -H., Mauro, D., Stephens, B., & Li, X. (2018). "As We Grow, It Will Become a Priority": American mobile start-ups' privacy practices. *American Behavioral Scientist*, *62*(10), 1338–1355. https://doi.org/10.1177/0002764218787867

Coombs, W. T. (2012). *Ongoing crisis communication: Planning, managing, and responding* (3rd ed.). Sage.

Coombs, W. T. (2017). Revising situational crisis communication theory. *Social media and crisis communication*, *1*, 21–37.

Cornelissen, J. (2004). *Corporate communications*. Sage.

Cottle, S. (2006). Mediatized rituals: Beyond manufacturing consent. *Media, Culture & Society*, *28*(3), 411–432. https://doi.org/10.1177/0163443706062910

Dixit, P. (2020, April 8). Google told its workers that they can't use Zoom on their laptops anymore. *BuzzFeed News*. https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom

Frenkel, S., Confessore, N., Kang, C., Rosenberg, M., & Nicas, J. (2018, November 14). Delay, deny and deflect: How Facebook's leaders fought through crisis. *The New York Times*. https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

Gal, O. (2020, April 1). The facts around Zoom and encryption for meetings/webinars. *Zoom Blog*. https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/

Huang, G., Li, X., Chen, W., & Straubhaar, J. D. (2018). Fall-behind parents? The influential factors on digital parenting self-efficacy in disadvantaged communities. *American Behavioral Scientist*, *62*(9), 1186–1206. https://doi.org/10.1177/0002764218773820

IBM Ponemon Institute Research. (2020). *Cost of a Data Breach Report 2020*. https://www.ibm.com/security/digital-assets/cost-data-breach-report/

Kiambi, D. M., & Shafer, A. (2016). Corporate crisis communication: Examining the interplay of reputation and crisis response strategies. *Mass Communication and Society*, *19*(2), 127–148. https://doi.org/10.1080/15205436.2015.1066013

Kim, N., & Lee, S. (2018) Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea. *International Journal of Business Communication*, *58*(4), 2329488418777037. https://doi.org/10.1177/2329488418777037

Kim, S., Avery, E., & Lariscy, R. (2009). Are crisis communicators practicing what we preach? An evaluation of crisis response strategy analyzed in public relations research from 1991 to 2009. *Public Relations Review*, *35*, 446–448. https://doi.org/10.1016/j.pubrev.2009.08.002.

Kinsky, E. S., Gerlich, R. N., Brock Baskin, M. E., & Drumheller, K. (2014). Pulling ads, making apologies: Lowe's use of Facebook to communicate with stakeholders. *Public Relations Review*, *40*(3), 556–558. https://doi.org/10.1016/j.pubrev.2014.03.005

Li, X., Chen, W., & Straubhaar, J. D. (2018). Concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication*, *12*, 1269–1290.

Lillington, K. (2020, April 2). Think you're bad at video-conferencing? Boris Johnson is worse. *The Irish Times*. https://www.irishtimes.com/business/technology/think-you-re-bad-at-video-conferencing-boris-johnson-is-worse-1.4218175

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

Lucero, M., Tan Teng Kwang, A., & Pang, A. (2009). Crisis leadership: When should the CEO step up? *Corporate Communications: An International Journal*, *14*(3), 234–248. https://doi.org/10.1108/13563280910980032

Marcus, A. A., & Goodman, R. S. (1991). Victims and shareholders: The dilemmas of presenting corporate policy during a crisis. *The Academy of Management Journal*, *34*(2), 281–305. https://doi.org/10.2307/256443

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, *58*, 2078–2091. https://doi.org/10.1002/asi.20672

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*, 215–236. https://doi.org/10.1177/0093650211418338

Parks Associates. (2019, July 9). Parks associates: 79% of Consumers are concerned about data security or privacy issues. *PR Newswire*. https://www.prnewswire.com/news-releases/parks-associates-79-of-consumers-are-concerned-about-data-security-or-privacy-issues-300881440.html

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*, 6–14.

Radin, M. (2015). *Boilerplate: The fine print, vanishing rights, and the rule of law*. Princeton University Press.

Scoble, R., & Israel, S. (2013). *Age of context: Mobile, sensors, data and the future of privacy*. Patrick Brewster Press.

Singer, N., & Perlroth, N. (2020, April 20). Zoom's security woes were no secret to business partners like dropbox. *The New York Times*. https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html

Somers, M. (2020, December 9). Zoom's CFO on 3 ways to fix mistakes during rapid growth. *MIT Sloan*. https://mitsloan.mit.edu/ideas-made-to-matter/zooms-cfo-3-ways-to-fix-mistakes-during-rapid-growth

Strauss, V. (2020, March 31). FBI issues warning about 'hijacking' of online classes by intruders after schools report serious disruptions. *The Washington Post*. https://www.washingtonpost.com/education/2020/03/31/fbi-issues-warning-about-hijacking-online-classes-by-intruders-after-schools-report-serious-disruptions/

Triantafillidou, A., & Yannas, P. (2020). Social media crisis communication in racially charged crises: Exploring the effects of social media and image restoration strategies. *Computers in Human Behavior*, *106*, 106269. doi:https://doi.org/10.1016/j.chb.2020.106269

Warren, T. (2020a, April 1). The pressure mounts as Zoom risks becoming a victim of its own success. *The Verge*. https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response

Warren, T. (2020b, April 29). Google and Microsoft chase after Zoom with new features and free services. *The Verge*. https://www.theverge.com/2020/4/29/21240942/google-meet-free-zoom-response-microsoft-teams-features

Weick, K., & Browning, L. (1986). Argument and narration in organizational communication. *Journal of Management*, *12*, 243–259.

Yuan, E. (2020a, April 2). A message to our users. *Zoom Blog*. https://blog.zoom.us/a-message-to-our-users/

Yuan, E. (2020b, April 8). Update on Zoom's 90-day plan to bolster key privacy and security initiatives. *Zoom Blog*. https://blog.zoom.us/update-on-zoom-90-day-plan-to-bolster-key-privacy-and-security-initiatives

Yuan, E. (2020c, July 1). CEO report: 90 Days done, what's next for Zoom. *Zoom Blog*. https://blog.zoom.us/ceo-report-90-days-done-whats-next-for-zoom/
Zoom Video Communications, Inc. (2019). Form 10-Q. Retrieved from SEC EDGAR.

Author Biographies

Wenhong Chen is an associate professor of media studies and sociology, the founding codirector of Center for Entertainment and Media Industries, and a Distinguished Scholar in the Robert Strauss Center for International Security and Law at the University of Texas at Austin. She has more than 90 publications, including articles in top-ranked journals in the fields of communication and media studies, sociology, and management.

Yuan Zou graduated from the Heinz College, School of Public Policy and Management, Carnegie Mellon University in 2021 with a Master's degree and worked as an intern at the Woodrow Wilson Center for International Scholars in 2020 in Washington, DC.