Seeking Connectivity: Grappling with Data Privacy in Digital Social Settings

Morgan Banville, Massachusetts Maritime Academy
Danielle Koepke, Marquette University

This article overviews how computers and writing scholars may grapple with data privacy in a gaming application, and on a social media platform. We question how privacy impacts the embodied experiences of the people interacting in those digital spaces. To address the complexities of data privacy, we discuss the precarity of information in digital spaces in the wake of *Roe v. Wade* being overturned. Our article questions: how do computers and writing scholars navigate spaces that gamify our work and create connectivity, while simultaneously putting our privacy at risk? How can, or should, computers and writing scholars support digital activist projects for reproductive justice while also negotiating issues of privacy and data collection? The article contributes to understanding data privacy concerns through connectivity in gaming spaces and through storytelling experiences on Instagram to advance advocacy for and against reproductive justice. Computers and writing scholars have a role in designing, circulating, and caring for digital stories and the bodies connected to them; as such, they should critically engage with digital advocacy stories and the privacy invasion embodied by storytellers.

Keywords: data privacy, gaming, graduate students, advocacy, embodiment

As scholars in computers and writing, we believe that, because we play a role in designing, circulating, and caring for digital stories and the bodies connected to them, we should also critically engage with digital advocacy stories and the privacy invasion embodied by storytellers. Throughout the article, we provide suggestions for computers and writing scholars and instructors, whom we view to overlap significantly with technical communicators and technical and professional communication (TPC) courses. As such, this critical engagement extends to how we teach digital advocacy and privacy within the TPC classroom. To address the complexities of data privacy, or how individuals control their personal information, we discuss the precarity of information in these digital spaces in the wake of *Roe v. Wade* being overturned. We believe that, in the wake of the court ruling, digital spaces used for connectivity became even more precarious due to the restrictions and legalities of sharing private information,

 DOI: https://doi.org/10.37514/PCW-B.2025.2616.2.02

such as any content related to reproduction (i.e. birth control, menstruation, abortion, etc.). The Supreme Court's June 2022 ruling in *Dobbs v. Jackson Women's Health Organization* overturned *Roe v. Wade* and eliminated the federal constitutional right to abortion. Since then, many state legislatures have created new abortion restrictions and bans. Research has shown that abortion bans of all types have the greatest impact on people in marginalized groups (Oberman, 2022; Jarman, 2015; McGinn Valley et al., 2023; Foster 2020). In particular, Liza Fuentes (2023) showed how individuals who face systemic racism and other forms of oppression, especially Black and Indigenous women, may encounter compounding barriers to obtaining an abortion. Reproductive justice is an important site for inquiry due to its intersections with other social justice issues, digital activism, and ongoing political turmoil. We highlight the tension between the need to share for activist purposes/in precarious situations and the privacy risks associated with that sharing. The virtual workspace that we highlight is a space where privacy risk is elevated, as is social media.

In this article, we interrogate data privacy as it manifests in a gaming application called Gather.Town and on the social media platform Instagram, contributing to further understanding(s) of how precarious events, such as the COVID-19 pandemic and nationwide abortion bans, has changed the United States' habits of work and play in digital spaces, especially as it relates to surveillance. We follow Morgan Banville's (2023) definition of surveillance, which is the "collection of both visible and invisible data/information derived from those being observed, suggesting an application of power over the observed audience, who are often not informed of such collection" (p. 32). We consider how privacy impacts both digital spaces and the embodied experiences of the people interacting in those digital spaces (Johnson et al., 2015). We therefore question: how do computers and writing scholars navigate spaces that gamify our work and create connectivity, while simultaneously putting our privacy at risk? How can, or should, computers and writing scholars support digital activist projects for reproductive justice while also negotiating issues of privacy and data collection?

Definitional Work: The Surveillance Assemblage

As Estee Beck and Les Hutchinson Campos (2021) noted, "scholars of computers and writing have addressed issues of surveillance and privacy within writing infrastructures through course management systems, plagiarism detection software, and social media used in classrooms" (p. 3). This article does have implications for classroom use; however, it can further contribute to writing infrastructures, defined as the role language, through writing and identification, plays in shaping our understanding of objects and bodies

(Boyle, 2018; Ching, 2018). Infrastructures are not neutral, and "exert agency over everything from how we communicate to how bodies move" (Frith, 2020, p. 406). Our case examples contribute to understanding data privacy concerns through connectivity in digital infrastructures such as Gather.Town and Instagram to advance advocacy for and against reproductive justice. We specifically focus on examples that assist computers and writing scholars with negotiating privacy concerns in digital spaces, all the while grappling with seeking connectivity. Users seeking connection in digital gaming and social media spaces often navigate tensions between genuine connectivity and sacrifice of privacy. [1]These social spaces of digital connection offer users a feeling of control over their profile, interactions, and information; the reality is that users are not in control of their data privacy—technology companies are. We view technology companies' role in collecting data as an example of the powerful ways in which surveillance capitalism persists (Zuboff, 2019). The intricacies of the privacy tradeoff and grappling with connectivity contribute to ways that users are involved in the surveillance assemblage. The surveillance assemblage is complex and inextricably tied to privacy and data concerns, lateral surveillance, and consent.[2]

Joseph Turow, Michael Hennessy, & Nora Draper (2016) for example, indicated that marketers are misrepresenting a large majority of Americans by claiming that Americans give out information about themselves as a tradeoff for benefits they receive (p. 3). To the contrary, the survey reveals most Americans do not believe that 'data for discounts' is a square deal. Turow et al. (2016) reported that marketers justify their data-collection practices with the notion of tradeoffs, "depicting an informed public that understands the opportunities and costs of giving up its data and makes the positive decision to do so" (p. 3). For example, a Yahoo report (2014) concluded that online Americans "demonstrate a willingness to share information, as more consumers begin to recognize the value and self-benefit of allowing advertisers to use their data in the right way." The end goal of this "tradeoff" illusion, according to Turow et al. (2016), is to claim to policymakers and the media that "Americans accept widespread tracking of their backgrounds, behaviors, and lifestyles across devices, even though surveys repeatedly show they object to these activities" (p. 3). The data collected as a tradeoff is inextricably tied to the surveillance assemblage that occurs digitally.

1 A user is a person "who is trying to get something done and has a clear objective in mind" (Rose, 2024, p. 2).

2 Surveillance assemblages operate by "abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention" (Haggerty & Ericson, 2000, p. 605).

In the assemblage process, groups which were "previously exempt from routine surveillance are now increasingly being monitored" (Haggerty & Ericson, 2000, p. 606). Even before the fall of *Roe*, Maria Novotny and Les Hutchinson (2019) offered critical interrogation of surveillance in technologies, uncovering the tracking of users in women's health apps. These technologies claim to give users more control over the storage and use of their information and data while at the same time giving third parties access to that data. Since *Roe*, we are seeing an increase in hyper-surveillance of people within states that have banned or severely limited abortion. Though written over two decades ago, Kevin Haggerty and Richard Ericson's discussion of privacy's role in the surveillance assemblage remains relevant to current day: "privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation" (2000, p. 616). We believe that computers and writing scholars can engage in coalitional work in their own practice, but also in the classroom to equip students with the tools to dismantle oppressive digital platform practices that impact material bodies.

Case 1: Trading Privacy for Connection

What follows is a case example of not just the need for increased privacy protection, but also a point of intervention for computers and writing scholars seeking to communicate in digital spaces while also remaining private. Oftentimes privacy and security are terms used interchangeably; in this case example, we urge users to consider the platforms they use and reimagine how to communicate about what it means to be *secure* for consumers to protect their [private] personal information.

Gather.Town, an online space marketed for use to "Communicate, collaborate, and feel more connected in a persistent space that reflects your unique team culture", was used by technical and professional communication (TPC) graduate students during the peak of the COVID-19 pandemic in 2020 to gamify their work (Gather, 2023). The graduate students were part of the Council for Programs in Technical and Scientific Communication (CPTSC) Graduate Student Committee. Gamifying workspaces certainly has many benefits; however, there is a greater need for cybersecurity protocols to be addressed when sensitive company information, personal information, and societal implications are at stake in the gamified space. Cybersecurity, though related, is different from data privacy: data privacy "insists on the protection of user data, while cybersecurity requires thorough audit trails" (Mikac, 2022). Cybersecurity is focused on *preventing* security breaches, and in our case examples, is deeply intertwined with data privacy's decision of *when* and *how* data will be shared with a third-party. We want to focus on such

consequences: that of breaching data, as well as consequences of third-party access just from using a platform.

Despite the usage of this platform for increased connectivity and collaboration, the lines between work and play were blurred. Although the Gather company provides extensive privacy and security reporting, as a graduate student user in the space, there were still extensive lateral surveillance, often referred to as peer-to-peer surveillance, concerns. So, how do we navigate spaces that gamify our work and create connectivity, while simultaneously putting our privacy at risk? The answer is not so straightforward—and surprise—depends on the context.

Joanna Wallace (2022) wrote, for example, that gaming is the largest entertainment industry worldwide, and the COVID-19 "pandemic caused an enormous 26% surge in growth in 2019 and 2021 as users attempted to break up the monotony of lockdowns and stay close to friends and family." This yearning for closeness can cause users to "trade" values: that is, trade protection of personal information, for personal connection.[3] A popular claim is that people do not care about privacy (Banville, 2023, p. 60). Everything is already out there! In reality, people *do* care about their privacy. According to a study by MAGNA Media Trials and Ketch, 74% of people now rank data privacy as one of their top values (Ketch, 2022). There are privacy implications of using Gather.Town for both work and social life, which serves as a case example of the ways graduate students value connectivity over potential privacy invasion and lateral surveillance (Andrejevic, 2007). When using the application, users are able to "Stop by someone's desk, say hi in the hallway, and bring back water cooler chats. No scheduling required" (Gather, 2023). For example, when TPC graduate students met online, any student could "walk" into a meeting without notice. While it may be noted that Gather has updated their platforms since the initial usage in 2020, such considerations are applicable to any digital space. Gather (2023) now has a protocol where meeting rooms may be locked, chat history "disappears," doors have passwords, and guests must wait in waiting rooms. Despite Gather touting that they could make the chat history "disappear," their privacy policy suggests otherwise. While users may believe the history is "gone," as Gather (2023) suggested, "When all users leave a private area, the chat history will be erased so the next group won't see your notes," the privacy policy states, "Gather may store chat messages. When stored, they are encrypted at rest" (Gather Privacy Policy, 2023). Though the messages are encrypted, Gather is still subject to distributing such content of the messages to law enforcement, as well as distribution to third-parties that

3 The privacy paradox refers to the "conflict between individuals express[ing] concern over privacy and their apparent willingness to surrender that privacy in online spaces in exchange for very little of value" (Reilly, 2021, p. 33).

connect to Gather such as "Google Integration, Outlook Integration, Slack Integration" and more.

Regardless of these updates, computers and writing scholars must critically question the dissemination of information in this politically charged time. For example, in the wake of *Roe v. Wade* being overturned, digital spaces are particularly vulnerable for sensitive information to be distributed unknowingly from participants. Since Gather was used as a space for graduate students to connect, commiserate, and collaborate across geographical locations, content that would lead to arrest in some states created heightened anxieties about what information is and could be shared with third-parties.[4] Though Gather provides information about "cross border data transfers" between the EU/UK, there are not any mentions of how data is *secured* across borders in the United States (2023).

Aside from the lateral surveillance concerns in the space, that is, peer-to-peer surveillance, there are also data privacy implications. According to a 2023 study conducted by Usercentrics, a leading Consent Management Platform (CMP) provider, 90% of mobile games are not in compliance with privacy regulations. This means millions of gamers around the world have no control over how their personal data is collected, stored, and used. As with many systems and applications, games such as Gather.Town are not exempt from complying with the law. Gather.Town may be used as an example for students to discuss compliance protocols; such data collection implemented by the "game" invades privacy further creating vulnerabilities for, in this case, graduate students who are already in precarious positions such as those who are multiply marginalized, international students, first generation, and more.

With such considerations in mind, Gather.Town could be introduced into the TPC and writing classroom space as a tool to use with students, while also carefully critiquing and considering potential privacy and surveillance implications, digital and not. For example, according to Gather's Data Processing Addendum effective as of November 2023:

> 4.1. Gather will not disclose Personal Data to any individual or to a third party other than: . . . (iv) as required by applicable law or a valid and binding order of a law enforcement agency. Except as otherwise required by law, Gather will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("Demand") that it receives, and which relates to the Personal Data.

4 Location map of U.S. state policies on abortion: https://www.guttmacher.org/state-policy/explore/state-policies-abortion-bans

The information that would be of particular interest to students, instructors, and practitioners (given the target audience of Gather), is highlighted: Gather "except as otherwise required by law" would notify customers of any law "demand" that they receive. That is, if you are within a state that currently bans abortion, and you discuss such information with a coworker, Gather can share this information with law enforcement. Though Gather does not have any responsibility to interact with whomever is making a demand for information, they also do not say that they won't interact with them. There has been a significant move for companies, especially menstruation applications, to take a stance regarding the safety and well-being of their consumers. For example, according to Catherine Roberts (2022), the company Period Tracker suggested that it would not comply with a subpoena designed to convict someone for having an abortion. Though it is unclear when Period Tracker published their blog, they wrote: "We would rather close down the company than be an accomplice to this type of government overreach and privacy violation."

Gather is one of many platforms that companies are using to promote connectivity. Though this is feasible, and certainly did provide a means for connection for TPC graduate students, privacy and security concerns should be addressed and noted. In particular, if instructors wanted to introduce students to critical digital literacies such as privacy, annotating Gather's Privacy Policy would be a crucial first assignment. From there, instructors could overview "hidden" implications, such as what is suggested in the "Usage, Location and Tracking Cookies" section. Gather could have the most airtight Privacy Policy and Data Processing "Addendum" in the world, but that does not mean the third-parties that have access to consumer information do as well.

Case 2: Trading Privacy for Advocacy

In this case example, we encourage users to be wary of the vulnerable information they share on social media, even in pursuit of social justice movements. Computers and writing scholars are uniquely positioned to think and act critically, rhetorically, and ethically regarding technical documentation such as privacy policies and application settings as well as multimodal and digital communication via technologies such as Instagram. These skills and expertise, paired with a social justice orientation, can position computers and writing scholars as scholar-activists disseminating digital literacies and practices to users for ethical engagement on social media platforms. In doing so, they make visible the embodied experiences tethered to a story, which are often re-experienced by storytellers (Novotny & Gagnon, 2019) as the story circulates. For example, users may not be conscious of the risk to privacy and

security when they share their vulnerable lived experiences on social media in hopes of forwarding the reproductive justice movement.[5] Deemed by some as #slacktivism, digital engagement with and creation of content for social change has grown as a staple activist practice. Jennifer Nish (2022) cited digital activism as one of many methods needed to successfully pursue social change, not only as a gateway to other activist practices but also as a method with its own benefits for accessing and participating in social justice movements. The wide circulation afforded by Instagram, which seamlessly links to Twitter, Facebook, etc., is indeed a benefit to spreading awareness, informing an audience, and building coalitions. But the uncontrollable rhetorical velocity (Ridolfo & DeVoss, 2009) of stories of reproductive [in]justice on social media after the fall of *Roe v. Wade*, paired with the ease of remixing content or cross-platform sharing, threaten the privacy of users. In recent cases, these stories have even been used as evidence against individuals engaging in 'illegal' abortions (Davis, 2023). Users must be made aware of these potential dangers when asked to share their vulnerable stories by activist organizations or when deciding to do so themselves.

Storytelling has been a method used by reproductive justice activists long before the rise of social media (Silliman et al, 2004). But sharing stories in digital public spaces requires an ethical awareness and digital [privacy] literacy that most users are not taught. For instance, the phrase "My Body, My Choice," a slogan often chanted in marches for reproductive rights around the globe, has been co-opted by anti-abortion advocates to question a pregnant person's willingness to impose their control over another "body," that of an unborn fetus (Savas, 2023). This same tactic was used by advocates against COVID-19 vaccinations to question a pregnant woman's right, *in this context*, to choose what is done to her body. Once out in the digital public, lived experiences of reproductive injustice are often re-purposed for alternative agendas. For example, a reel that was originally promoting abortion services as reproductive justice can be remixed to stitch in harsh anti-abortionist attacks and can still apply #reproductivejustice as a hashtag.[6]

Policies related to social media are far behind reality. Instagram's privacy policy is provided by its umbrella company, Meta Platforms, Inc., which also owns Facebook and Messenger, Threads, and WhatsApp. In regard to data, Instagram collects information from users and stores it for a variety of reasons:

5 Reproductive Justice has four main tenets: the right over bodily autonomy, the right to have kids, the right to not have kids, and the right to parent kids in safe and healthy environments (SisterSong, 2023). The movement seeks to center the most marginalized individuals and is multifaceted, intersectional, and coalitional.

6 I intentionally chose not to describe a specific account, story, or person here to avoid further unwanted circulation of an embodied experience of reproductive injustice.

for product promotion, external research, public safety, and more. These policies, which can be only slightly altered by users' account settings, allow for sharing of information with third-parties due to various reasons, including legal requests from third-parties such as civil litigants, law enforcement and other government authorities; applicable law or legitimate legal purposes; and the safety, security and integrity of Meta Companies, Meta Products, users, employees, property and the public (Meta Privacy Policy, 2023). This means that a user's posts, stories, reels, and direct messages are not private, even if their account is marked private. Information about a user's location, device, network, created content, and viewed content could be used to implicate them in perceived criminal activity, such as seeking abortion services in states where abortion is illegal or sharing resources about at-home abortions. It also means that if users have not limited Meta's access to their camera roll – which is not unheard of given the functionality of Instagram as a visual-dominant platform – then Meta could pass along location-related information, time stamps, and content provided via the user's camera roll regardless of whether images have been uploaded to Instagram or not. Additionally, Meta's privacy policy states that it shares information across its products, meaning that something shared in a seemingly private space like Facebook Messenger, such as pregnancy test results, is not private nor secure. Reflecting on "public safety," it is worth asking: whose perspective on public good or safety is being held as the standard? What are their values, and who might they view as "dangerous" to public safety regarding reproductive health?

Meta's privacy policy is storified in its presentation with inviting images and "highlights" that provide the basics of each section. This structure nests the most pertinent information behind one or more clicks. Individual users and organizations sharing the stories of others should be aware of the potential for risk, invasion of privacy, and/or investigation based on interactions, posts, or messages. Even users who have privacy features activated are vulnerable if they share an experience of reproductive injustice with a friend, organization, reporter, or someone else who then shares it publicly. While it is important to embrace the ways in which stories are intertwined and not necessarily owned solely by any one person, it is also important to recognize the real harms that could come to a person living in a state in which abortions are banned. Recently, the right to contraception has also been under attack (National Women's Law Center, 2024). If it becomes a "public safety issue" to stop women from using certain or all contraceptives, what is to stop law enforcement from requesting data from Instagram to find those breaking that law? The content that users create and interact with on Instagram is not private and could be used to incriminate users for seeking out alternative reproductive health care or services.

Computers and writing instructors who want students to engage with movements such as reproductive justice should approach their pedagogical praxis with care and caution. Despite the "trend" factor of incorporating social media, stories, and digital activism into the classroom, instructors must be wary of how they ask students to interact with, respond to, and/or analyze user content related to reproductive justice. For instance, Danielle Koepke (forthcoming) theorized practices of care to support student engagement with digital activist stories that prioritizes the embodied experiences of storytellers while developing students' critical digital literacies and ethical awareness of the complications and complexities of digital connectivity. When framed with care, students can learn a lot from these digital and multimodal communication events that will better prepare them for future engagement in their own careers, communities, and digital activism.

Synthesis of Cases: How to Navigate the Privacy-Connectivity Tension

Sites of surveillance, such as our case examples with Gather.Town and Instagram, are emblematic of the surveillance assemblage. David Lyon (2007) mentioned that despite the ubiquity of surveillance technologies, it is important to study specific "sites of surveillance" in order to understand their nuances (p. 25). In our cases, the ways in which our physical body becomes vulnerable is through our identity (through sharing personal information) being distributed through platforms. Our participation in sites such as Gather.Town and Instagram for connectivity renders the body susceptible to systems that seek to further marginalize and harm. We focused on these platforms because they were and are used to communicate potentially compromising information. Thus far we have referenced themes such as trading data privacy for connectivity, as well as the tension between companies taking stances on "safety" and "well-being" of consumers versus the actual decision making of said stances. Let's envision this:

> Marcie is a graduate student in Texas. She is seeking connectivity with fellow students across the nation. Marcie identifies as a cisgender woman, and recently missed her period. The stress of missing a period, as well as the yearning for a support group has led Marcie to seek guidance and support on a social media platform.

In this imagined scenario, Marcie is being surveilled in a variety of ways (both seen and unseen). Perhaps laterally, Marcie's family noticed that she has been distant: she moved to Texas for the graduate program and has not been

communicating as much. Marcie is part of a vulnerable and precarious population, not just because of her status as a graduate student, but also because she is concerned that she may be pregnant. *Who can she share this concern with?* When Marcie moved to Texas, she was recommended to join a group of fellow graduate students via social media. In the group were some people who had children of their own. Marcie, after weeks of interacting with the group and developing a sense of trust and belonging, disclosed with one of the members that she was afraid she was pregnant. This disclosure, however, is not private; it can be passed along to third parties. Abortion is completely banned in Texas because of a state law that went into effect July 1, 2022. Individuals can travel out of state to get an abortion, if they have access. Marcie doesn't have transportation, though. The exceptions that may allow individuals to get an abortion in Texas include: "to save the pregnant person's life and to prevent serious risk to the pregnant person's physical health" (Abortion Finder, 2024).

As a nation, we have seen the effects of people assisting or even knowing about someone having an abortion. Take for example the case in Texas, where an ex-husband made a "Rule 202" request — "a filing that usually precedes a lawsuit when illegal activity is suspected. If approved, the court could allow the man to seek documents related to the alleged procedure and order the woman and others accused of helping her to sit for depositions" (Coronado, 2024). As the article suggests, the Texas abortion ban provides for enforcement either through "a private civil action or under the state's criminal statutes;" meaning that those involved could be punishable by up to life in prison for anyone held responsible for helping a woman obtain an abortion (Coronado, 2024).

Marcie is at risk of facing a legal battle due to the surveillance assemblage she is part of. All messages that she shared in a seemingly private space are subject to training the social media platform's AI, as well as being shared with law enforcement. Because historically excluded populations are expected to do more emotional labor within the white capitalist heteropatriarchal society that we live in (hooks, 1984), these populations seek relief through community, often through virtual connection. They may also feel a responsibility to share or disclose, to help someone else similar to them avoid, in this case, lack of access to care, accidental pregnancy, and so forth. Imagine that the woman Marcie shared her concerns with accidentally left her computer open. Her partner saw the conversation, and reported suspicion that Marcie might try to have an abortion to local authorities. *What should Marcie do?*

We put a lot of responsibility onto individual people when technology companies should be held accountable for the ways they collect and distribute data. While we can, and will, give some broad guidance for what users can do, we believe that it is fruitless without a collective effort. Public pressure does lead to change. Take for example, the period trackers that store data locally

and don't allow third-party tracking—Drip, Euki, and Periodical (Roberts, 2022). Without sharing this information or urging applications and platforms to reimagine what it means to protect users, those seeking to track menstruation in states currently banning abortion might believe that there is only one solution: don't track at all. We can still connect, and we can still support reproductive justice efforts, but not without a critical approach to data privacy. So, in your next meeting, perhaps suggest an application who focuses on protecting the users, rather than opting into the majority vote or "most popular" platform (broadly speaking). Small acts of resistance can lead to larger forms of activism (Banville, forthcoming).

Conclusion: So, what do we do now?

Since *Roe v. Wade* was overturned, the use of stories to advance advocacy for and against reproductive justice has risen. Such politicized events contribute to an added layer of precarity for already-vulnerable populations who are subjugated to hyper-surveillance. The hyper-surveillance, in this example, occurs geographically and digitally, requiring individuals to trade their privacy for connectivity. Computers and writing scholars can play an important role in digital activism for the reproductive justice movement through careful circulation of and honorable engagement with stories. However, each individual must know their own potential risks, such as those imposed by university policies. For instance, many public universities can request content from emails, learning management systems, and research-related work. This calls into question our role as scholar-activists, as we may end up doing more harm than good for those most impacted by injustice. It is essential to carefully negotiate how we can best support digital activist work without co-opting it in the classroom, in our research and writing, or through our ties to the university. Privacy is a human right, but it is not an individual responsibility; it is a collective one. This work calls for coalitional approaches across designers, researchers, instructors, graduate students, and community members.

Let's return to our initial question: how do computers and writing scholars navigate spaces that gamify our work and create connectivity, while simultaneously putting our privacy at risk? We suggest computers and writing scholars use their technical skills and expertise to demystify privacy policies and what happens with data collected through gaming and social media apps while also seeking out more secure methods for connectivity. Though we have not used the services ourselves, it is said that Kumospace is a feasible option to use as a messaging, meeting, and gathering space. According to Kumospace privacy policy (https://www.kumospace.com/privacy), the company is fully Service Organization Control Type 2 (SOC 2), Health Insurance

Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR) compliant. There are drawbacks, including that the free version is limited to five users. Users could also download a virtual private network (VPN) such as Windscribe or a similar tool: this certainly does not solve the platform precarity of games and apps such as Gather.Town. and Instagram, however, it does add a layer of potential protection. Downloading a VPN unfortunately puts the onus on the individual, instead of a collective approach towards privacy. For scholar-activists, some have found higher levels of security and control on Discord (https://discord.com); however, their privacy policies are something to be wary of as well. There just does not seem to be a perfect, secure, system. And perhaps that's what we need from future computers and writing scholars.

As instructors, we can advocate for a critical awareness towards implementation of applications, technologies, and platforms within and outside of the classroom space. Our second question asked: How can, or should, computers and writing scholars support digital activist projects for reproductive justice while also negotiating issues of privacy and data collection? We believe that computers and writing scholars should critically engage with digital advocacy stories and the privacy invasion embodied by storytellers. To attend to this call, advocacy can begin in the classroom space and through our roles as computers and writing scholars in the design process. It is crucial to communicate or translate potential dangers of data privacy collection: to do so, we can raise awareness by being advocates in our individual spaces, as well as through the digital platforms we have access to (ironic, right?). Banville (2023) argued that due to recent shifts in surveillance technologies, scholars and instructors in computers and writing must call attention to and explore technological ethics including "describing how data and information are collected, who has a right to privacy and why, and communication exchanges between employer/employee and the public," such as through applications like Gather.Town and Instagram (p. 310). In our roles—from instructor, to student, to administrator, and more— we can intervene in the tradeoff fallacy through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns as they relate to the platforms we choose to use and incorporate in our everyday.

References

Abortion Finder. (2024, October 3). Abortion in Texas. https://www.abortionfinder.org/abortion-guides-by-state/abortion-in-texas

Andrejevic, Mark. (2007). *iSpy: Surveillance and power in the interactive era.* University Press of Kansas.

Banville, Morgan C. (2023). Am I who I say I am? the illusion of choice: Biometric identification in healthcare (Order No. 30603350). ProQuest Dissertations & Theses Global. (2830119112), https://www.proquest.com/docview/2830119112

Banville, Morgan. (Forthcoming). Surveillance for the public: Digital activism and advocacy through coalitional work. In Clark, E., Partin Patterson, A., Blackmon, C.R., Allen, N., Bikmohammadi, M., Dighton, D., Eble, M., and Banks, W. (Eds.), *Practicing digital activisms: On rhetoric, writing, and technical communication's social justice obligations.* Utah State University Press.

Beck, Estee, & Hutchinson Campos, Les. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom.* Utah State University Press.

Boyle, Casey. (2018). *Rhetoric as a posthuman practice.* Ohio State University.

Ching, Kory L. (2018). Tools matter: Mediated writing activity in alternative digital environments. *Written Communication, 35*(3), 344–375. https://doi.org/10.1177/0741088318773741

Coronado, Acacia. (2024, May 13). Texas man tests out-of-state abortions by asking court to subpoena his ex. *The Associated Press.* https://www.nbcdfw.com/news/local/texas-news/texas-man-tests-abortion-law-subpoena-ex/3539667/

Davis, Wes. (2023, July 11). Meta-provided Facebook chats led a woman to plead guilty to abortion-related charges. *The Verge,* https://www.theverge.com/2023/7/11/23790923/facebook-meta-woman-daughter-guilty-abortion-nebraska-messenger-encryption-privacy

Foster, Diana Greene (2020). *The turnaway study: Ten years, a thousand women, and the consequences of having - or being denied - an abortion*. Scribner.

Frith, Jordan. (2020). Technical standards and a theory of writing as infrastructure. *Written Communication, 37*(3), 401-427. https://doi.org/10.1177/0741088320916553

Fuentes, Liza. (2023, January). Inequity in US abortion rights and access: The end of Roe is deepening existing divides. *Guttmacher.* https://www.guttmacher.org/2023/01/inequity-us-abortion-rights-and-access-end-roe-deepening-existing-divides

Gather. (2023). Gather Presence Inc. https://www.gather.town/

Gather Privacy Policy. (2023, October 13). https://www.gather.town/privacy-policy

Gather's Data Processing Addendum. (2023, November 14). https://www.gather.town/dpa

Haggerty, Kevin, & Ericson, Richard. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622. https://doi.org/10.1080/00071310020015280

hooks, bell. (1984). *Feminist theory: From margin to center*. South End Press.

Jarman, Michelle. (2015). Relations of abortion: Crip approaches to reproductive justice. *Feminist Formations,* 27(1), 46-66.

Johnson, Maureen, Levy, Daisy, Manthey, Katie, & Novotny, Maria. (2015). Embodiment: Embodying feminist rhetorics. *The Journal of the Coalition of Women Scholars in the History of Rhetoric and Composition, 18*(1).

Koepke, Danielle. (Forthcoming). A praxis of care for activist stories of reproductive justice in the digital classroom. In Clark, E., Partin Patterson, A., Blackmon, C.R., Allen, N., Bikmohammadi, M., Dighton, D., Eble, M., and Banks, W. (Eds.), *Practicing digital activisms: On rhetoric, writing, and technical communication's social justice obligations.* Utah State University Press.

Lyon, David. (2007). *Surveillance studies: An overview.* Polity Press.

Meta Privacy Policy. (2023, December 27). https://privacycenter.instagram.com/policy/?section_id=10-HowDoWeRespond

McGinn Valley, Taryn., Zander, Meghan., Jacques, Laura., & Higgins, Jenny A. (2023). 'The biggest problem with access': Provider reports of the effects of Wisconsin 2011 Act 217 medication abortion legislation. *Wisconsin Medical Journal*, 122(1), 15-20. https://wmjonline.org/wp-content/uploads/2023/122/1/15.pdf

Mikac, Erik. (2022, March 29). Cybersecurity vs. Data Privacy: What is the Difference? *CBT Nuggets.* https://www.cbtnuggets.com/blog/certifications/security/cybersecurity-vs-data-privacy-what-is-the-difference

National Women's Law Center. (2024, May 30). The right to contraception act: enshrining the right to birth control in federal law. https://nwlc.org/resource/the-right-to-contraception-act-enshrining-the-right-to-birth-control-in-federal-law/

Nish, Jennifer. (2022). *Activist literacies: Transnational feminisms and social media rhetorics.* University of South Carolina Press.

Novotny, Maria & Gagnon, John. (2018). Research as care: A shared ownership approach to rhetorical research in trauma communities. *Reflections: A Journal of Community-Engaged Writing and Rhetoric*, 18(1), 71-101.

Novotny, Maria & Hutchinson Campos, Les (2019). Tracing the future lineage for OBOS: Reproductive health applications as a text for feminist rhetorical inquiry. Women's Health Literacy and Our Technological Future, *Peitho* 21(3), 645-654. https://wac.colostate.edu/docs/peitho/article/tracing-the-future-lineage-for-obos-reproductive-health-applications-as-a-text-for-feminist-rhetorical-inquiry/

Oberman, Michelle. (2022). What will and won't happen when abortion is banned. *Journal of Law and the Biosciences,* 9(1), lsac011. https://doi.org/10.1093/jlb/lsac011

Period Tracker. (2024). On data privacy. *GP Apps.* https://gpapps.com/2022/05/19/on-data-privacy/

Reilly, Colleen. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition, 61*. https://doi.org/10.1016/j.compcom.2021.102652

Ridolfo, Jim, & DeVoss, Dànielle Nicole. (2009, January 15). Composing for recomposing: Rhetorical velocity and delivery. *Kairos: A Journal of Rhetoric, Technology, and Pedagogy*, 13(2). https://kairos.technorhetoric.net/13.2/topoi/ridolfo_devoss/intro.html

Roberts, Catherine. (2022, August 30). These period tracker apps say they put privacy first. Here's what we found. *Consumer Reports.* https://www.consumerreports.org/health/health-privacy/period-tracker-apps-privacy-a2278134145/

Rose, Emma. (2024). Who Is the User? Researching Audiences for Technical Documents. In Kirk St. Amant & Zemliansky Pavel (Eds.). *Technical Writing Spaces: Readings on Writing, Volume 6.* WritingSpaces.org; Parlor Press; The WAC Clearinghouse. https://wac.colostate.edu/books/writingspaces/writingspaces6/

Savas, Leah. (2023, February 20). Unpacking 'my body, my choice.' Unpacking culture series, *Crossway*, https://www.crossway.org/articles/unpacking-my-body-my-choice/

Silliman, Jael, Gerber Fried, Marlene, Ross, Loretta, & Gutiérrez, Elena (eds). (2004). *Undivided rights: Women of color organize for reproductive justice*. Haymarket Books.

SisterSong. (2023). Visioning new futures for reproductive justice declaration 2023. https://www.sistersong.net/visioningnewfuturesforrj

Turow, Joseph, Hennessy, Michael, & Draper, Nora. (2016). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2820060

Usercentrics. (2023, April 18). Consent in mobile games: Hidden benefits and low-hanging fruit! *Usercentrics GmbH.* https://usercentrics.com/resources/mobile-games-report/

Wallace, Joanna. (2022, December 13). Gaming industry: The need for cybersecurity (protocols). *Coralogix.* https://coralogix.com/blog/gaming-need-cyber-security/

Yahoo! (2014). Advertising, the balancing act: Getting personalization right. https://advertising.yahoo.com/Insights/BALANCING-ACT.html

Zuboff, Shoshana. (2019). *Age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.