

Zoombombing Your Toddler: User Experience and the Communication of Zoom's Privacy Crisis

Journal of Business and Technical
Communication

1-7

© The Author(s) 2020



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/1050651920959201

journals.sagepub.com/home/jbt



Sarah Young¹

Abstract

In spring 2020, not only did the teleconferencing platform Zoom experience an onslaught of new users who were now social distancing due to the COVID-19 crisis, but it also faced its own crisis due to the privacy of its product. For those working in technical and professional communication, the Zoom example illustrates not only a way to communicate in an emergency but also a way that privacy can cause a crisis in the first place. Drawing from literature on crisis communication and the experiences users described in the Zoom CEO's blog post, the author concludes that while Zoom did indeed have technical issues that contributed to its privacy crisis, users also experienced its technology in unexpected ways, and the company underestimated the privacy expectations of its new users. Zoom's privacy crisis ultimately provides a useful discussion of why it is increasingly important for companies to incorporate privacy by design and to be frank

¹Erasmus University Rotterdam, Rotterdam, Zuid-Holland, Netherlands

Corresponding Author:

Sarah Young, LEaDing Fellows Postdoc, Erasmus University Rotterdam, 3000 DR, Rotterdam, Zuid-Holland, Netherlands.

Email: young@eshcc.eur.nl

about their privacy practices with a public who has a growing interest in, and dissatisfaction with, corporate privacy practices.

Keywords

corporate blogging, crisis communication, online meetings, privacy, user experience

In early April 2020, students in the Netherlands were remotely meeting with their class on the videoconferencing software Zoom, taking social distancing measures due to COVID-19, when they were unexpectedly subjected to “pornographic and racist images” (Mühlberg, 2020). This practice of hijacking a videoconference to insert offensive content has become so global, from children’s storytelling to church services, that it has been dubbed “Zoombombing” (Read, 2020). This was not Zoom’s only privacy issue though, and Zoom faced other criticisms for their software, such as those concerning encryption and data-gathering issues (Wagenseil, 2020). In response to criticism of Zoom’s technology, Zoom and its CEO, Eric S. Yuan, utilized an important platform for CEO communication, the corporate blog (Ngai & Singh, 2014), releasing a series of messages to address the company’s privacy and security controls. But what appears to drive Zoom’s privacy crisis was not always a failure of technology. The crisis was also driven by a failure of user assessment. By providing a content summary of Zoom’s “A Message to Our Users,” published on its blog on April 1 (Yuan, 2020), I demonstrate that while Zoom does indeed have technical issues that contribute to its privacy crisis, another important catalyst of Zoom’s crisis was its failure to understand customer expectations. This article, then, provides a useful contribution to discussions of the privacy crisis, a crisis that can only increase as more activities are carried out online in a post-COVID-19 environment.

The Privacy Crisis and User Experience

Zoom’s issues fall under a larger genre of crisis—the privacy crisis. For an organization, a crisis is an incident or event that represents “a threat to the organization’s reputation and viability” (Pearson & Mitroff, 1993, p. 49) and can range from something grave to a matter of maligned public perception (Choi & Chung, 2013). And according to Rule (2012), *privacy* has been defined in terms of values and claims to personal autonomy or the desire for

protection from disclosure. Put together, the privacy crisis, then, involves, at minimum, a threat that revolves around both the values and the legalities of controlling individuals' visibilities or information. A privacy crisis can be caused by a variety of things, such as when cell phone numbers and addresses are leaked during a natural disaster (Wu et al., 2011), personal information is leaked during corporate data breaches (Veltos, 2012), or, in the case of Zoombombing, a technology fails to live up to privacy expectations by allowing internet trolls to bombard toddlers with pornography and racism during story hour.

Privacy lapses can affect user experience because privacy is one aspect that users assume will be part of technologies. A satisfying user experience, then, can depend on whether users believe their privacy is protected. While what is a "reasonable" expectation of privacy has been debated (McArthur, 2001), users tend to expect at least some measure of privacy when they are online (Yao et al., 2007). Developers are thus encouraged to think about what users expect from products and either meet those expectations or transparently communicate potential concerns (Senarath & Arachchilage, 2018).

"A Message to Our Users"

Zoom illustrates what appears to be a privacy crisis due to its inability to determine user expectations. The disconnect between user privacy expectations and what Zoom delivered is best seen through a content summary of Yuan's April 1, 2020, "A Message to Our Users," in which he addressed at least 17 privacy matters the company was dealing with (Yuan, 2020). I will briefly summarize the three basic sections of this message. In the first, untitled section, Yuan

- explained how he and Zoom appreciated being able to facilitate connectivity during the current health crisis.
- acknowledged that users grew from 10 to approximately 200 million, with the target audience no longer enterprises but instead a whole range of private users.
- commented that Zoom "did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home."
- admitted shortcomings by saying that "we recognize that we have fallen short of the community's—and our own—privacy and security expectations."

- apologized for the past and foreshadowed a response plan for the future.

In the second section of the blog, “What We’ve Done,” Yuan outlined Zoom’s response to the privacy crisis by

- naming current privacy issues (like Zoombombing).
- listing specific dates when the company had already addressed privacy concerns.
- focusing on updated privacy policies and controls for education users and explaining more technical issues that involved the collection of data.

Finally, in the third section, “What We’re Going to Do,” Yuan

- outlined outstanding privacy and security issues.
- unveiled a 90-day plan stressing transparency and collaboration.
- concluded with this call to Zoom users: “Together, let’s build something that can truly make the world a better place!”

A main takeaway from this message emerges in the first, untitled section, consisting of seven paragraphs in which Yuan detailed how Zoom failed to understand its users. In doing so, Yuan implied that if Zoom had understood the potential uses of its product or imagined how the company would grow, it could have preemptively addressed many privacy concerns before they affected a mass number of individuals.

This failure to preemptively address privacy concerns is especially illustrated by the case of Zoombombing. Privacy controls such as passwords and waiting rooms as well as screen-sharing controls existed in the software, but they were not set by default. Instead, Zoom focused on appealing to users’ desire to easily join a conference rather than on the privacy controls that would make it harder for them to join (Peters, 2020). The company seemed to assume that Zoom users wanted convenience over privacy, but the backlash against Zoombombing proved otherwise. Users wanted privacy, and some rejected Zoom because of its perceived vulnerabilities. Looking at unintended uses, then, should be a basic function of user experience (UX) research, as Lauer and Brumberger (2016) explained:

Ideally, UX also strives to accommodate how users appropriate information products and content in unanticipated ways and for their own purposes as well

as how those products position users to act in the world by the way they are designed and the options they allow for. (p. 248)

Had the company exercised a little more foresight into potential uses, at least for Zoombombing, it might have been able to prevent at least one very public crisis.

While privacy satisfaction is not as commonly discussed as other measures that aid in better user experience, such as a low error rate, it is increasingly important to consider. If there is a mismatch between technological function and technological expectations, like there was with Zoom, users might have a negative experience and turn away from the product in general. As Zoom found out when their product was shunned by a variety of audiences (Hellard, 2020), expectations for a more autonomous control of information are rising higher on the list of what users might consider fundamental technological needs.

Conclusions for Post-COVID-Privacy Crises

Overall, while brief, this discussion of Zoom's privacy crisis provides a good entry point into the conversation on contemporary privacy crises and the importance of considering user expectations. In the future, this discussion can help make the "privacy-as-crisis" more visible, which is especially critical in a post-COVID-19 world where people's everyday activities are increasingly occurring online. Further, the creeping digital surveillance of medical information and the many other ways of digitally staying connected while socially distancing make it more and more important to think about both privacy by design (Langheinrich, 2001) and the privacy ideologies technological affordances grow out of this ever-more online and surveillance-aware world.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project has received funding from the European Union's Horizon, 2020 research and innovation programme under the Marie Skłodowska Curie grant agreement No 707404.

References

- Choi, J., & Chung, W. (2013). Analysis of the interactive relationship between apology and product involvement in crisis communication: An experimental study on the Toyota recall crisis. *Journal of Business and Technical Communication*, 27(1), 3–31. <https://doi.org/10.1177/1050651912458923>
- Hellard, B. (2020, April 9). *Who has banned Zoom and why?* <https://www.cloudpro.co.uk/collaboration/8518/who-has-banned-zoom-and-why>
- Langheinrich, M. (2001). Privacy by design: Principles of privacy-aware ubiquitous systems. In G. D. Abowd, B. Brumitt, & S. Shafer (Eds.), *Ubicomp 2001: Ubiquitous computing* (pp. 273–291). Springer. <https://doi.org/10.1007/3-540-45427-6273-291>
- Lauer, C., & Brumberger, E. (2016). Technical communication as user experience in a broadening industry landscape. *Technical Communication*, 63(3), 248–264.
- McArthur, R. (2001). Reasonable expectations of privacy. *Ethics and Information Technology*, 3(2), 123–128. <https://doi.org/10.1023/A:101189801029>
- Mühlberg, B. (2020, April 8). *Zoom-bomb: Porn, racist content streamed to students during online class.* <https://nltimes.nl/2020/04/08/zoom-bomb-porn-racist-content-streamed-students-online-class>
- Ngai, C., & Singh, R. (2014). Communication with stakeholders through corporate Web sites: An exploratory study on the CEO messages of major corporations in greater China. *Journal of Business and Technical Communication*, 28(3), 352–394. <https://doi.org/10.1177/1050651914524779>
- Pearson, C., & Mitroff, I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *The Executive*, 7(1), 48–59.
- Peters, J. (2020, April 3). *Zoom adds new security and privacy measures to prevent Zoombombing.* <https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms-default>
- Read, B. (2020). *“Zoombombing” is a horrifying new trend.* <https://www.thecut.com/2020/04/what-is-zoombombing.html>
- Rule, J. (2012). “Needs” for surveillance and the movement to protect privacy. In D. Lyon, K. D. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 64–71). Routledge.
- Senarath, A., & Arachchilage, N. (2018). Understanding user privacy expectations: A software developer’s perspective. *Telematics and Informatics*, 35(7), 1845–1862. <https://doi.org/10.1016/j.tele.2018.05.012>
- Veltsos, J. (2012). An analysis of data breach notifications as negative news. *Business Communication Quarterly*, 75(2), 192–207. <https://doi.org/10.1177/1080569912443081>

- Wagenseil, P. (2020, May 9). *Zoom privacy and security issues: Here's everything that's gone wrong (so far)*. <https://www.tomsguide.com/news/zoom-security-privacy-woes>
- Wu, S. Y., Wang, M. H., & Chen, K. T. (2011). Privacy crisis due to crisis response on the Web. In G. Wang, S. R. Tate, J. Chen, & K. Sakurai (Eds.), *2011 IEEE 10th international conference on trust, security and privacy in computing and communications* (pp. 197–205). Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/TrustCom.2011.28>
- Yao, M., Rice, R., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722. <https://doi.org/10.1002/asi.20530>
- Yuan, E. S. (2020, April 1). *A message to our users*. <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users>

Author Biography

Sarah Young is a LEaDing Fellows Postdoc at Erasmus University Rotterdam. She researches surveillance and technical communication, especially artificial intelligence in the law enforcement context. She previously worked in the United States as a security clearance investigator.