A GUIDE TO ONLINE SAFETY FOR ACADEMICS: DOXX MITIGATION, SOCIAL MEDIA, LAW, POLICY, AND TECHNOLOGY

Aaron Roussell and Max Parmer
Portland State University

In our terminally-online age, everyday academics from undergrads to full professors experience doxxing and other forms of ritual media humiliation. These incidents relate to their writing, their public commentary, private correspondence revealed, digital stalking, political hitjobs, or the efforts of an unfriendly or ideologically motivated colleague, administrator, or journalist. Historically speaking, there is a nothing new or unusual about public outrage regarding radical academics, but the ubiquity of social media technology alters the practices, reach, and speed of reactionaries considerably. The gravity of such fallout can range from simply annoying (e.g., a heavy proportion of online mentions refers to the incident) to career changing (e.g., notorious incident must be addressed in every public presentation, regardless of subject or forum) to career ending (e.g., enough pressure can prompt actions tantamount to termination). Moreover, it can be scary and potentially place the target in physical danger. The energies of the target become absorbed by mitigating the incident and its fallout instead of academic or organizing work; political comrades' activities similarly become reoriented to defense.

Academics whose main form of political activity is public engagement seem the most likely to experience these concerns. Yet exchanges in intimate classroom settings where instructors operate with the assumption that their discussions will not make national news are also vulnerable. Even those experienced in the public arena can be surprised at the strength, coordination, and effectiveness of oppositional, right wing political actors. As Kamola discusses in Chapter X of this volume, the well-funded rightwing outrage machine implants detection mechanisms at the undergraduate level, grows specialist media organizations devoted to amplifying these manufactured scandals, organizes policy and legal organizations devoted to prosecuting these scandals, and funds think tanks and embedded academics who give such charges intellectual veneer. Academic organizers may have less to fear from this vast outrage-o-sphere than those whose bread and butter is public battle over culture wars, but by the same token, the consequences of successful right-wing operations have the potential to be even more devastating to organizing efforts. And, of course, off-the-cuff/pithy classroom comments or even a single slide can be recorded/photographed, de-contextualized, and flashed all over Fox News whether or not one is engaged in subversive activity.[1]

Doxxing is the archetypical attack we use to structure this guide. Doxxing is the practice of researching, compiling, and publicly broadcasting personally identifying information of a target including legal name, "dead" names, phone numbers, home address, social media accounts, bank accounts, social security numbers, family members, and whatever other personal details can be collected. This information is linked to worst possible interpretation of the original concerns in front of a loyal audience comprising anywhere from thousands to millions of followers. For example, if a target published a commentary piece in support of police abolition

[1] Our colleague was blindsided in such a manner during remote teaching over the pandemic. In teaching about debates regarding diversity in high education, they reproduced the title of a news article [TIME?] "Is Math Racist?" in a PowerPoint. A student captured the image and forwarded it to an organization looking to weaponize and monetize examples of so-called "wokeness" and the professor confronted surprise online harassment the following day.

or Black Lives Matter, the doxxer provides personal information to their followers which results in harassment, home visits, and other forms of intimidation in order to chill public speech, additional activism, and public movement. In the best-case scenario, the target is forced to focus on their well-being at the expense of public activity. Moreover, by coming to the attention of the doxxers, out-of-context information (e.g., social media screenshots, disproven allegations, unflattering interpretations of private concerns) or even outright lies can be weaponized to discredit the target (best case scenario) or threaten the livelihood or the life of the target.[2] Doxxing of academics can have ripple effects as well, curtailing research into sensitive topics and devitalizing subfields.

Like any effective social pressure tool (e.g., boycotts), doxxing itself is neither good nor bad. Doxxing has been a longstanding go-to tool for antifascists, Klanwatches, and other community defense groups. “Removing the hoods,” so to speak, raises the stakes for far right organizing to the point that those with fascist views are deterred from publicly airing them, connecting with others who hold them, and fomenting strategy to bring them about. The key difference, we argue—besides the obvious problem of genocidal viewpoints morphing into organized genocidal political movements—is that rightwing organizations rely on cults of personality and celebrity which can be uniquely vulnerable to such tools. Less hierarchical organizing uninterested in monetizing outrage can practice better security culture without sacrificing effectiveness.

Some practices can make doxxing harder to begin with and mitigate a doxx once it happens. In considering the full arc, beginning with a Twitter post to the Fox News story shared widely over Facebook (much like the spread of a virus), the goal is to flatten the curve. “Success” can mean simply that an initial broadcast is not amplified, or is of limited duration and spread. While malicious, rightwing actors often have short attention spans and isolated pieces of information are more difficult to monetize and weaponize than broad, deep, and integrated personal information. State actors have broad informational reach, discretion, and penetration, but (usually) have a much higher bar for intervention.

The advice sketched below is intended for individual academics, but much can also apply to groups oriented towards social/academic change. Security level, of course, ought to relate to the importance and secrecy of the information being protected. Nearly anything can be accessed with sufficient time, motivation, and resources; the key questions are 1) how to avoid having state and rightwing actors focus those resources where they would be most devastating, and 2) how to maintain personal and organizational effectiveness within a reasonable and practical security regime. Therefore, we discuss below a mix of general best preparatory practices for anyone in the Information Age, a guide for how to mitigate the effects of doxxing and other rightwing attacks, and an exhortation to community defense. Your mileage, as they say, may vary.

Relationships and community

In thinking about the differences in activism and organizing, one of the main pillars of good practice is to develop and maintain communities of care. Watching out for one another and participating in mutual aid and care labor that binds us closer together reaps a variety of benefits from individual-level mental health concerns to pre-figuring the world in which we actually want to live. For our purposes here, there is safety and security among those who eschew hierarchical, dictatorial, and exploitative arrangements in favor of mutual aid even if we occupy different

[2] Discuss ODU prof?

positions in this racial capitalist patriarchy (see Morris, 2019).[3] Get to know university administrative assistants, academic advisors, and schedulers. Not only do make the whole place run and are the first line of defense when things blow up, but they are often a friendly bunch of highly competent people who are crucial figures in the academic enterprise—that is, potential comrades.[4] Ongoing exchanges and relationships of care and trustworthiness in times of calm make navigating crises easier.

In the case of doxxing, avoid isolation. Even though crawling in a personal hole may be tempting and explaining the vagaries of a coordinated smear to family, friends, and trusted coworkers can be mortifying, this is of crucial importance. Hopefully, much care labor has already been mutually exchanged and high levels of trust built; such practices are both beneficial in and of themselves and prophylactic in times of crisis. Remember, these are the folks who will help keep you safe. Put time and care into your interactions.

Convene meetings or phone calls with close friends and confidantes, especially those who may be in the crossfire. Remain calm and confident; the goal is not to freak them out, but rather to prepare them and protect them as well. Avoid wild speculation in favor of the concrete steps that you all will collectively take to secure pieces of internal information against external threat. If appropriate for real life interventions, craft a safety plan covering contingencies at work, home, or other frequented places. We will discuss this below in more detail, but don't be afraid to ask for their support—daily check-ins, stop-bys, staying at their houses for a time, monitoring email, etc.

Infotech and Social Media

While one can theoretically perform traditional academic duties without engaging with social media (or even going online—one older colleague still physically mails in journal manuscripts), the reality is that this is both impractical and unlikely. Networks are how community is built and how new research and commentary gains traction. Some academics' continued employment is linked to public reach and engagement. Below are some things to think through in determining what your media footprint actually is and what you would like it to be.

What's out there and how do I control it?

You may be surprised. Search engines, particularly ones with registered accounts, over time begin to tailor search results that bias users' understanding of the true spread of information. Search for your names and social media handles, with and without quotation marks, and see what comes up. To be thorough, use all the major engines such as Google, Bing, and DuckDuckGo. To defeat the bias/registration problem, use private browsing or "Incognito mode," depending on your browser.

A great deal of "private" information is actually publicly available, albeit scattered about. These data sources are scraped and organized by various private companies that function as major public information compilers—for a fee they will tell an investigator, for example, a person's address, arrest record, previous names, and places that they've lived. The specific

[3] Precisely *because* we labor under a racial capitalist patriarchy, straight white cis men in particular must be vigilant and accountable in their relations. Too often this class of person is able to take without giving or fails to value or even recognize the invisibilized labor of women and femme-presenting people.

[4] When one of us underwent a doxx, the departmental advisor and office manager handled menacing phone calls by pretending to agree to transfer the caller to the target. They then left the harasser on hold until they disconnected themselves.

companies change unpredictably but the most popular and comprehensive currently include Spokeo, Whitepages, Truepeoplesearch, and Intellius. You are likely to find at least some details about yourself (and likely your family) available for free and additional private details available for a fee. These companies are legally required to allow self-removal, and they will grudgingly comply, but they are not required to make it easy. These companies *re*download updated datasets wholesale periodically and thus re-add you organically at intervals, requiring a new takedown request.

Controlling this information is a bit like holding a live fish—it's not easy to grab, slippery to hold, and will definitely fight capture. Some people prefer to search themselves periodically and request these takedowns manually; others prefer a paid service such as Delete.Me which combs these sites and makes these requests automatically. Since information and infotech companies are continually popping up, setting up Google alerts with name(s) and social media handles helps (although is hardly a panacea). For more serious information control, sign up for fraud alerts with bank and credit card companies.

Social media: What you control directly

Everything on a social media platform is owned by that media company. Most cooperate with law enforcement to a greater or lesser extent and those lines blur and change often. That said, most social media companies promise a high level of control over personal data—that is, you get to select what is public facing data, what is availability to selected individuals, and what is known only to the company itself. Familiarize yourself with the privacy settings on the social media you use, set them at levels that match your tolerance for public exposure, and check them often for platform changes. The old activist saying "Never put in writing anything you don't want read back to you in court," is adaptable here: Anything you post can be screenshotted and photographed, stripped of context, recontextualized in any way imaginable, and interpreted in the most menacing light by whoever is reading over the shoulder of the person you have the least intimate connection to within your privacy settings.

Consider how closely personal accounts ought to be linked with professional accounts and where organizing/activism falls in that web. Professional accounts must use your professional names associated with your professional activity (writing, presentations, scholarship, opinion pieces, syllabi, etc.). If you're at the beginning of a doxxing crisis or if you do not wish to separate these pieces of yourself but wish to minimize your footprint, remove your name and face from profiles and social media handles to isolate your professional account from your personal life. Untag yourself from photos and ask family and friends to do this on accounts they control; remove anything not institutional from your posted CV. Depending on the prevalence of your name, this can create confusion and muddy the waters for those with ill intent. Sharing some information with the world is inevitable as a public facing professional, but limiting that to the workplace institution responsible for your safety can be helpful.

If you wish to place as much distance between your personal, professional, and/or activist/organizer worlds as possible, the most straightforward way is to create a pseudonym. A good pseudonym is not immediately identifiable (no personal pics) and does not closely resemble your name or social location. Ideally, it refers back to its own email address and can have its own phone number. While there may be overlap in who is in your personal, professional, and organizing circles, these identities should not reference one another.[5] Such a pseudonym can

[5] Through self-googling, a colleague recently realized that their Twitter handle was included on a professionally-related webpage with their real name, even though the Twitter account itself was completely anonymous.

have a robust presence, cross-referencing across multiple social media platforms and providing additional levels of complexity for those wishing to destroy reputations and threaten safety.

Institutional channels: Limiting the scope of public records requests and subpoenas[6]

Although superficially similar, public records requests (PRRs) and subpoenas are generated by different authoritative bodies and processed differently. PRRs cost the requestor money, while subpoenas are a legal tool. Both, however, render unto third parties (and thus potentially the public) information that was not previously available, much of which can be private, potentially damaging, and only tangentially related to the issue at hand, creating the possibility of a cascading number of scandals. This nightmarish outcome however is not a guarantee—the shrewdness of both the requestor and the requestee can limit significantly the amount of material revealed.

Emails and employment-related documents sent, received, and referenced by those employed at public universities are in the public domain unless otherwise protected. Official university channels are open to the curious, provided they spend the money it takes to inconvenience the university employees tasked with compliance. Public records requests are increasingly used by savvy propagandists and journalists. Professional antagonists with high profile publishing outlets backed by rightwing dark money can rake a lot of muck and any email sent within that ecosystem is eligible for forfeit.

If that sets hearts a-racing, examining the process can help to quiet the mind. In the PRR process at Portland State (processes differ, but not by much), a requester submits their inquiry to a public records officer, who usually works within the university's information technology sector. The request must be relatively specific—i.e., one cannot simply request to peruse the entirety of a target's email account—and must abide by federal privacy guidelines regarding protected educational data. (FERPA still matters.) A list of names or specific set of words/ideas/phrases is typical. The university employee runs the query against the document set (typically email or documents within the University-provided cloud space or Google Doc set) to estimate labor costs. Together with a monetary quote, an outline of the potential amount of data is passed back to the requester who can accept the quote, revise it, or reject it altogether.

If the requester accepts, the document set is reviewed by the university general counsel's office. Throughout, the job of university counsel is to rule out irrelevant material and guard against third party privacy violations such as FERPA. Counsel's job is *unequivocally* to protect the university, not you. Although these interests may overlap, that determination belongs to counsel—not you. Our goal here is to limit the judgment calls that counsel must make. Below we discuss a few ways to drastically limit the material available.

First, separate official from personal communications as much as possible. We have been astonished to find that a worryingly high number of academics conduct *all* of their business—professional, medical, personal, legal, otherwise—through their university-provided ".edu" accounts. Get a non-edu email! Do it now![7] Access to university email is entirely at the pleasure of the university. Should a university employee abruptly be accused, however erroneously, of an infraction, access to their official account can be limited or denied *at will* with *no immediate*

[6] Although this section wades into the legal arena, none of the thoughts expressed here should be interpreted as "legal advice"—that is, we are not lawyers and it is not specifically tailored to a retained client, but rather oriented to the general provision of knowledge and proliferation of good data and communication hygiene.
[7] We wish simply to express spillover incredulity here.

recourse, irrespective of whether this is even advantageous for the university.[8] Moreover, during the authorization of a faculty strike in 2014, administration made noises at our university that they might shut off email access. This could have crippled strike mobilization in the short term, even if such actions ultimately run contrary to law or labor practice.

Nearly any alternative email is better, but for security purposes (at the time of this writing), Gmail is okay and will resist most data requests. Yahoo, Hotmail, and AOL are not as good (and your more tech-savvy friends may laugh at you). Services with excellent privacy records include Protonmail.com and Riseup.net. This goes double for those participating in faculty unions: do not discuss union business on university accounts! If someone emails you about such business from a university account, forward to your alternative account and politely inform them as to why—this will help them and their security culture as well.

Still, let's acknowledge the inevitability that sensitive topics will be mentioned within the university's email ecosystem. The temptation to begin referring to such problems (people, situations, etc.) by pseudonyms, initials, or other circumlocutions may be strong. Resist it! In terms of limiting the potential scope of a PRR, be clear and precise in your communications. Refer to the topic directly with the awareness that these may be read externally. Name names, not "that problem person." Circumlocutions muddy the water and can expand information's qualifying potential for PRR. If a requester can infer that a communication between two parties occurred within a particular time frame, for instance, the query may become "TO or FROM party X and Y on ZZZ dates" rather than "TO or FROM party X and Y referring to [explicit search terms]". The former is likely a much broader swathe of communication than the latter. And if one has been precise in their language, the former is less likely. Deleting emails does not remove them from a university's primary server.

Subpoenas are another matter. A subpoena's scope is typically wider, particularly for criminal subpoenas. Again we have the public vs. private distinction: Subpoenas for university accounts will typically come through university counsel directly to the target. If private email account is subpoenaed, in a civil matter it will come to the target directly, while in a criminal matter it will come to your service provider (e.g., Google) which is why selecting providers with a good data privacy record can be important.

Tech things to know

Obviously, the sky is the limit for this section. One can never know everything about information security, since it is its own field and constantly evolving. Still, there are a few guidelines that can go a long way.

Technology usually is not equal, equivalent, or interchangeable. For example, although all popular web browsers have some form of "private" browsing, these functions differ considerably in actual performance. Internet Explorer's private browsing still records visitation history, while Firefox and Chrome "private" browsing is much stronger. Surveillance capitalism is ubiquitous, but some firms are more careful than others. Infotech security analysts have learned that Google specifically will resist data requests except legal warrants and National Security Letters (Drummond, 2013; Whittaker, 2013), although their ad selling and data harvesting algorithms remain mysterious (Silverman & Talbot, 2022). Although no panacea, the

[8] We have personally observed the curious dynamic of a professor losing access to their university email unexpectedly. Having lost that communication pathway and barred them from campus, the university had to ask the *faculty union* to convey messages—such as "what is your alternative email address"—to a stunned and confused professor.

end-to-end encrypted Signal messaging app is more secure than say iMessage or WhatsApp (Electronic Frontier Foundation, 2014, n.d.). And Zoom, we've learned, will readily capitulate to pressure from the Chinese government or anti-Palestine liberation activists (Speri & Biddle, 2020; Wang, 2020).

Malware for hire is a thing (NSO Group, Dark Basin), US is not known to use these firms currently but this can always change.

Oh no, I've been doxxed!

As with several of our examples, sometimes there is simply no preparing. You wake up one morning to a flood of harassment over email, your phone, or your social media accounts. Or an urgent communication from a friend informing you that you were featured in a story on Campus Reform or Fox News, prepare for the worst. Or—and this happens more than one might think—an email from an anonymous account informing you that you are the topic of discussion on 8chan, TruthSocial, Parlor, or other rightwing communications forums.

Your biggest strength in these situations is your community. If you have a union, your first step out to be to alert those in the union charged with your protection, namely your shop steward or grievance officer. Hopefully people in these positions will be able to help triage your general defense as well as any academic administrative attacks that result from the situation. Share the situation with trusted coworkers and work-friends. Assemble a team and/or ask a competent friend to do this with you. As a note to union organizers, propose such a notion when someone comes to you with such a concern. Your anti-doxx support team should help attend to physical and emotional needs as well as academic. Members who are out of the line of fire can help assess the threat, implement countermeasures, and also organize meal trains and a friendly ear.

You will also have to engage with your larger institution. There is very likely a person on staff who is paid to counteract cyberattacks and online threats of various sorts. This person can normally be reached at "abuse@youruniversity.edu". Alert this person immediately. They will likely offer you a menu of options depending on your situation. For example, if the impact is primarily a flood of threatening email, the abuse officer can offer to help filter your email. (You can also choose an individual you know and trust to do this—just make sure to change your passwords.) Determine who is in charge of your departmental website and have your contact information temporarily removed until you feel the threat has passed.

You will also need to talk to the people who answer the department's phones and communications, since they may be directly impacted—these folks will be answering abusive phone calls, doing website removal, etc. If the situation is severe, you may need to talk to your supervisor who may have to field such communications as well and combat lies and harassment on your behalf. If you can stomach it (and if not, ask for help!) track down the source of the concern. This will help backstop your explanations. You can use resources like the Southern Poverty Law Center, Anti-Defamation League, Hatewatch, or FacultyFirstResponders[9] articles to explain the degree of the concern and what bad actors are behind it (Tiede et al., 2021). If the threat is more local and specific, area antifascists may have information on the forces at work.[10] For more, see Kamola's chapter in this volume for how to contextualize such attacks for these

[9] facultyfirstresponders.com/how-to-respond-to-campus-reform

[10] For instance, in Portland, Rose City Antifa maintains an online series of articles and data on local hate groups and individuals of various fascist flavors, some of which intersect with on-campus concerns. (Rose City Antifa, 2019).

audiences—rather than concern for "what *you* did", explain and remind your comrades that there is a vast network of money and media dedicated to engineering such harassment.

When a doxx occurs, mitigation is the goal. Change your email and social media passwords. If the concern is serious, consider asking for a different university phone number and/or contact your phone company and change your number.[11] Changing your listed address from your residence to a PO Box is another way to keep unhinged people from visiting you. In addition to data sources you control (e.g., your CV or personal webpage), you can ask to be removed from the public section of the elections public records office.[12] In a different sense, mitigation means flattening the curve: use sound judgment of course, but engage as little as possible in the doxx. The right wing harassment machine thrives on spectacle and refusing to play into that narrative can keep the instant concern from dragging out.

While on-campus political violence remains fortunately rare in the US as of this writing, it does exist and should be taken seriously, as should the possibility of academic-related threats following you home (Kafka, 2021). Care for personal safety is not the same as paranoia. Threats against academics mostly occur in online or remote settings—veiled or graphic images or statements on social media platforms and/or emails and phone calls containing similar content. Rightwing home visitations are rare, but the authors can personally confirm that this has happened in Portland to doxxed activists. Talk over your concerns with your team and/or find a local organization that does community defense. We are not capable here of comprehensively addressing in-person physical threats, but there are many commonsense security measures one can employ including front-door peepholes, motion sensor lights, window and door alarms, door jammer lock, etc. You can always attend to door knocks by asking who it is through the door. (This of course applies to anyone—neighbors, unfriendly rightwingers, or law enforcement officers who can slide their search warrant under the door.) Even though such scenarios are rare, checking in regularly with your team can help assuage fears and enhance responses to avoid such scenarios—staying with a friend, or having friends over both feels good and makes you a harder target.

Sometimes dangerous situations happen, either at home or at work. Alerting an emergency contact is a priority if the time and space is available. Indeed, if possible, the best response is usually to leave the location. If this is impossible, prioritizing deescalation can help distract the opponent from carrying out violent intent. Deescalatory conversations are content free; they are meant to calm, confuse, or distract those who may intend harm. Ideally remain six feet or more away without making sudden motions, prepare always to run or dodge, and with your hands always visible. Successful deescalations can take a very long time and may require significant recovery time afterward.

If you feel safe calling police, this could help you, depending. However, a strong note of caution here: Police are very often situation escalators. Depending on your social statuses, history with police, and ascribed characteristics, they may not even see you as the victim.[13] Moreover, many officers may not see angry armed rightwingers as threatening, as police maintain a robust relationship with white supremacy (Johnson, 2019). This should not be

[11] This is a go-to practice for many scenarios, such as stalking. Your mileage may vary on this however. If you find it useful and manageable, keeping your number may allow you to measure and track the volume and spread of the harassment. Calls and harassing messages receding over time, actionable threats, and keeping track of area codes can all be leveraged to your advantage depending on your capacity, interest, and emotional threshold.

[12] In Oregon, that is located here: sos.oregon.gov/voting/documents/SEL550.pdf

[13] Police are notoriously poor at incorporating online communications into their notion of "threat" as well. If the threats that precede a dangerous situation occurred online, the explanation required may obviate their presence.

interpreted as advice one way or the other in the moment but rather an exhortation toward having a sober consideration of the dis/advantages of involving police in advance of potential situations.

Community Defense

Hopefully this chapter has induced the reader to take seriously the concerns we introduced in advance of potential situations that may develop through academic (or otherwise) organizing and activism. To paraphrase the hoary old saying, the ounce of prevention it takes to think through these concerns can prevent the pound of unexpected doxxing from happening in the first place, allow you to know when it is coming, and mitigate its effects should it arrive.

A few pithy take-homes: Make sure to check yourself out online; know what the world will see when they look for you. Envision worst case scenarios when planning, even knowing that these are unlikely. Imagine your written or recorded statements will read back to you in court by a hostile attorney or university official. Prepare by building community defenses—talk to your colleagues, coworkers, confidantes, and support groups. Use your union and community resources. Employ secure(r) technology choices and social media; be consistent in your pseudonymous activity. Most importantly, be proactive—if someone you know is going through this kind of situation, assist in their defense!

References

Drummond, D. (2013, January 27). *Google's approach to government requests for user data*. Google: The Keyword: Safety & Security. blog.google/technology/safety-security/googles-approach-to-government-requests/

Electronic Frontier Foundation. (2014, November 4). Which messaging technologies are truly safe and secure? *Electronic Frontier Foundation*. eff.org/press/releases/which-messaging-technologies-are-truly-safe-and-secure

Electronic Frontier Foundation. (n.d.). Secure messaging scorecard. *Electronic Frontier Foundation*. \eff.org/pages/secure-messaging-scorecard

Johnson, V. B. (2019). KKK in the PD: White supremacist police and what to do about it. *Lewis & Clark Law Review*, *23*(1), 205–261.

Kafka, A. C. (2021, July 26). Could political rhetoric turn to campus violence? *The Chronicle of Higher Education*. chronicle.com/article/could-political-rhetoric-turn-to-campus-violence

Morris, C. D. (2019, February 10). Why misogynists make great informants. *Make/Shift Magazine; Feminist Anarchist Border Opposition*. ia902605.us.archive.org/17/items/WhyMisogynistsMakeGreatInformants/misogynists_great_informants.pdf

Rose City Antifa. (2019, June 2). *Mike Mahoney: PSU College Republicans host a fascist propagandist*. rosecityantifa.org/articles/mike-mahoney

Silverman, C., & Talbot, R. (2022, December 21). Porn, piracy, fraud: What lurks inside Google's black box ad empire. *ProPublica*. propublica.org/article/google-display-ads-piracy-porn-fraud

Speri, A., & Biddle, S. (2020, November 14). Zoom censorship of Palestine seminars sparks fight over academic freedom. *The Intercept*. theintercept.com/2020/11/14/zoom-censorship-leila-khaled-palestine/

Tiede, H.-J., McCarthy, S., Kamola, I., & Spurgas, A. K. (2021). Data snapshot: Whom does Campus Reform target and what are the effects? *Academe, Spring 2021*. aaup.org/article/data-snapshot-whom-does-campus-reform-target-and-what-are-effects

Wang, Y. (2020, December 22). How Zoom violated its own terms of service for access to China's market. *Human Rights Watch*. hrw.org/news/2020/12/22/how-zoom-violated-its-own-terms-service-access-chinas-market

Whittaker, Z. (2013, January 28). What Google does when a government requests your data. *ZDNET*. zdnet.com/article/what-google-does-when-a-government-requests-your-data/