Risky Research:

An AoIR Guide to Researcher Protection and Safety

AoIR Risky Research Working Group

Contributors: *Alice Marwick, Dafna Kaufman, Jacob Smith, Patricia Aufderheide, Jessica Beyer, Emma L. Briant, Coppélie Cocq, Laura Dilley, Sam DiBella, Radhika Gajjala, Kamile Grusauskaite, Alex D. Ketchum, Zelly Martin, Janice Metzger, Erin McInerney, Rachel Moran, John McNutt, Suay Melisa Oezkula, Victoria O'Meara, Riccardo Nanni, Carolina Parreiras, Katy Pearce, Ryan Payne, Meredith Pruden, Christian Sandvig, Caighlan Smith, Sam Srauy, Zeerak Talat, Leonie Tanczer, Robert Tynes, Antonia Vaughan, Shenja van der Graaf, Courtney Vowles, Michele White.*

Table of Contents

1. Introduction and Background

2. Collective Risk Mitigation and Responses to Harms

3. Document Scope and Goals

4. Am I at Risk?

5. Designing Research Projects with Risk Mitigation in Mind

6. Mitigating Individual Cybersecurity and Privacy Risks

7. Handling the Potential Outcomes of Risky Research

8. Working with Institutions

9. Conclusion

10. Resources

11. Related Reading

References

Acknowledgments

1. Introduction and Background

At the AoIR conference in November 2022, several scholars gathered to confront a pressing challenge: the growing risks of conducting research in an increasingly complex digital landscape—an issue discussed repeatedly at prior AoIR events.

We define risky research as scholarship that exposes researchers to harm from external actors. This often includes work on politically or socially controversial topics, such as disinformation, extremism, LGBTQ+ issues, critical race theory, reproductive justice and feminisms, and climate change. The risks are heightened for scholars with racialized or marginalized identities, those facing economic precarity, or both.

The harms of risky research are well-documented: networked harassment, emotional and mental health impacts, privacy violations, job loss, and reputational damage (Doerfler et al., 2021; Massanari, 2018; Sobieraj, 2020). These dangers are further amplified by a global, algorithmically-shaped media ecosystem, where threats can originate beyond a researcher's immediate location or cultural context.

In 2016, Data & Society published the first guide to help researchers mitigate these risks. While still relevant, it was designed for an earlier political and sociotechnical climate and is now outdated. More recently, the Research Support Consortium published an impressive guide for researchers handling harassment, but its scope is limited to that specific threat. Thus, the Risky Research Working Group was formed.

As the premiere association for internet research, AoIR has a strong history of critical scholarship and is well-placed to address these challenges. The **AoIR Ethics guidelines** have been adopted worldwide, helping researchers design ethical studies and navigate Institutional Review Boards (IRBs) and human research ethics committees.

This document is similarly designed, offering:

- A framework for understanding the risks researchers face,
- Guidelines for mitigating threats at individual, institutional, and collective levels,
- Strategies for responding to attacks in real time, and
- A curated set of resources and best practices for researchers at all stages of their careers.

The Working Group argues that research institutions must shift from an individualized paradigm, where researchers bear sole responsibility for managing their own risks (and are often blamed when those efforts inevitably fail), to a collective paradigm that prioritizes community resilience of our community and demands institutional accountability (Mattheis & Kingdon, 2021; Vaughan, 2021). This shift not only strengthens the broader ecosystem of knowledge (Sun et al., 2022), but also provides more robust protections for those working within it (Payne et al., 2023).

Ultimately, safeguarding researchers is not just about mitigating harm, but about ensuring that vital, high-risk scholarship can continue in environments that are increasingly hostile toward critical research.

2. Collective Risk Mitigation and Responses to Harms

A Peer Support and Care Networks

B Holding Institutions Accountable

2. Collective Risk Mitigation and Responses to Harms

Much of this document focuses on how individual researchers can mitigate or respond to harassment, violence, and other consequences of risky research. However, it is critical to emphasize: ***researchers are not at fault for these harms.*** A scholar can follow every recommendation in this guide and still experience significant threats.

While most risk mitigation resources focus on what individuals can do, no researcher can fully prevent or account for structural harms alone. Institutions, in particular, must recognize the often-invisible labor that scholars—especially those with minoritized identities, precarious socio-economic situations, or doing radical/critical work (such as feminist, decolonial and anti-colonial, and queer studies researchers)— are *already performing* to prevent harassment in digital spaces. Such researchers must engage in "safety work" (Vera-Gray, 2017) to avoid harm, which directly impacts their ability to navigate academic systems and advance their careers.

Instead of frameworks emphasizing "individual resilience," institutions must examine their role in researcher safety. Risk mitigation should not be an individual responsibility, but must be thought of as collective work. Similarly, activists and scholars have suggested that social media platforms should offer resources and support to survivors of cyberviolence, particularly those connected to acts of gender-based violence. Such calls demand accessible resources, enhanced filtering of keywords/content, and expert partnerships (Citron, 2023; Suzor et al., 2019). This paradigm acknowledges that platforms play a role in risk, and thus should also play a role in prevention and care for participants.

Throughout this document, we explore how institutions and administrators can create lasting protections for scholars engaged in high-risk research, such as rapid-response teams and trauma-informed protocols. Researchers themselves must recognize the unequal distribution of risks across different groups and communities. Strengthening collective approaches to mitigation, safety, and care requires ongoing commitment to evidence-based strategies, institutional accountability, and structural change.

Peer Support and Care Networks

Researchers studying online spaces often feel isolated within their geographic regions or academic institutions. This sense of disconnection is especially pronounced during geopolitical crises or global health emergencies, when collaboration feels more difficult. However, by expanding our notion of community beyond our departments to include the broader network of internet researchers, we can develop stronger, more unified strategies for mitigating harm. A key step in collective risk mitigation is establishing *peer support*

and *care groups* at local, national, and global levels. These structures help researchers prepare for potential risks, process their experiences, and avoid isolation, which should not fall solely on those most vulnerable to harm. Institutions should create dedicated spaces for peer support, such as online or in-person meetings where researchers can share experiences, discuss anxieties, and exchange coping strategies. Support networks must also account for differences in how harassment affects individuals based on identity and positionality. A one-size-fits-all approach does not work; gender- and race-blind policies fail to protect everyone equally.

Holding Institutions Accountable

While academia's precarity and competitiveness can feel isolating, solidarity is essential. As researchers, we must work together—not only in knowledge production but in fostering safer and more equitable conditions for all. This includes demanding institutional support for colleagues facing harassment, even when we are not directly affected. Research institutions must be held accountable for protecting intellectual freedom and ensuring the safety of their scholars. Institutions should provide ongoing support for researchers facing harassment, including follow-up conversations, trauma-informed resources, and clear demonstrations of solidarity. While no universal policy can eliminate these risks, stronger institutional commitment can reduce the burden on individual researchers and foster a more resilient academic community.

Building on the work of transformative justice movements—such as community-based interventions against gender-based violence, prison abolitionist networks, and mutual aid initiatives—we emphasize collective care and accountability (Rentschler, 2017). Traditional institutional mechanisms often fail to protect vulnerable researchers, instead reinforcing hierarchies that leave them without meaningful recourse. In contrast, peer-led, trauma-informed approaches center the needs of those affected and distribute responsibility across the academic community. By learning from grassroots movements that prioritize harm reduction, community resilience, and survivor-centered support, we can create more effective and sustainable strategies for protecting researchers engaged in high-risk work.

3. Document Scope and Goals

3. Document Scope and Goals

This document is focused on risk to people undertaking research. While we heartily endorse the work of human research ethics committees, institutional review boards, and AOIR in articulating potential risks to people whose information is used to inform research, that is not the purpose of this guide.

Instead, this document has four key objectives:

1. Help researchers assess whether their work may put them at risk, and outline the threats they may encounter
2. Provide concrete steps for researchers to mitigate risks, respond to threats, and access resources for institutional advocacy.
3. Offer recommendations for universities, think tanks, and nonprofits to better protect employees engaged in risky research.
4. Explore collective approaches to risk mitigation that extend beyond individual responsibility and leverage the strength of our broader research community.

Building on the **AoIR Ethics Guidelines**, we emphasize the need for care not only for research subjects but also for researchers themselves. By promoting institutional accountability and collective strategies, this guide seeks to foster a safer and more supportive environment for scholars working in high-risk areas.

To speak to an international audience, we note risks that are specific to certain countries or regions, and welcome contributions from scholars across the globe. While *all* researchers face some level of risk, those with minoritized or marginalized identities, precarious employment, or those working under fascist or authoritarian political conditions often experience heightened vulnerability. Scholars in non-tenured or contingent positions—including undergraduate and graduate students, postdocs, adjuncts, and independent researchers—are particularly susceptible to harm, with fewer institutional protections available to them.

We also acknowledge that while high-profile consequences often come from hostile actors like far-right extremists, researchers can be and are harmed by people across the political spectrum, including those who may share their ideological positions. Risks can also originate from governments, corporations, social platforms, other researchers, and even non-political factions such as online fandoms. This guide acknowledges these complexities and aims to equip researchers with strategies to navigate them.

4. Am I at Risk?

A Is your research risky?

B Should you consider risky research?

4. Am I At Risk?

Risky research makes the scholar vulnerable to external harms. Their career, reputation, family, or life could be threatened because of the research questions they ask and how they answer them. Of course, any research can have unforeseen consequences, but what qualifies as "risky" is very dependent on context. The same research project may lead to radically different outcomes for different scholars, depending on factors such as geopolitical context, researcher identity, and institutional support. This section outlines key considerations for assessing whether a research project may carry heightened risks and how scholars can navigate these challenges.

Is your research risky?

In some cases, scholars are fully aware that their research is risky. However, risks are not always obvious. A project that once seemed uncontroversial may become politically sensitive over time, or a researcher may not initially realize that their work could open them to harms. Mentors and advisors play a crucial role in helping emerging researchers assess potential risks. Supervisors should guide students and early-career scholars in identifying vulnerabilities and developing strategies for navigating them.

There are four categories of risk researchers might encounter:

1. Politically charged topic areas and findings that challenge powerful actors
2. Methods or findings that challenge technology companies
3. The researcher's positionality (including their marginalized and/or racialized identity)
4. The researcher's visibility.

We've included questions below that researchers might ask themselves to help understand whether they might become a target for their work

1. Politically Charged

First, scholars that research topics that are politically charged or map onto major contemporary political controversies are at risk, particularly if the topic overlaps with the concerns of a political fringe, such as the extreme right. Scholars conducting this type of research are likely to be aware that their research is controversial, but they may not be aware that their research is risky. Potential risky topics might include critical race theory, DEI, feminism, reproductive justice, climate change, criticism of powerful corporations or the state, and LGBTQIA+ issues. They can also include contemporary political debates such as questions of election security or the impact of disinformation on political outcomes. Scholars researching non-democratic governments or politically and socially restrictive contexts should know that government actors, ideologically-motivated communities, or corporations could target them.

Research on less obviously controversial topics (income inequality, social platforms, corporate ownership, etc.) may oppose the interests of those in power, such as corporations and nation-states. Scholars engaging in this work may find it more difficult to

gauge the “risk” involved in such research.

Questions scholars engaged in this type of work might ask themselves are:

- Is this topic considered controversial? By whom?
- Is this project critical of or directly counter to the interests of powerful actors (political parties, nation-states, corporations, online/offline movements)?
- Am I entering into any existing political or charged debate, either implicitly or explicitly?
- If I consider the extremes of the political spectrum, does my research support or counter politicized narratives espoused by an extreme group?
- Does this research challenge narratives about history and/or highlight dominant groups’ historical culpability for atrocities or other historical events?
- Does my work critique dominant narratives —including the framing of historical events— held by a government or group with a known history of targeting activists/researchers/journalists with repressive intent?
- Does my research potentially contribute to technologies or policies which will be detrimental to society? Could my research be used to support regressive or anti-democratic social or political movements?
- How visible is my research area right now? Is it widely covered in the media or a frequent “trending” topic of discussion in online spaces?

2. Challenging technology companies

Second, internet researchers in particular are susceptible to attacks from technology companies, particularly if they use methods that violate a platform's Terms of Service (ToS), such as auditing social platforms and scraping platform data. These methods can be met with dismissal by institutional or ethical review boards and even criminal or civil charges. For example, Facebook helped terminate a research project examining how misinformation spreads through political ads on the platform (Ortutay, 2021). The platform sent cease and desist letters to the academics involved and then outright banned them from the site. While the researchers argued that their investigation demonstrated flaws in the Facebook Ad system, Facebook asserted that the researchers’ methods violated the platform’s privacy practices. Even if a project’s methods do not violate the ToS, platforms like X may take action against researchers who publish findings that cast them in a negative light. For example, Meta leveraged its legal team to challenge the credibility of researchers from the Federal University of Rio de Janeiro in Brazil after they exposed flaws and negligence in the platform's ad moderation (Nakamura & Orrico, 2024).

Researchers might ask themselves:

- Do my project’s methods technically violate a platform’s Terms of Service, or related laws such as the US’s Computer Fraud & Abuse Act?
- Are my findings critical of a specific platform, and do they provide findings that might, if publicized, cast aspersion on a platform with a track record of litigious action?

3. Researcher's Positionality

Third, scholars with **racialized and/or marginalized identities, as well as those from underrepresented groups in academia, face a higher risk of networked harassment and efforts to discredit their work.** When their work intersects with politically charged topics, these scholars are far more likely to be targeted with networked harassment, intimidation, efforts to create economic hardship, reputational harm, and other abuse.

In addition, **scholars with racialized and/or marginalized identities can be treated as invaders who must be purged from online spaces even if they are engaging in research that does not appear to intersect with a contemporary political issue.** For example, a scholar engaging in a cultural study of a fandom or an online gaming space may be a target because an assumed participant in that space (e.g., white, cis, straight, male, young) finds out that the researcher has a different identity, regardless of research topic.

Questions scholars might ask themselves in addition to those above are:

- Am I from a demographic group or groups that are racialized and/or minoritized?
- Are the people or spaces that I am studying a culturally cohesive entity who engage in boundary policing of non-members of their community?
- Can I determine or hypothesize the demographic composition of the group under study? Do the dominant identifiers for the group exclude me?
- Do the people in the spaces I study expose beliefs that marginalize any particular population or argue, even implicitly, that any particular demographic group(s) have negative characteristics? For instance, for scholars studying video gaming communities, there may be a collective view in some communities that women create drama in video game groups/guilds or women are not as good players as men.

4. Researcher's Visibility

Finally, a researcher's *visibility* can itself present risks. Any topic can become risky if motivated actors dredge up old articles, conference papers, or social media posts and use them as "evidence" for networked harassment or other harms. Scholars should be aware that new political controversies may retroactively make past work, once unnoticed, suddenly contentious. Moreover, bad faith actors can use online archives (such as the Internet Archive and archive.today) and researchers' social media or institutional profiles to unearth old material that would otherwise be difficult to find.

Questions scholars might ask themselves about this might include:

- Do my public profiles, such as my personal or institutional webpages, include a description of my research interests or topic area? How easy is it to find my contact information?
- Has my previous research been targeted?
- How visible am I on social media? Do I have a large audience that might share my work with individuals who might place me at greater risk for harassment? Alternatively, does this visibility provide some "cover" for my work, if I have already established myself as an expert in this area who can access resources to support me if threats are made?

- Do I engage in public scholarship, such as being quoted in the press, holding public lectures, appearing on podcasts or television, and so forth?
- Do my racialized and/or marginalized identities place me at risk of being targeted if earlier information about me is shared? (This is especially harmful for trans people, for whom publicizing a deadname can be distressing or dangerous in itself.)
- Do I have friends or family who might be easily identified if I were to be targeted, and how easy is it to find their contact information? (This is especially important for people with an uncommon surname shared with family members.)

Should you conduct risky research?

A researcher might decide to continue their research project even if they believe it puts them at risk — many researchers do! But it's also fine if they decide it's not worth the risk. Scholars can conduct controversial research and not face any negative consequences for it, or face severe consequences for something they didn't think would be controversial. Here, more senior scholars who supervise PhD students and early career researchers may need to help them decide whether to continue their research.

If someone determines that their potential project is risky, they should ask themselves these questions to decide whether or not to proceed:

- How easy is it to find your work? Are you dissertating, primarily publishing in academic journals, or writing for broader public outlets?
- Do you expect, or are you expected, to have a "public face" to your research?
- Where are you in your career? Do you have a supportive advisor? Is your employment precarious, or do you have tenure? Do you have the resources to support yourself if your research must be paused or halted? Are you, or could you be in the future, in a location where the government is supportive or hostile to academics?
- Are you involving people with fewer privileges and protections than you? These might include undergraduates, informants, participants, graduate students, postdocs, and non-tenured colleagues.
- What level of institutional support do you have? Who, or which communities, could you contact for support and care? What is the track record of the institution you're in regarding the protection and support of researchers?

The answer to the last question can be difficult to assess; ask your peers or find out if any other scholars at your home institution have suffered adverse consequences and what the institution did, or failed to do, to support them. This will vary depending on the country, whether your institution is public or private, your department, and so forth.

5. Designing Research Projects with Risk Mitigation in Mind

- **A** Working with Hostile or Deceptive Populations
- **B** Working with Big Data or Platforms
- **C** Supervising Students and Postdocs
- **D** Legal Defense
- **E** Working with Traumatic Material
- **F** Accessing Risky Material
- **G** Data Protection
- **H** Grant Applications
- **I** Certificates of Confidentiality
- **J** Fieldwork
- **K** Confidential Communication Channels
- **L** Publishing and Disseminating Research
- **M** Friends, Family, and Loved Ones

5. Designing Research Projects with Risk Mitigation in Mind

Researchers and their institutions can follow these preliminary steps in the *research planning and design stage* to minimize or mitigate risks to researchers and/or research participants. When designing a project, researchers should consider whether to work with hostile populations; safeguarding students, postdocs, staff and personal networks; working with traumatic materials; ensuring data protection; and conducting fieldwork in unsafe physical conditions, amongst others.

Working with Hostile or Deceptive Populations

Some research is risky because it requires working with populations that may be actively hostile to research, academia, or established institutions in general. Organizations that establish research ethics involving human subjects traditionally view research participants as having less power than those researching them, which prioritizes protecting and minimizing their risk. However, as Adrienne Massanari (2018) points out, groups like the far-right complicate these dynamics, in that they can cause real material harm to researchers investigating them. For example, although researchers are strongly discouraged from conducting covert research or deceiving their research subjects, this may be necessary to prevent harassment or doxxing (the revealing of personal, identifiable information about an individual without their consent, such as their home address, telephone number, credit card information, date of birth, or even national identification number, discussed below in Section 7).

Researchers may choose not to conduct in-person interviews or ethnography for their own safety, and opt for digital ethnography, discourse analysis, or desk research. In researching disinformation or propaganda, researchers may encounter attempts to deceive, manipulate, or silence the research. Emma Briant (2024) observes that academic researchers face ethical frameworks when interviewing powerful actors that raise risks and challenges which journalists do not share. These risks may raise particular difficulty for researchers of actors and industries characterized by deceptive activities and/or information asymmetry — risks that may be greater in legal contexts outside the United States (Briant, 2024: 386-387).

For scholars who choose to do traditional human subjects research on hostile populations, it can be challenging to build rapport with people whose values and ideas are not just different from the researcher, but may be directly oppositional (Segers et al., 2024). A researcher's risk is compounded when dealing with populations that may be overtly sexist, racist, homophobic, and so forth. However, this is deeply dependent on the researcher's identity. One study found, for example, that far-right participants were much more likely to talk to female researchers because they found them less threatening (Gelashvili & Gagnon, 2024). If a researcher plans to work directly with hostile or deceptive populations, this will require careful methodological planning; we have listed helpful academic articles on these topics in the Related Reading section.

Working with Big Data or Platforms

Researchers working with large datasets, tech company data, or platform data face a particular set of risks. For example, in recent years, tech companies and social media platforms have responded to researchers investigating them by launching legal threats, including lawsuits and cease-and-desist letters. Tech actors and leaders, bolstered by large sums of money and expansive legal resources, can terminate a research project, even if it is carefully designed. Later in this section, we offer advice for researchers considering these methods, such as ways to obtain relatively affordable legal counsel. While platforms and sites have made it increasingly difficult to acquire large data sets without inside relationships and/or money, some scholars have called for approaches such as "ethical client-side" data collection (Halavais, 2019). With informed consent, this approach would allow for a partnership with users, the very creators of the data, which could shift balance away from governments and powerful corporations. Additionally, the recently-passed EU Digital Services Act includes provisions for mandatory platform data access for vetted researchers, which is scheduled to go into effect in 2025. It is unclear how the union will implement or enforce this act, or how researchers can apply for data access (European Commission, 2024).

Supervising Students and Postdocs

Researchers that work with undergraduate students, graduate students, or post-docs should take precautions when collaborating on risky research topics. Whenever possible, researchers should hire students and postdocs who have an interest in the field and previous experience with similar topics, especially those working on hate speech, violence, and/or the far-right. Leading researchers should have an honest and ongoing conversation with students about the possible risks of such research and share any available university resources at their disposal (counseling, campus police, policies to protect students). They should also ensure that students and postdocs always have the option to take breaks or work on non-risky projects and maintain their funding.

Researchers that run a lab or a similar research group should set up a support group for their students to share their experiences and facilitate connections between students and other researchers doing similar work through their academic network (listservs, professional organizations, etc.). Some institutions even offer monthly clinical supervisions with a therapist. While this practice is more common in disciplines such as psychiatry and social work, other disciplines could include it in research grant budgeting.

At minimum, institutions should advise that supervisors of graduate students whose projects are risk or trauma-based, or whose positionality as a researcher places them at greater risk of distress, undergo mental health first aid training. Where appropriate and applicable, supervisors and supervisees may consider establishing a distress protocol *for the researcher* if they experience distress in response to the data gathered through the course of their research. This protocol should outline early warning signs of distress or or vicarious trauma (Moran & Asquith, 2020) and identify strategies for mitigating distress and/or responding to it, which may include regular debriefing with supervisors and/or a

therapist, reflexive journaling and/or creative practice, and alternative tasks for the researcher to undertake. Supervisors should encourage that individual researchers create a personal safety plan to share with others, especially those with a history of mental health problems and/or suicidal tendencies.

Lead researchers can also model best practices. For instance, early career scholars doing risky research should be advised not to use their personal phone or laptop and set up a separate email address for their research (many universities allow email accounts to have multiple “aliases”). When it comes to publishing collective work, lead researchers should let students choose whether or not to publish under their own name. Publishing with attribution is important for early career scholars, but it also presents potential risks. Faculty researchers should discuss the pros and cons of this decision with students so that they can make an informed choice. If students do not want their name associated with risky research projects, consider removing student names from public project-related content or assigning persistent pseudonyms that could be changed later.

Finally, some researchers fear that risky research that involves exposure to or immersion in extreme positions may lead the researcher to adopt those positions themselves (“radicalization”). However, we were unable to find empirical, or even anecdotal, evidence that this has actually happened; in most instances where a researcher has taken up far-right positions, they had a propensity to such views before beginning their work. We found that it is far more likely that students will suffer from vicarious trauma from viewing extremist material, which makes it imperative that researchers supervising such students are aware of this risk and take steps to mitigate it.

Faculty researchers and principal investigators (PIs) have more job stability and privilege, and should advocate for their students within departments and institutions. Their advocacy efforts may include training students on cybersecurity best practices, allowing students to work on other projects, making riskier projects optional, acting as the point person for all media inquiries and public discussions of the risky project, and creating a communicative safety plan for times when students feel the consequences of risky research more acutely. If negative consequences do occur, leading researchers should advocate for the needs of their students to the university and, if necessary, assist them in locating resources.

Legal Defense

When designing a research project that may involve methods contrary to a website or platform's ToS, researchers should explore whether their university or a nearby institution offers free legal clinics. Different countries have varying legal frameworks, so researchers should familiarize themselves with the potential legal implications of their work. These clinics provide legal advice tailored to the research's public interest implications.

In the United States, Harvard Law School's Cyberlaw Clinic provides student researchers with free legal guidance, and the Tufts Cybersecurity Clinic for the Public Good offers free

security consulting for nonprofit organizations. Additionally, many U.S. universities allow graduate students to purchase affordable legal insurance, which typically includes a limited number of consultation hours with a generalist attorney. While these attorneys may not specialize in internet or platform research, they can assist with contract reviews and responses to cease-and-desist letters. In such instances, it is crucial to recognize that the university counsel's office primarily protects the university's interests, which may lead to overly cautious advice. For example, they might instruct a graduate student to cease all research on a topic as a precautionary measure, viewing this as a low-cost solution to potential litigation risks. See Section 8 for more information.

Working with Traumatic Material

When conducting risky research, scholars may encounter traumatizing materials, including graphic images, videos, firsthand exposure to conflict zones, or other evidence of atrocities. Many researchers are unaware that working with distressing media content in an office or other non-field setting can be as traumatizing as fieldwork, due to repeated exposure (Eyewitness Media Hub, 2015). This phenomenon, referred to as “research related trauma,” can manifest in both physical and psychological symptoms, including mood swings, depression, strained interpersonal relations, headaches, nausea, and chest pains (Loyle and Simoni, 2017). Despite these risks, academic institutions often fail to acknowledge or address the long-term toll such work can take on researchers.

Before engaging with a project involving traumatic materials, researchers should assess their own risk factors and discuss them with their community or network. During data collection, they should establish boundaries, such as avoiding exposure to distressing content in the evening, and set aside time for reflection and discussion. When working with traumatic media content, strategies like muting or minimizing sound, pausing videos, and taking regular breaks can help manage emotional strain. Researchers should also identify the types of content that affect them most deeply and develop a plan for handling such material, including informing colleagues or research leaders. When sharing sensitive materials with others, researchers should provide content warnings to minimize potential harm. Supervisors or PIs should model healthy practices by maintaining a sustainable work pace, taking breaks from exposure, and openly acknowledging the emotional challenges of the work.

Accessing Risky Material

Working with risky material like sexually explicit content, hate speech, and extremist media has practical implications beyond its traumatic potential. For example, in some countries it is illegal to access terrorist media. Researchers should also consider whether they will report material that is illegal or harmful, such as violent threats or sexualized images of minors, and if so, to who. Flagging content on social platforms is fairly low-risk to the researcher; one study of terrorism researchers found that 42% had reported “dangerous actors or violations of the terms of service” to a social platform (Khalil, 2021). This becomes much trickier when reporting content on fringe websites, private chat channels, or online archives, or reporting to law enforcement. While there is no legal

obligation in the US or UK for researchers to report even illegal content (McLoughlin, 2021; O'Connell, 2010), there may be a moral obligation.

When planning a project, researchers should consider these questions ahead of time:

- Are you mentally, emotionally, and practically prepared to report content?
- Do you know who to report content to?
- How will you determine whether or not to report content?
- Does the content include an explicit or detailed threat? For example, does it mention a particular place, time, and method?
- Is it targeted towards a specific person?
- Does it involve personal information, as in doxxing?
- Does it involve children or minors? Child sexual abuse material (CSAM) can be reported via the NCMEC's Cybertipline, even if you are outside the United States; the EU, for example, relies on NCMEC reporting to identify CSAM.

Some online communities, such as far-right message boards, claim to monitor the IP addresses of those who access them. When accessing extremist online spaces, researchers should always use a clean browser with a virtual private network (VPN) and save websites as PDFs to avoid revisiting the live site. It is also generally unwise to access risky material on university-owned computers.

Data Protection

When designing a project involving risky subjects, researchers should consider data protection during the planning stage. In some cases, universities or granting bodies may require a risk assessment or data management plan before beginning a project, which allows researchers to think through these issues in detail. Most ethics boards or IRBs will also mandate safety measures to protect participants, which can, in turn, benefit researchers.

For most projects involving risky topics, participants should be deidentified and anonymized. For example, paraphrasing interview transcripts in published materials can prevent identification through language patterns, particularly in small communities. Researchers should avoid collecting personal data on vulnerable participants unless it is strictly necessary for the study. Conversely, when researching powerful individuals who should be held accountable, "naming and shaming" may be necessary.

To safeguard both researcher data and participant identities, researchers should carefully follow their institution or locale's regulations on data storage. Some people choose to use multiple encrypted and backed-up drives instead of cloud storage. When possible, using physical notebooks, paper diaries, or in-person conversations—rather than emails or digital records—can enhance security. Any physical records should be stored in a locked, researcher-only accessible location.

Data protection is a critical aspect of researcher safety, particularly in light of cases where government entities have subpoenaed research materials. As discussed later in Handling

Lawsuits and Subpoenas, limiting the collection of sensitive personal data and ensuring proper deidentification can help mitigate legal and ethical risks down the line.

Grant Applications

When writing grant applications, keep risk mitigation in mind. Researchers should include budget items for increased researcher safety, such as training for research staff and PIs, information security and storage, encrypted devices, confidential transcription services, therapy or counseling, and/or increased safety protocols. As universities worldwide face increasing threats, ensuring the security of research data has become a major concern. Researchers may need access to secure information storage solutions beyond university infrastructure, which can be budgeted for.

Certificates of Confidentiality

Note: This section is specific to research in the United States

In the US context, certificates of confidentiality prohibit the disclosure of identifiable, sensitive research details to anyone not connected to the research, except when the participant consents or in a few other unique situations. The act of Congress generates these certificates, which work to shield and protect the privacy of research participants. Certificates of confidentiality act as a safeguard “against the disclosure of potentially identifiable data, including as part of lawsuits and subpoenas” (Research Support Consortium). One study found that most cases involving legal demands for research data were frequently resolved without giving up participant information (Wolf et al., 2012).

Some grant providing institutions and organizations, such as the National Institutes of Health (NIH) and the Department of Health and Human Services (HHS), automatically give certificates of confidentiality to studies under their purview. When designing a research project, researchers should consider whether their projects might need certificates of confidentiality. They should also check whether their project will be automatically granted a certificate or if they need to apply before their research starts. Researchers not associated with the NIH can apply for a certificate of confidentiality through an online system.

Fieldwork

Some research projects may require fieldwork at a risky site— for example, with far-right participants or in authoritarian countries. The following advice is for people undertaking such fieldwork.

Determining Risky Travel Destinations

Researchers conducting fieldwork abroad should check if their home country provides a list of destinations deemed inadvisable for travel. For example, the United Kingdom's Foreign and Commonwealth Office (FCO) maintains a "foreign travel advice" list that includes travel warnings, safety and security information, and health risks. Conducting fieldwork in a country that one’s home nation advises against visiting may be complicated. Their home university may prohibit such travel or, at the very least, require approval from university administrators. Additionally, the university can approve the trip,

but the researcher may be ineligible for university or general insurance coverage.

Informing Key People

Before starting fieldwork, researchers should make a list of "key people" to inform about their risky research. This differs based on national and institutional context.

In the United States, researchers should inform the Chief Information Officer and Campus Safety of the location and potential risk of their fieldwork. Graduate students should also notify their advisor, PI, or senior colleagues. If possible, the researcher should keep their institutions and supervisors updated of any discomforts they may have had in the field. Keeping institutions and supervisors updated on any discomfort or concerns that arise in the field can help identify risks that may be difficult to recognize while immersed in research and building trust with participants. (Note that if one's research could be deemed illegal, such as violating a platform's ToS or the Computer Fraud and Abuse Act, it may be necessary to remain discreet within the larger institution. Talk to an experienced mentor for advice.)

In Europe, graduate researchers typically first consult their advisor when planning fieldwork. They should discuss potential risks and confirm whether their advisor is available for ongoing communication during their research. Additionally, researchers should notify their university's security services, ethics committee, and research safety committee (if available). These committees can document the researcher's travel plans and provide essential guidance and support.

Researchers should also have a trusted person local to their fieldwork, preferably someone who knows the local language(s) and customs. In such situations, prioritizing prevention is key. Researchers should not hesitate to let their support networks know if unusual or worrisome events unfold.

Formal and informal support networks are crucial for researchers undertaking risky or potentially traumatizing fieldwork (Schultz et al., 2023). Researchers can establish these networks through snowball networking, social media, conference listservs, or even cold-emailing other researchers in the field. Building these communities before starting fieldwork allows the researcher to rely on a support system while in the field. During fieldwork, staying connected with experienced researchers through messaging, video calls, or other virtual exchanges can offer valuable stability and reassurance (Schultz et al., 2023).

Minimizing Risk in Lone Fieldwork

Researchers often face situations where they must conduct fieldwork alone, which can be uncomfortable, frightening, or even dangerous.

To minimize risks, researchers should consider the following strategies (Demery & Pipkin, 2020):

- Discuss potential risks with colleagues and supervisors and develop appropriate preparations.
- Familiarize themselves with and adhere to international laws, local laws, and customs.
- Connect with other researchers who have experience conducting fieldwork in related high-risk locations.
- Take advantage of opportunities to enhance field safety, such as self-defense training, first aid courses, or cultural history education about the site.
- Maintain regular contact with field site managers, informing them of their plans and whereabouts as a point of contact.
- Always carry proper credentials, including identification, relevant permits, and proof of university or institutional affiliation.

This structured approach can help researchers navigate the challenges of solo fieldwork with greater safety and confidence.

Documenting Risk During Fieldwork

When a researcher feels at risk, it is crucial to document the situation in detail. If this feels overwhelming or emotionally taxing, involve or contact a friend or trusted colleague. While risk and perceived threats can be harmful, they may also provide valuable data. However, the safety of documentation depends on the research context, and researchers should assess whether recording details could pose additional risks.

Researchers should do a **quick risk assessment** asking themselves:

- Is my personal and digital space likely to be breached?
- Are there any people who pose a risk to me who may go through my belongings or files?
- If I identify a specific risk, do I know who is making threats and what their goals are?

If the researcher **answers "yes"** to the above questions, documenting threats may carry greater risk and require more care. In such cases, they should consider whether a trusted person can securely store the files. If so, copies of the documentation can be sent to them and then deleted from the researcher's devices and workspace to prevent unauthorized access. Alternatively, researchers might send physical documentation to their home address by post, provided they trust the postal service, as a way to remove sensitive materials from their immediate environment.

If the researcher **answers "no"** to these questions, they should document their experiences in a physical notebook and keep that notebook on their person, or safely tucked away. Researchers must make sure not to leave their notes anywhere they may be lost or found by risky agents. Researchers should make a copy of their notes, back them up, and secure them with a password if possible.

Confidential Communication Channels

Researchers should consider using encrypted communication channels when they conduct research or talk to colleagues. This is especially important if the researcher works for a public institution and is in an area where email is subject to public records requests. Beware that the protection provided by encryption for data at rest can be bypassed by spyware or direct physical access to a phone or computer.

Below are some examples of encrypted services for communication:

- **Protonmail**: a free and secure email service where data is protected under Swiss privacy law.
- **Signal**: a free open-source, encrypted messaging service for instant messaging, voice calls, and video calls. Signal does not collect metadata, but does collect phone numbers. Signal is broadly recommended as the most secure end-to-end encryption (E2EE).
- **WhatsApp**: a free instant messaging and voice-over-IP service. WhatsApp is end-to-end encrypted by default. The service relies upon Signal's protocol, collects metadata, and shares data with Meta for marketing and profiling.
- **SecureDrop**: an open source file submission system, with its own protocol, used by newsrooms and nonprofits for whistleblowers to securely transfer sensitive documents
- **RiseUp**: a volunteer-run organization that provides email, mailing lists, private wikis, real-time collaborative text editors, and file upload services.
- **Jitsi Meet**: an encrypted and open source video conferencing service.

Services to avoid:

- **Facebook Messenger and Instagram Direct**: Free instant messaging services developed by Meta Platforms. These services do not offer end-to-end encryption and Meta will have access to that data.
- **Telegram**: Does not use end-to-end encryption by default.
- **X**: We do not recommend using X. While X allows its users to directly message each other, these messages will not be end-to-end encrypted by default. There is no end-to-end encryption on group messages, photos, or videos. Flaws that would allow for breaking the encryption have been reported.

Publishing and Disseminating Research

Before a researcher publishes or disseminates research that they have deemed risky, they should contact trusted colleagues and institutions. During this conversation, a researcher should explain that they anticipate receiving backlash from their research and would like to figure out ways the person or institution can support them should that happen. For example, the researcher might arrange for a friend to read their email or BlueSky messages if they are harassed online, or they might inform campus security that hostile actors are targeting them.

Researchers may consider publishing under a persistent pseudonym or a different first name than their legal name to avoid having their academic identity connected to their

friends and family. A persistent pseudonym is akin to a “pen name” in that the author always uses the same name, but it differs from the author’s legal name. Even a different first name can make the author much more difficult to find, especially if their last name is common, like Li, Smith, or Garcia.

Graduate students have the right to embargo their dissertation projects. A dissertation embargo means that the writing is restricted, and only the title, abstract, and citation information are released to the public. The actual text is not released to the public and is kept hidden for a period of time (typically one to five years). Universities will hold different policies regarding embargoes; therefore, researchers must be in communication with their university’s graduate school or institutional repository. If their dissertation involves risky research, an embargo can be useful because after the embargoed time, the researcher may have found more stable employment which is less vulnerable to attacks, or other risks of their research may have died down. Many universities in the United States, the United Kingdom, and Australia allow dissertation embargoes; outside these regions, students should check their university’s specific policy.

When accepting talk invitations, researchers should find out if their talk will be recorded and published to YouTube or other social platforms. Often, a researcher will need to sign a release to enable this; researchers are well within their rights to refuse. Speakers can also ask their hosts not to use their photo to promote the talk, and use an illustration or stock photograph instead.

Recently, there has been a surge of accusations of plagiarism in the United States, primarily driven by conservative groups targeting critical scholars, especially those studying DEI or LGBTQIA+ issues. In these cases, academics are discredited over minor and/or inconsequential errors in their earlier work, such as failing to properly attribute a source. Typically, their critics use AI tools to scrutinize scholars' publications for missing quotation marks, paraphrasing errors, or lack of attribution. In other cases, some professors have been accused of using generative AI tools to generate work, but AI detection tools are highly fallible. These trends serve as a warning to researchers that such tactics could be used against them. As a result, it is crucial for scholars — especially those whose work defends the legitimacy of DEI or queer civil rights — to exercise extreme caution when publishing and sharing their research.

Friends, Family, and Loved Ones

Researchers should consider whether their dependents or loved ones, such as children, partners, or parents, could be at risk due to their association with the researcher. These individuals may face unintended consequences, making it important to discuss the potential risks of sharing information online, including photos or public familial connections. Families or social groups could transition to encrypted communication apps such as Signal or WhatsApp for private communication. However, not all loved ones may be equally supportive of these privacy measures, which could create tension within their support network. Addressing these concerns early can help navigate potential challenges and ensure a shared understanding of the risks involved.

6. Mitigating Individual Cybersecurity and Privacy Risks

A Data Privacy and Cybersecurity Practices

6. Mitigating Individual Cybersecurity and Privacy Risks

Anyone can face risks regardless of how many preventative steps they take. It is very important not to criticize or blame anyone for experiencing harm, even if they could have done more to protect themselves. This section outlines steps and best practices researchers can adopt before and during the research process to help minimize harmful consequences.

Data Privacy and Cybersecurity Practices

There are a variety of preventative technical solutions that can be used to protect privacy if a researcher is at risk of being harassed, doxed, stalked, or blackmailed. Practicing baseline cybersecurity and privacy practices can shore up several immediate vulnerabilities. We recommend a researcher spends a few weeks *before* disseminating any research engaging in these basic operational security (OpSec) measures. Guides like Equality Labs' *Anti-Doxing Guide for Activists* provide detailed, step-by-step instructions on protecting one's online information and making digital devices more secure. First, researchers should assess what personal information is publicly available, a practice sometimes referred to as "self-doxxing."

To minimize risk, consider the following steps:

- **Search for personal information online**:
  - Google your name and check university websites for publicly listed details.
  - Look up your address on sites like Whitepages.com, Spokeo, or other data aggregators.
  - Check to see if your office location and office hours are posted on university websites.
  - See if your phone number appears on your CV or other publicly available documents.
- **Assess social media and pseudonyms**:
  - Search for any pseudonyms you have used, past or present, to see if they are linked to your full name or other identifying details.
  - Review profiles on LinkedIn, Facebook, Twitter/X, and other platforms to check what appears in search results.
  - Adjust the privacy settings on all accounts you are currently using to ensure only information you are comfortable sharing is visible.
- **Check older and archived accounts**:
  - Look for inactive accounts on older websites (e.g., MySpace, Flickr)
  - Search the Internet Archive and archive.today to see if personal information is still accessible.
  - Delete unused accounts when possible.
  - If you are a long-time Twitter/X user, consider archiving your old tweets.

- **Secure shared documents**:
  - If using cloud-based platforms like Google Docs, ensure that files are only accessible to trusted collaborators.
- **Enlist a second opinion**:
  - Ask tech-savvy friends or colleagues to conduct similar searches—they may find information you overlooked.

Once a researcher has an idea of what information is publicly available, they should take action to remove or restrict access to it. If their information appears on white page sites or data broker sites like Acxiom, they should use the site's opt-out page to request that it be removed. The Big Ass Data Broker Opt-Out List provides links and instructions for 50+ of these sites and ranks them by level of importance. Commercial services like DeleteMe will do a mass opt-out for a fee and monitor the accessibility of personal information on other platforms. Researchers affiliated with a larger institution or center should check whether their organization has a subscription to such a service that affiliates can use.

Depending on the need for appointment scheduling, researchers should make their Outlook or Google Calendar private. A publicly accessible calendar can inadvertently expose personal details about their schedule and location to unverified individuals. Similarly, removing personal contact information like email, phone, and office number from publicly accessible CVs can help reduce risk. Researchers should reach out to university staff to remove any personal information from university websites, and communicate with other faculty and staff about their privacy concerns. For example, a researcher might tell whoever answers the department phone not to reveal anything about them without explicit permission.

Before a researcher disseminates any research, they should consider deleting their Twitter/X account or making it private. X is a key site for online harassment and is increasingly unsafe. BlueSky and Mastodon are good alternatives. We recommend that researchers change their privacy settings on any social media site to require two-factor authentication (2FA) and use strong passwords. They also might consider using an online pseudonym and different profile pictures for each site so that they cannot be easily tracked.

Once the researcher is confident that their personal information is secure and no longer publicly accessible, they should begin to build out cybersecurity protocols that will protect them in the future. Researchers should create an alternative email that they can use for all public-facing interactions, and set it to forward emails to their “real” email. This allows scholars to communicate with others without revealing their “real” email, and if the “fake” email is compromised, they can delete it without too many repercussions. Researchers should create a Google Voice (US, Canada, UK, parts of EU) or Dingtone (available in more countries) number to use when they don’t want to share their personal or office phone number.

Researchers should also create strong and unique passwords for all their accounts and

devices. Check which apps or sites have access to each other and remove anything unwanted. We highly recommend using a password manager like KeePassXC, 1Password, or LastPass to keep track of passwords. Note that there is a difference between password managers that keep information in the cloud and locally-stored password managers; local password managers are more secure but more complicated to use, especially with multiple devices.

Researchers should check whether their emails, passwords, or accounts have been compromised in data breaches. Websites like HaveIBeenpwned and password managers like 1Password and Chrome will check saved passwords against known data breaches and alert the user if any have been compromised. Enabling two-factor authentication (2FA) on one's phone adds an extra layer of security, helping protect accounts even if passwords are leaked before they can be changed. Additionally, watch out for phishing scams designed to trick users into sharing personal information or downloading unverified files. To avoid falling for a phishing scam, always manually check website URLs before entering passwords or sensitive data, and never install or download software without knowing its source.

Finally, if a researcher lives with a partner, roommate, or family member, encourage them to undergo similar steps. Avoid posting publicly about spouses, children, or other dependents and make sure they are aware of online safety precautions.

7. Handling the Potential Outcomes of Risky Research

- A Handling Harassment
- B Responding to Harassment
- C Handling Stalking and Threats
- D Handling Doxxing and Hacking
- E Handling Blackmail and Extortion
- F Handling Lawsuits and Subpoenas
- G FOIA Requests and Privacy Requests
- H Handling Reputational or Professional Damage
- I Handling Research-Related Mental Health Care

7. Handling the Potential Outcomes of Risky Research

If researchers experience harassment or other harms, they should not blame themselves or take responsibility for the actions of hostile actors. Many women are encouraged, in both overt and subtle ways, to take personal responsibility for how others react to them. However, it is essential to remember that the harasser, not the researcher, is at fault (Veletsianos and Hodson, 2018).

Harassment, doxxing, or blackmail can be isolating, but researchers should resist withdrawing from their community. For example, blackmail and ransomware tactics are often intended to isolate the victim and convince them that telling others about the situation will lead to further harm. This is done intentionally to make the victim think that the only thing they can do is accede to the perpetrator's demands.

Depending on the attack, researchers may need to keep their circle of trust small and be selective about who they confide in. Some friends, colleagues, or mentors will be better equipped to understand the situation and offer meaningful assistance than others. (It is worth creating a thoughtful, strategic list of trusted contacts and the types of support they can provide.)

While for many researchers it may be common sense to involve the police or state, this can be risky, uncomfortable, or frightening for people from marginalized groups, who suffer disproportionately from police discrimination and violence, or who research national security. In the United States, the ACLU and NAACP provide guides for people from marginalized communities on how to interact with police and understand their rights in many different contexts.

Handling Harassment

The most well-known consequence for risky research is harassment. "Harassment" is a fairly broad term encompassing actions ranging from name-calling to death threats and physical violence, but scholars have identified multiple types of harassment. Dyadic harassment is when one person harasses another repeatedly over time; this resembles stalking or cyberstalking. Networked harassment happens when a group of people, often loosely connected through social media, targets an individual for harassment. Each participant may send only one or two messages, but the target experiences it as an onslaught of hate. Normalized harassment exists in spaces where hateful language is common (such as some online games or sites like 4Chan) and women, people of color, LGBTQIA+ people, etc. may be routinely subject to slurs or sexual harassment just for existing (Marwick, 2023). In other cases, people may use the term harassment when they are subject to legitimate criticism. For example, YouTuber Carl Benjamin (Sargon of Akkad) repeatedly targeted feminist game critic Anita Sarkeesian, but accused her of "cyberbullying" him when she spoke out against his criticism. In this context, researchers

should be most concerned with networked harassment, although dyadic harassment is also possible.

Gamergate, the famous 2014-2015 campaign targeting female video game developers, critics, researchers, and their supporters, brought networked harassment into the mainstream. Notably, Gamergaters targeted members of the Digital Games Research Association (DiGRA), furthering a conspiracy theory that feminists were "infiltrating" video game research to bring down video games. This campaign specifically targeted feminist video game scholars, several of whom are AoIR members. Shira Chess and Adrienne Shaw (2014, 218) later discussed their experiences in a journal article, writing:

> ***The focus on DiGRA and our own work has given us a jarring reminder of how often feminist research and ideology become targets for hate speech, regardless of the specifics or context. As feminist research becomes a more prominent part of other research areas, we realize that the results are often mixed. While our research, and the research of other feminist scholars might help create more awareness, it also opens scholars up to the very harassment they are studying.***

Unfortunately, more than a decade later, these issues are more salient than ever.

Responding to Harassment

If a researcher is actively experiencing harassment, they should immediately turn off mobile notifications to reduce stress. If possible, they can ask a friend or partner to review them instead. The amount of time a researcher might need to turn off mobile notifications will vary depending on the nature and intensity of the harassment. For some, 72 hours will be long enough, while for others it may be days or even weeks. Scholars should also block their harassers immediately. If there is a risk of SWATting—where harassers falsely report an emergency to send police or emergency services to their address—they should contact local law enforcement preemptively. This is especially critical in countries where police officers carry firearms, as SWATting can escalate into a life-threatening situation. Additionally, researchers should inform their institution about the harassment to ensure they receive appropriate support and protection.

Handling Stalking and Threats

As researchers engage in potentially controversial work, they may become targets of public anger, increasing the risk of stalking. While stalkers and their victims can be of any gender, women are at a higher risk of being stalked. In its most extreme forms, stalking can lead to physical assault or even death, but even when it does not escalate to violence, stalking often causes long-term psychological, social, and economic harm (Logan, 2023). Victims may feel compelled to move or leave their jobs to escape their stalker, and even after the harassment ends, often struggle to feel safe (Logan & Showalter, 2023). There is an ongoing debate about whether cyberstalking is simply an extension of offline stalking

or a distinct behavior. Although it is often perceived as less serious than offline stalking, cyberstalking can inflict the same psychological, emotional, and financial damage (Kaur et al., 2021).

For researchers experiencing cyberstalking, blocking the harasser is often the first step. However, platform policies vary—X (formerly Twitter) recently removed the ability to block accounts, while platforms like BlueSky still allow it. In some cases, muting, hiding, or restricting access to one's content may be a better choice than outright blocking, as these options prevent the antagonizer from knowing they have been muted, potentially reducing retaliation. The Online Harassment Field Manual provides a platform-specific guide to available muting and blocking tools.

The decision to report harassment, stalking, or abuse online is a personal one. Reporting produces a paper trail of documentation and may lead to consequences for abusers, such as platforms removing the harmful content or deactivating the abuser's account. Historically, platforms have not always been supportive or responsive to reports of abuse or stalking (Amnesty International, 2018), so researchers should be prepared for the strong possibility that reporting will not lead to meaningful outcomes. Each platform has different community standards and requirements, and researchers may need to familiarize themselves with the specifics of each one. Researchers may also want to enlist friends, family, or trusted colleagues to help monitor harassment, report violations, and share in the emotional and logistical burden of responding to cyberstalking.

Handling Doxxing and Hacking

State-backed hackers increasingly target not just governments and politicians, but civil society— including researchers, academics, NGOs, and journalists—to obtain documents or communications that can be weaponized to fuel conspiracy theories, drive distrust, or silence and intimidate critics (Briant, 2023a, 2023b). Identifying the perpetrators behind such attacks may take months, and once hacked information leaks onto social media, it may be framed as public-interest journalism. As Briant (2023a) points out, "hacks and spyware threaten the vital secrecy that protects free expression of both journalists and the protection of their sources under Article 10 of the European Convention on Human Rights (ECHR)" — consequences that can also threaten researchers (287). Scholars have struggled to get hacked information, or disinformation derived from it, removed from platforms, despite the fact that distributing hacked data violates social media policies. Since sophisticated hacks can happen even with the use of encryption and Multi-Factor Authentication, researchers should consider minimizing their use of email for sensitive communications.

Hacks are a common source of information used for doxxing, the unauthorized exposure of an individual's personal, identifiable details, such as their home address, telephone number, credit card information, date of birth, or national identification number. Doxxing is typically intended to intimidate its targets, and can escalate into physical violence, including SWATting, physical altercations, threats or violent acts towards the target and their loved ones, property damage, and increased surveillance (Molas, 2024). Beyond

physical risks, doxxing can also carry legal and policy repercussions. It is often used in lawfare, the strategic exploitation of legal systems to undermine, discredit, or silence individuals (Kittrie, 2015).

In the US, doxxing can also take the form of Freedom of Information ACT (FOIA) requests of public university employees and researchers. In the European Union, data subjects have more rights due to the General Data Protection Regulation (GDPR). The "Right to Erasure," or the Right to be Forgotten, enables victims to request that their personal data be removed from websites. However, this is hard to enforce in practice. For more information, see the GDPR Right to Be Forgotten website.

If a researcher has been doxxed, documenting their experience is important. When possible, the researcher should take screenshots, download the webpage involved, use a web archive like archive.today to record it, or use other methods to keep track of the event. When compiling these, we highly recommend that the documentation be time-stamped with visible URLs; see Crash Override's So You've Been Doxed guide. This documentation can be essential, both for the researcher's own reference and for police or legal authorities assisting them in the future. This does not mean the researcher should leave the dox up if they can help it. Once the dox is recorded, contact the site hosting the doxed information; Pastebin, for example, has procedures for removing private information.

Handling Blackmail and Extortion

Risky research can, in rare cases, lead to blackmail. While there are no documented cases of scholars facing politically motivated blackmail, this may become more common in the future. Academic institutions, including the University of Calgary and Regis University, have already faced blackmail-fueled ransomware attacks (CERN, 2020). During these attacks, highly organized and well-resourced criminal networks demand payment in exchange for restoring access to their computer systems. Similar tactics could eventually be used to target individual researchers, pressuring them to pay ransoms or abandon certain research projects.

Additionally, researchers who experience doxxing, privacy breaches, or data hacks may face personal or sexual blackmail. This form of sextortion (Hendry, 2021), commonly reported by social media users whose accounts have been compromised, could become an increasing risk for researchers engaged in public-facing work.

Online blackmailing can take many forms, including phishing scams, data or photo hacks, and catfishing. These tactics can cause emotional distress, financial loss, and reputational damage for researchers. As outlined throughout this document, the best preventative measures include using password managers, enabling two-factor authentication, and being educated and aware of common phishing tactics and scams.

In most blackmailing scenarios, we suggest that researchers not engage, negotiate, or pay the blackmailer, as this rarely ensures safety and often leads to escalating demands.

Instead, cut off communication with the blackmailer, seek emotional support from trusted sources, and document all interactions with the blackmailer. There is no need to face these attacks alone; leaning on a support network can provide both emotional reassurance and practical assistance in navigating the situation.

Handling Lawsuits and Subpoenas

Note: This section is specific to US law.

Researchers can face lawsuits or subpoenas for risky research. For instance, US Representative Jim Jordan sent Congressional subpoenas to American researchers who had worked on public-private partnerships targeting disinformation or received NSF funding for similar research. Platforms may also target researchers who publish findings that make them look bad, often by claiming they violate their ToS or even the Computer Fraud and Abuse Act (e.g., by scraping). Elon Musk sued the nonprofit Center for Countering Digital Hate for research that showed that disinformation was rampant on Twitter/X, which he claimed led to them losing advertisers, under the guise that they had scraped Twitter/X data without authorization. “Grassroots” activists like Turning Point USA have also sued university and non-profit researchers.

In the context of researcher-produced data, courts in the United States have not established a “researcher-participant privilege,” similar to the doctor-patient privilege doctors are granted in US healthcare (Haney-Caron, Goldstein, and DeMatteo, 2015). For instance, the Belfast Project, generated by historians at Boston College, accumulated oral histories regarding paramilitary organizations and their members in Northern Ireland. The participants signed agreements that stated the “ultimate power of release” of the taped conversations and transcripts remained with the participants. Yet, when United Kingdom authorities requested access to the Belfast Project’s data as part of an investigation of a 1972 murder, the materials were subpoenaed and a district court asserted that the government can decide in such cases to force academic researchers to share their data. In the United States, the best current legal protection for researchers from such subpoenas is to verify they have obtained a certificate of confidentiality for their project/research (such protections are also discussed in the section Certificate of Confidentiality (CoC)). However, it is not known whether CoCs will hold up in court in a highly polarized US political climate in situations involving illegal practices that were formerly legal (such as abortion or gender-affirming care in some states)**.**

FOIA Requests and Privacy Requests

Researchers who work at public universities in the US, Australia, or Europe should know that their email, any documents stored on university servers, and any documents attached to an email may be requested by anyone under the Freedom of Information Act (FOIA). This is also true for anyone who corresponds with employees at public universities; people whose records are not subject to FOIA requests, such as employees at private universities or think tanks, can have their personal information unveiled through FOIA requests. Unfortunately, many actors have begun to weaponize FOIA requests, especially for people receiving public or government funding.

University responses to FOIA vary greatly by institution in the US and Australia, because FOIA laws are state-specific. At some institutions, the University Records office will handle the entire request and will only inform the researcher after it is finished. At other institutions, the researcher may be expected to handle the request themselves, which can be extraordinarily onerous depending on the request. Researchers at public universities in the US should contact their university's Public Records department and find out what the researcher's responsibility will be if they are FOIA'd and what types of records are exempt. In some states, emails that include students are exempted, as are ongoing research projects.

Countries outside of the United States also enforce open record laws. For instance, the 21st century has seen the use of such requests in order to harass climate scientists in Australia and the United Kingdom (Halpern, 2015). Privacy legislation such as the GDPR or "Right to be Forgotten" in Europe can also be used by hostile research subjects to request access to data used to misrepresent the research(er) in an influence operation. It can also be used to require deletion of data, with potential implications for censorship of critical information. Researchers in legal situations need greater protections, as FOIA and GDPR requests may be used simultaneously to overwhelm the researcher. An environment of constant scrutiny and surveillance can discourage and suppress scholarly work.

If researchers are subject to GDPR or FOIA, we recommend using one of the confidential communication channels listed in Section 5 (Confidential Communication Channels) rather than official university email to discuss risky research. Researchers should not use their university-provided computer; they should use a personal computer, and avoid storing documents in university-provided cloud storage such as OneDrive. This may violate university policy and researchers should provide stored information when required by law. However, the university will most likely not ask for information stored on personal computers or in private accounts.

In any of these cases, researchers should not expect that their university's lawyers are legally required to protect or represent them. Importantly, the researcher's interests and the interests of the university and its lawyers may not align. In some cases, the researcher may be able to receive pro bono legal coverage if their cause is sympathetic from entities such as the Researcher Support Forum, the American Civil Liberties Union, the Electronic Frontier Foundation, the Foundation for Individual Rights and Expression (FIRE) or similar groups. The UMass Amherst toolkit also offers advice for recommended email usage and details regarding FOIA requests.

Handling Reputational or Professional Damage

Critiques of researchers can manifest in various forms. When a researcher is being attacked or criticized in a public venue, they should pause to consider what exactly they are being denounced for and by whom. Critics usually fall into two categories: sympathetic forces or hostile forces. Most of this document assumes hostile forces; if the alt-right attacks a researcher, for example, most people in their academic circles will

probably be concerned and understanding. Sympathetic forces, on the other hand, share the political or ideological views of the researcher or are fellow academics. Their critiques can be far more harmful to one's professional standing. If a researcher is accused of stealing someone's work, making a sexist/racist comment, conducting unethical research, or violating another shared norm, their reputation is much less likely to survive.

When dealing with sympathetic forces, especially if a researcher is accused of something they believe they did not do, there is an impulse to explain themselves on public platforms, such as on Twitter/X or through a Medium post. If only people knew the entire story, they think, then others would take their point of view. However, this is extremely likely to backfire. When a researcher is accused by people with less power than them of violating power differentials, the researcher should take the time to try to get past their defensiveness and see if the accusations are correct. If they are, the researcher should give an honest apology and try to rectify the harms of their actions. If they are not, it's probably best to say nothing. In either case, a defensive statement is much worse for a researcher's reputation and the optics of the situation than saying nothing at all. However, if a researcher knows individuals trusted within key communities of concern, if they can reach out to them to speak on the researcher's behalf.

A researcher might handle such a situation differently if hostile actors harass them. In such cases, hostile forces can attack a researcher's publications and research, but may also bring up personal matters unrelated to their work. Different forms of harassment may call for varied responses. While it is painful to be attacked personally, directly interacting with the perpetrator rarely stops the harassment. If a researcher works with a supportive academic institution or research group, and harassers are making false claims regarding their research, it can be worthwhile to generate a response quickly and publicly. This response does not have to be directly in conversation with the harasser(s) or accuser(s), but through a venue of the researcher's choice where they can articulate their "truth" or account of what happened. Usually, institutions advise that researchers say and do nothing in response to this harassment, but once rumors or false information have had time to circulate unobstructed, it can be much harder to delegitimize them. Therefore, researchers should have a contingency plan already in place with institutions if such circumstances occur and have access to trusted advisors who understand the media and legal landscape who can offer their wisdom regarding a researcher's particular situation.

It is significant to note that a researcher's positionality may affect how they should handle harassment of a personal or intellectual nature. Since members of marginalized and precarious communities receive the most harassment and often the most vitriolic comments from harassers, it is crucial to protect such members of our intellectual community.

Being harassed on social media or sued will not be good for a researcher's professional reputation. This is especially true for people in precarious positions such as adjuncts, graduate students, and post-docs. In some instances, institutions have sought to publicly distance themselves from targeted faculty members, which can appear to legitimize the

abuse and exacerbate the harassment the faculty member receives. As noted above, an attack can have significant impacts on the target's mental health and well-being. Harassment can hinder a researcher's career and work performance, such as not meeting tenure milestones or being discounted from potential promotion. Researchers may also face professional consequences such as job loss, refusal of visas, being denied tenure or promotion, and the weaponization of complaints protocols against faculty.

Handling Research-Related Mental Health Care

The mental health consequences of risky research are serious. This type of research often involves threatening and stressful situations, personal risk, and the consequences of witnessing highly negative situations (Newman, Simpson & Handschuh, 2003; Rager, 2005). This creates hazards for researchers and their ongoing well-being.

At the same time, the culture of academia can provide additional stress and trauma. Mental health researchers have highlighted the concerning mental health consequences of pursuing graduate school and academic careers overall (Gewin, 2021; Murguía Burton & Cao, 2022; Nicholls, Nicholls, Tekin, Lamb & Billings, 2022). In some ways, the expectations that researchers have for themselves create a situation that sets up unrealistic standards for behavior and response to harms. The consequences of mental illness can be severe, leading to failed careers and relationships, burnout and even long-term disability and suicide.

Mental health and physical health are intertwined, which means that health issues have mental health consequences and vice versa. Fortunately, there are resources available to help researchers maintain their mental health in the face of the occupational hazard of trauma engagement. Understand that feeling stressed, anxious, or depressed about horrible situations is normal. A sensible person witnessing a murder or a child in pain ought to respond with negative emotions. Consider that there are a variety of risks in certain types of research and that planning to deal with those dangers is part of research planning. Researchers should be honest with themselves about the risks they might encounter. Self-care can help researchers protect themselves from threats to mental health (Lee & Miller 2013; Rager, 2005; Steadman, 2023).

Risky research often deals with broad structural issues that individuals cannot resolve alone. These structural barriers are why we believe that developing safety and care strategies, such as creating a support system, including people studying similar topics, is perhaps the most helpful thing one can do to handle the mental health consequences of risky research. In other cases, especially when viewing traumatic material, it may be useful to check in with friends and family who do not do such research to obtain an accurate assessment of how the work is impacting their mental and physical health. People who research risky material often become desensitized and may adopt "black humor" or other coping mechanisms; sometimes it can be helpful to get opinions from those outside the bubble (Pearson et al., 2023).

Researchers with health insurance and access to professional therapy should obtain mental health services. There are fairly standardized recommendations for improving one's daily mental health, such as sleeping, eating well, and regular exercise. If a researcher suspects that their mental health is suffering due to their research, it is probably advisable to take a break from it for as long as possible. If researchers are not sure, the American Psychiatric Association provides a list of symptoms that indicate that someone might need professional mental health treatment. Most importantly, research is an occupational hazard and one's employer should be responsible for providing access to mental health care. However, this is not always possible or realistic. If a researcher does not have health insurance, there are options for free and sliding scale mental health resources. For instance, the United States has organizations such as the National Association of Free and Charitable Clinics and Mental Health America to help uninsured or underinsured individuals find care.

Crisis Resources

If a researcher needs help quickly, crisis resources include emergency call resources (such as calling 911 in the US) and helplines (See Section 10, Resources), walk-in crisis centers, and hospital emergency rooms or urgent care centers. All of these options can connect researchers to an appropriate resource.

Individual Practitioners

Medical and mental health professionals can offer a range of services, including diagnosis/assessment, testing, supportive treatment, psychotherapy and psychiatric medications.

Mental Health Clinics/Centers

These provide more comprehensive services than an individual provider. Many provide a team approach. Employee Assistance Programs or Counseling centers at universities also provide a range of services.

Hospitals and Long-Term Care Facilities

These provide services required by people with more serious issues or issues that require an inpatient approach. Substance abuse is frequently one of those problems.

The appropriate approach to treatment depends on the individual, their specific problem, and the situation. Practitioners or treatment teams assess these factors to determine the best course of action. Psychotherapy is the most common intervention, with various approaches, including insight-oriented therapy, cognitive behavioral therapy, task-oriented therapy, and behavioral methods. Therapy can be conducted individually, in groups, or within families.

In addition to psychotherapy, medically trained practitioners may prescribe psychotropic drugs, which require careful monitoring due to potential side effects. In severe cases, hospitalization may be necessary. The rise of remote mental health services has expanded access to care, allowing individuals to receive treatment virtually. Those with health

insurance may have part or all of their treatment costs covered.

Mental health challenges are a natural part of life—they are not moral failures or character deficiencies.

8. Working with Institutions

A Advocating for Yourself with Your Institution

B Best Practices for Institutions

C Teaching

8. Working with Institutions

Working with institutions can be one of the most frustrating parts of this process. Most institutions are not educated about researcher risk. Many are very averse to negative publicity and often shy away from controversial projects and researchers even if the public criticisms are unfair. In this section, we suggest that institutions owe it to their researchers to prepare for these moments and support researchers in ways that address their digital, physical, and psychosocial needs.

Advocating for Yourself with Your Institution

Before a researcher begins their work, it is worthwhile to notify their institution, campus safety network, Chief Information Security Officer or equivalent, and colleagues of their upcoming research project. Unionized researchers should notify their union representative(s) about the risks they face in their research. Scholars should educate their employer (PI, department chair, lab director, etc.) about the realities of online harassment and similar harms. Ideally, researchers could explain what leadership and administrators should do, including sample language for public statements of support; the idea is to make employers partly responsible for helping to minimize the risk. (This guide and toolkits from UMass Amherst and the Researcher Support Consortium can help.) Once a research project is completed and the researcher is considering publication or media work, they should reach out to trusted institutional colleagues if they expect to receive backlash and discuss how they can support the researcher should that happen.

Best Practices for Institutions

For research institutions, it is worth acknowledging that online harassment and intimidation are occupational hazards for scholars who engage in public scholarship. As such, it is important to pledge institutional support for such scholars. This harassment, if left unresolved, has negative consequences for the researcher, the institution, and society as a whole. In such instances, researchers should be able to come to their institutions for help, guidance, and assurance that they will have institutional support. Institutions including UMass Amherst and the Researcher Support Consortium have developed toolkits for institutions to help their researchers if crises arise. These toolkits provide detailed support for institutions to aid their employees, including FOIA policies, pre-made forms, checklists, and other paperwork that might become useful during researcher harassment.

These toolkits highlight how planning and designing proactive measures to handle such moments allow for safer, more diligent responses. For example, the Research Support Consortium highly recommends that institutions, particularly universities, create research support teams made up of communication specialists, security professionals, administrators, and public relations staff that can prepare standard protocols. During crises, clear and supportive communication between the researcher(s) and institutions supporting said researcher(s) is crucial. But there is also a need for cogent communication

with external sources such as the media, politicians, other institutions, or the general public. While such moments of crisis are stressful for researchers and institutions alike, preparation and diligent followthrough can mitigate the damage for both.

UMass Amherst's toolkit includes a response and prevention guide for department chairs, who are often the first person a faculty member or graduate student will contact in the case of research harassment. This guide offers advice regarding communication with the researcher, activating a support system, deciding upon a response to the harassment, and long-term prevention and preparation plans.

The Research Support Consortium also suggests institutions add resources on trolling, doxxing, harassment, and other risks to a Media Relations or Communications office website. This can be a small, but useful step in supporting public scholars. With these resources, institutions can include a statement of support for their scholars, indicating that if researchers receive harassment they should contact the institution, which will help and protect them. Institutions could also hold workshops that openly discuss the harmful consequences of public risky research and brainstorm alternative ways to conduct research that might leave scholars less vulnerable.

Teaching

The UMass Amherst toolkit offers useful advice for researchers teaching at universities. One key recommendation is to post class materials only on password-protected websites. Additionally, instructors should ensure that students understand these materials are protected by copyright, meaning they cannot be shared without the professor's explicit permission. This copyright protection also extends to recordings made during class sessions. While most universities would consider unauthorized sharing of such materials a violation of their conduct policy, this rule should be clearly established if it is not already in place. In US states where professors are required to post syllabi online, we recommend creating a stripped-down version removing keywords like "equity" or "transgender" and posting the full version only on your password-protected campus learning management system.

9. Conclusion

9. Conclusion

This document underscores the importance of recognizing and managing the multiplicity of risks that researchers face — both online and offline — when their work intersects with politically or socially contentious topics, powerful corporate or government interests, or their own marginalized identities. Whether a project involves controversial subject matter, deceptive or hostile populations, or large-scale datasets prone to scrutiny, careful planning and risk assessment is necessary. This guide lays out strategies for designing a study with data protection in mind, establishing communication protocols, and ensuring mental health resources are available. Unfortunately, no matter how conscientious a researcher is, it's impossible to fully protect oneself from the consequences of risky research.

Moreover, as thoroughly as individual researchers may prepare themselves, collective solutions and institutional support remain fundamental in truly addressing the challenges of "risky research." Departments, professional associations, and universities must provide legal guidance, technical assistance, and psychosocial care on a routine basis — not just during moments of crisis. This includes securing more comprehensive funding for counseling or therapy, working closely with IRBs and ethics committees to adapt protocols for evolving digital threats, and establishing clear procedures for responding to harassment or potential harm to researchers. Such measures can foster an environment where scholars do not have to shoulder the weight of risk management alone.

The path toward fostering a healthier, more inclusive research landscape depends on a shared commitment from individual researchers, academic communities, and the institutions that guide them. By collectively supporting safety protocols, institutional policy changes, and stronger networks of care, we protect the freedom to investigate pressing issues — no matter how controversial they may seem. Ultimately, acknowledging and planning for risk can transform the research process from a solitary endeavor into a collective responsibility, advancing scholarship that is as conscientious and caring as it is rigorous.

10. Resources

A Guides and Toolkits

B Location-Specific Resources

C Paid Services

D Mental Health Resources

10. Resources

Guides and Toolkits

General Guides

- Researcher Support Consortium
- Cyber Civil Rights Initiative Online Safety Center (for victims of intimate image abuse)
- VOX-Pol Researcher Resources
- Academic Freedom Crisis Toolkit
- Without My Consent Tool Guide to Fight Online Harassment
- Surveillance Self-Defense Tips and Tools
- Dish of the Day: The Digital Care Meal (Portuguese, Spanish and English)

Feminist Guides

- Take Back the Tech (Take Control of Technology to End Gender-Based Violence)
- Feminist Helplines (Digital Defenders Partnership)
- CFFP Intersectionality and Cybersecurity Toolkit
- Engage in Public Scholarship!: A Guidebook on Feminist and Accessible Communication, Ketchum 2022
- Feminist and Accessible Publishing, Communications, and Technologies
- Kit de Cibercuidado para Activistas

Privacy, Doxxing, and Harassment Guides

- So You've Been Doxed: A Guide on what to do next
- Equality Labs' Anti-Doxing Guide for Activists
- Anti-Doxing Guide for Activists Facing Attacks
- Doxing Prevention Harm Reduction Training
- Extreme Privacy: What it takes to disappear: Fourth Edition. Personal Data Removal Workbook, V. 4.0. July 2022. [PDF]
- How to Prevent Zoom Bombing and Secure Your Meetings
- Surveillance Self-Defense Guide (EFF) and their tips for researchers
- Manual opt-out guides for personal information sites like Spokeo
- Speak Up and Stay Safe: A Guide to Protecting Yourself from Online Harassment
- PEN America's Online Harassment Field Manual

Self-Care and Mental Health Guides

- Digital Safety Kit for Journalists
- SPJ Toolbox Mental health for journalists
- Self-care tips for journalists
- Recommendations for dealing with vicarious trauma from digital media (Eyewitness Media via Internet Archive)
- Journalism and Vicarious Trauma: A guide for journalists, editors, and news organizations (First Draft News)
- Managing Mental Health Podcast Episode with Extremist Media Consultant
- Handling Traumatic Imagery: Developing a Standard Operating Procedure (Dart Center for Journalism & Trauma)

Location-Specific Resources

General Guides (United States)

Arizona
- Address Confidentiality Program

Arkansas
- Address Confidentiality Program
- National Lawyer Guild

California
- Safe At Home address confidentiality program
- TechLEAD
- Citizens Privacy Coalition

Colorado
- Address Confidentiality Program

Connecticut
- Address Confidentiality Program
- Yale Privacy Lab

Delaware
- Address Confidentiality Program

D.C.
- Address Confidentiality Program

Florida
- Address Confidentiality Program

Georgia
- Encode Justice Georgia

Idaho
- Address Confidentiality Program

Illinois
- Address Confidentiality Program

Indiana
- Address Confidentiality Program

Iowa
- Safe at Home Program

Kansas
- Safe at Home Program

Kentucky
- Safe at Home Program

Louisiana
- Address Confidentiality Program

Maine
- Address Confidentiality Program

Maryland
- Safe at Home Program

Massachusetts
- Address Confidentiality Program
- PrivaZy

Michigan
- Address Confidentiality Program

Minnesota
- Safe at Home Program

Mississippi
- Address Confidentiality Program

Missouri
- Safe at Home Program

Montana
- Address Confidentiality Program

Nebraska
- Address Confidentiality Program

Nevada
- Address Confidentiality Program

New Hampshire
- Address Confidentiality Program

New Jersey
- Address Confidentiality Program

New Mexico
- Safety at Home Program

New York
- Address Confidentiality Program
- New York Cyber Abuse Task Force
- Clinic to End Tech Abuse
- Black Movement Law Project
- Calyx Institute: Privacy by Design for Everyone
- Surveillance Technology Oversight Project

North Carolina
- Address Confidentiality Program
- Encode Justice NC

Ohio
- Safety at Home Program

Oklahoma
- Address Confidentiality Program

Oregon
- Address Confidentiality Program
- PDX Privacy

Pennsylvania
- Address Confidentiality Program

Rhode Island
- Address Confidentiality Program
- Rhode Island Rights

Tennessee
- Safe at Home Program

Texas
- Alternate Address Program

Vermont
- Safe at Home Program

Virginia
- Address Confidentiality Program

Washington (WA)
- Address Confidentiality Program
- Stop Surveillance City
- Technology Enable Coercive Control Clinic (run by New Beginnings, an organization for domestic violence survivors)

West Virginia
- Address Confidentiality Program

Wisconsin
- Safety at Home Program

General Guides (Outside the United States)

EU

Right to be forgotten

Australia

eSafety Commission (see: Find Out What We Can Do)

Netherlands

https://www.wetenschapveilig.nl/: a national platform for academics receiving threatening, hateful, or intimidating reactions to their work

France

PAUSE: A program for researchers who cannot carry out research in their home country or country of residence due to censorship or other political, economic, or social barriers

Legal Services (United States)

- **Nonconsensual Image-based Abuse ("revenge porn")**
  - Cyber Civil Rights Legal Project
  - Without My Consent's Copyright Registration Guide
  - Without My Consent's Guide to State Laws 50 State Project Regarding Laws Against The Nonconsensual Distribution of Sexually Explicit Images
  - Stop Non-Consensual Intimate Image Abuse
- **The Foundation for Individual Rights and Expression (FIRE)**
  - Faculty Legal Defense Fund (FIRE)
  - FIRE's Guide to Student Fees, Funding, and Legal Equality on Campus
- American Civil Liberties Union
- Electronic Frontier Foundation
- Tufts Cybersecurity Clinic for the Public Good

Legal Services (Outside the United States)

United Kingdom

- Revenge Porn Helpline

Paid Services

- **360 Privacy**
  - Online data removal, dark web monitoring, etc.
- **ReputationDefender** by Norton
  - Search results removal, remove personal information, etc.
- **DeleteMe**
  - Removes your personal info from Spokeo and similar sites, people finders, public records search sites. ($129/year)
- **Kanary**
  - Finds & deletes unnecessary personal data from any website that puts you in harm's way. ($179.88/year)

Note: Consider asking your department or school to pay for such services, or building them into your grant applications. If you live with other people (partner, family, roommate, etc.), their records may include location information that can be used to locate you. If possible, consider signing them up as well for similar services.

Mental Health Resources

Crisis or Helplines

Before calling any helpline, consider:

- What are their operating hours?
- Is calling free, or is there a fee?
- Is the conversation confidential? For instance, many services have protocols for handling situations where someone mentions a suicide attempt or plans to harm themselves.
- What happens if the line is busy? It's often a good idea to try multiple times, consider calling back later, or explore alternative services.
- Think about text lines if you are uncomfortable talking on the phone. They are available in most countries.

Worldwide

- International Directory of Helplines
- Feminist Helplines Index

Brazil

- Centro de Valorização da Vida
  - Call 188

United Kingdom

- NHS
  - 111 - 24 hours every day
- Samaritans
  - 116 123. Email jo@samaritans.org
- Campaign Against Living Miserably (CALM)
  - Call 0800 58 58 58, open from 5pm–12pm every day
- Shout textline
  - (no calling required) - text SHOUT to 85258

Australia

- Lifeline
  - 24-hour counseling, support groups, and suicide prevention services. Call 13 11 14, text 0477 13 11 14 or chat online.
- Suicide Call Back Service
  - 24 hour support, call 1300 659 467.
- Beyond Blue
  - depression and anxiety - call 1300 22 4636, 24 hour support, or chat online.
- Head to Health
  - advice, connections to local mental health services. Call 1800 595 212.
- MensLine Australia
  - online counseling for Australian men. 24 hour support at 1300 78 99 78 or chat online.

EU

- Mental health helplines by country
- The following work in all EU member states:
  - Samaritans helpline: call 116 123
  - Give us a Shout text line: Text SHOUT to 85258
  - Campaign Against Living Miserably: call 0800 58 58 58

United States

- Call 911
- 988 Suicide & Crisis Lifeline
  - Call or Text 988
- Disaster Distress Helpline
  - Call or text 1-800-985-5990
- SAMHSA's National Helpline
  - 1-800-662-HELP (4357).
- National Alliance for Mental Illness
  - Call 1-800-950-NAMI (6264)
  - text "HelpLine" to 62640
  - email us at helpline@nami.org
- Crisis Text Line - text HOME to 741741
- American Psychological Association Crisis hotlines and resources

Finding a Mental Health Provider

Worldwide

- International Therapist Directory
- It's Complicated
  - Large directory of therapists in major cities worldwide

Australia

- Psychologist locator
- Finding affordable mental health help in Australia

EU

- European Association for Behavioral and Cognitive Therapists

United Kingdom

- Finding free or low-cost therapy in the UK
- Counselling Directory
- BACP Therapist Directory

United States

- Psychiatrist locator
- Psychologists by state
- Mayo Clinic (ND) tips for finding mental health providers
- National Alliance for Mental Health - Finding a Mental Health Professional
- Social Work
  - Clinical Social Work Association
  - Association of State Licensing Boards
  - National Association of Social Workers
- Nursing
  - American Psychiatric Nurses Association
- Mental Health Counseling
  - Psychology Today

11. Related Reading

- A Censorship
- B Gendered Harassment
- C Institutional Responses
- D Online Harassment
- E Research Ethics and Methods
- F Security
- G Support for Scholars

11. Related Reading

Censorship

Tanczer, L.M., Deibert, R.J., Bigo, D., Franklin, M., Melgaço, L., Lyon, D., Kazansky, B., & Milan, S. (2020). Online Surveillance, Censorship, and Encryption in Academia, I*nternational Studies Perspectives, 21*(1), 1–36. https://doi.org/10.1093/isp/ekz016

Tanczer, L., McConville, R., & Maynard, P. (2016). Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. *Journal of Global Security Studies*, *1*(4), 346-355.

Gendered Harassment

Binder, Ines and Hache, Alexandra. (2023). "A Feminist Conversation on Cyber-Security," GenderIt.org, https://www.genderit.org/editorial/feminist-conversation-cybersecurity

Citron, Danielle Keats. (2009). Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review,* 108: 373-415.

Eckert, S., & Riftkin-Metzger, J. (2020). Doxxing, privacy and gendered harassment: The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft, 68*(3), 273-287. https://doi.org/10.5771/1615-634X-2020-3-273

Haché, A., Fong, M., Jiménez, G., & Sánchez, M. (2022). *Digital security and feminist holistic protection as part of temporary relocation programmes for Human Rights Defenders*.

Hodson, J., Gosse, C., Veletsianos, G., & Houlden, S. (2018). I get by with a little help from my friends: The ecological model and support for women scholars experiencing online harassment. *First Monday* 23(8).

Jane, E. A. (2018). Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies, 18*(4), 575–591. https://doi.org/10.1080/14680777.2018.1447344

Linabary, J. and Batti, B. (2019). "'Should I Even Be Writing This?': Public Narratives and Resistance to Online Harassment," in *Gender Hate Online: Understanding the New Anti-feminism*, ed. Debbie Ging and Eugenia Siapera (Cham: Palgrave Macmillan), 317–46.

Pevac, M. (2022). The darker side of feminist scholarship: How online hate has become the norm. *Feminist Media Studies, 22*(5), 1287–1289.

Rentschler, C. (2017) Bystander intervention, feminist hashtag activism, and the anti-carceral politics of care. *Feminist Media Studies, 17*(4), 565-584, DOI: 10.1080/14680777.2017.1326556

Sobieraj, S. (2018). Bitch, slut, skank, cunt: Patterned resistance to women's visibility in digital publics. *Information, Communication & Society, 21*(11), 1700–1714.

Sobieraj, S. (2020). *Credible Threat: Attacks Against Women Online and the Future of Democracy*. Oxford University Press.

Institutional Responses

Gosse, C., O'Meara, V., Hodson, J., & Veletsianos, G. (2023). Too rigid, too big, and too slow: institutional readiness to protect and support faculty from technology facilitated violence and abuse. *Higher Education 87*: 923-941.

Online Harassment

Cocq, C.; Liliequist, E.; Okonski, L. Protecting the Researcher in Digital Contexts. *Proceedings of the 6th Digital Humanities in the Nordic and Baltic Countries Conference* (DHNB 2022) : 195-202. https://ceur-ws.org/Vol-3232/paper16.pdf

Ferber, A. L. (2018)."“Are you willing to die for this work?” Public targeted online harassment in higher education: SWS presidential address." *Gender & Society, 32* (3), 301-320.

Gosse, C., Veletsianos, G., Hodson, J., Houlden, S., Dousay, T. A., Lowenthal, P. R., & Hall, N. (2021). The hidden costs of connectivity: nature and effects of scholars' online harassment. *Learning, Media and Technology, 46*(3), 264-280.

Marwick, A. E. (2021). Morally Motivated Networked Harassment as Normative Reinforcement. *Social Media + Society, 7*(2). https://doi.org/10.1177/20563051211021378

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. MIT Press

Research Ethics and Methods

Ashe, S. D., Busher, J., Macklin, G., & Winter, A. (2020). *Researching the far right: Theory, method and practice.* Routledge.

Briant, Emma, L. (2024) Researching and Conceptualizing the Influence Industry. In: Emma L. Briant & Vian Bakir (Eds.) (2024). *The Routledge Handbook of the Influence Industry*. London: Routledge. Pp 379-394.

Conway, M. (2021). Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines, *Terrorism and Political Violence, 33*(2), 367-380, DOI: 10.1080/09546553.2021.1880235

Damhuis, K., & de Jonge, L. (2022). Going Nativist. How to Interview the Radical Right? *International Journal of Qualitative Methods*, 21. https://doi.org/10.1177/16094069221077761

Dickson-Swift, V., James, E. L., Kippen, S., & Liamputtong, P. (2008). Risk to researchers in qualitative research on sensitive topics: Issues and strategies. *Qualitative Health Research, 18*(1), 133–144

Kaul, A., Chavendera, D. D., Saunders, K., & Paphitis, S. A. (2024). Improving Emotional Safety, Coping, and Resilience Among Women Conducting Research on Sexual and Domestic Violence and Abuse. *Journal of Interpersonal Violence, 39*(5-6), 1327-1350. https://doi.org/10.1177/08862605231207617

Lee-Treweek, G., & Linkogle, S. (2000). *Danger in the field: Risk and ethics in social research.* Psychology Press.

Moncur, W. (2013). The emotional wellbeing of researchers: considerations for practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1883-1890). https://dl.acm.org/doi/10.1145/2470654.2466248

Ong, J.C. (2020). "Limits and Luxuries of Slow Research in Times of Radical War: How Should We Represent Perpetrators?" *Journal of Digital War 1*(1): 1-6.

Pearce, K. E. (2020). Unintended consequences of using digital methods in difficult research sites. In B. Foucault Welles & S. Gonzalez-Bailon (Eds.), *The Oxford handbook of networked communication*. (pp. 577-598). Oxford University Press. http://doi.org/10.1093/oxfordhb/9780190460518.013.26

Pollard, A. (2009). Field of screams: difficulty and ethnographic fieldwork. *Anthropology Matters, 11*(2).

Schrag, Z. (2010). *Ethical Imperialism.* Johns Hopkins University Press. https://doi.org/10.1353/book.471.

Toscano, E. (Ed.). (2019). *Researching Far-Right Movements: Ethics, Methodologies, and Qualitative Inquiries*. Routledge. https://doi.org/10.4324/9780429491825

Van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. *Research Ethics, 14*(4), 1-17.

Vaughan, A., Braune, J., Tinsley, M., & Mondon, A. (2024). *The ethics of researching the far right: Critical approaches and reflections*. Manchester University Press.

Voss, G. (2012). 'Treating it as a normal business': Researching the pornography industry. *Sexualities, 15*(3–4), 391–410. https://doi.org/10.1177/1363460712439650

Security

Garfinkel, S. L. 2018. "Privacy and Security Concerns When Social Scientists Work with Administrative and Operational Data." *The Annals of the American Academy of Political and Social Science 675* (1): 83–101. https://doi.org/10.1177/0002716217737267.

Hilhorst, D. J. M., Hodgson, L., Jansen, B., & Mena, R. (2016). Security guidelines for field researchers in complex, remote and hazardous places. International Institute of Social Studies.

Pearson, E., Whittaker, J., Baaken, T., Zeiger, S., Atamuradova, F., & Conway, M. (2023). Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field. Vox-Pol Researcher Security, Safety, and Resilience Project (REASSURE).

Smith, C. H., Ó Cluanaigh, D., Ravi, A.G., & Steudtner, P. (2016). “Holistic Security: A Strategy Manual for Human Rights Defenders.” Tactical Technology Collective.

Support for Scholars

Haney-Caron, Emily; Goldstein, Naomi E.; and DeMatteo, David (2015) "Safe From Subpoena? The Importance of Certificates of Confidentiality to the Viability and Ethics of Research," *Akron Law Review*: Vol. 48 : Iss. 2 , Article 5.

Houlden, S., Hodson, J., Veletsianos, G., Gosse, C., Lowenthal, P., Dousay, T., & Hall, N. C. (2022). Support for scholars coping with online harassment: An ecological framework. *Feminist Media Studies, 22*(5), 1120-1138.

San Roman Pineda, I., Lowe, H., Brown, L. J., & Mannell, J. (2022). Viewpoint: acknowledging trauma in academic research. *Gender, Place & Culture, 30*(8), 1184–1192. https://doi.org/10.1080/0966369X.2022.2159335

References

Amnesty International. (2018). *#toxictwitter: Violence and Abuse Against Women Online* (No. ACT 30/8070/2018). Amnesty International. https://www.amnestyusa.org/wp-content/uploads/2018/03/Toxic-Twitter.pdf

Briant, E. L. (2023a). Hack Attacks: How Cyber Intimidation and Conspiracy Theories Drive the Spiral of 'Secrecy Hacking'. in Steel, J and Petley, J. Routledge Companion To Freedom of Expression and Censorship, London: Routledge.

Briant, E.L. (2023b). Hacking is far more than a security issue. It chills free speech. *Index on Censorship*.

Briant, E. L. (2024). Researching and Conceptualizing the Influence Industry. In: Emma L. Briant & Vian Bakir (Eds.) (2024). The Routledge Handbook of the Influence Industry. London: Routledge. Pp 379-394.

CERN. (2020). Computer Security: Blackmailing Academia: Back to pen and paper? CERN. https://home.cern/news/news/computing/computer-security-blackmailing-academia-back-pen-and-paper

Chess, S., & Shaw, A. (2015). A Conspiracy of Fishes, or, How We Learned to Stop Worrying About #GamerGate and Embrace Hegemonic Masculinity. *Journal of Broadcasting & Electronic Media, 59*(1), 208–220. https://doi.org/10.1080/08838151.2014.999917

Citron, D. K. (2023). How to fix section 230. *Boston University Law Review, 103*(3), 713–761.

Demery, A.-J. C., & Pipkin, M. A. (2020). Safe fieldwork strategies for at-risk individuals, their supervisors and institutions. *Nature Ecology & Evolution, 5*(1), 5–9. https://doi.org/10.1038/s41559-020-01328-5

Doerfler, P., Forte, A., De Cristofaro, E., Stringhini, G., Blackburn, J., & McCoy, D. (2021). "I'm a Professor, which isn't usually a dangerous job": Internet-facilitated Harassment and Its Impact on Researchers. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW2), 341:1-341:32. https://doi.org/10.1145/3476082

European Commission. (2024, December 10). Delegated Regulation on data access provided for in the Digital Services Act [Text]. European Commission - Have Your Say. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en

Eyewitness Media Hub. (2015). “New research details full impact of graphic images on newsrooms – and how to cope.” Eyewitness Media Hub, now hosted by First Draft News. https://firstdraftnews.org/articles/new-research-details-full-impact-of-graphic-images-on-newsrooms-and-how-to-cope-with-it/

Gelashvili, T., & Gagnon, A. (2024). One of the Boys: On Researching the Far Right as a Woman. *Studies in Conflict & Terrorism, 0*(0), 1–22. https://doi.org/10.1080/1057610X.2024.2361953

Gewin, V. (2021). Pandemic burnout is rampant in academia. *Nature, 591* (7850), 489.

Halavais, A. (2019). Overcoming terms of service: a proposal for ethical distributed research. *Information, Communication & Society, 22*(11), 1567–1581. https://doi.org/10.1080/1369118X.2019.1627386

Halpern, M. (2015). Freedom to Bully: How Laws Intended to Free Information are Used to Harass Researchers. Center for Science and Democracy. https://www.ucs.org/resources/freedom-bully

Haney-Caron, E., Goldstein, N. E., and DeMatteo, D. (2015). Safe From Subpoena? The Importance of Certificates of Confidentiality to the Viability and Ethics of Research. *Akron Law Review*: Vol. 48 : Iss. 2 , Article 5.

Hendry, N. H. (2021). Sextortion. In K. Miller & K. Wendt (Eds.), The Fourth Industrial Revolution and Its Impact on Ethics (pp. 315–320). Springer International Publishing. https://doi.org/10.1007/978-3-030-57020-0_23

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change, 163*, 120426. https://doi.org/10.1016/j.techfore.2020.120426

Kittrie, O. F. (2015). *Lawfare: Law as a weapon of war*. Oxford University Press.

Lee, J. J., & Miller, S. E. (2013). A Self-Care Framework for Social Workers: Building a Strong Foundation for Practice. Families in Society, 94(2), 96-103. https://doi.org/10.1606/1044-3894.4289

Logan, T. (2023). Online Stalking Experiences and Harms Among Female Acquaintance Stalking Victims. *Victims & Offenders*, 1–21. https://doi.org/10.1080/15564886.2023.2172503

Logan, T., & Showalter, K. (2023). Work Harassment and Resource Loss Among (Ex)partner Stalking Victims. *Journal of Interpersonal Violence, 38*(1-2), 1060-1087. https://doi.org/10.1177/08862605221086649

Loyle, C. E., & Simoni, A. (2017). Researching under fire: Political science and researcher trauma. *PS: Political Science & Politics, 50*(1), 141–145.

Marwick, A. E. (2023). *The private is political: networked privacy and social media*. Yale University press.

Marwick, A. E., Blackwell, L., & Lo, K. (2016). Best practices for conducting risky research and protecting yourself from online harassment (Data & Society Guide). New York: Data and Society Research Institute. https://datasociety.net/pubs/res/Best_Practices_for_Conducting_Risky_Research-Oct-2016.pdf

Massanari, A. L. (2018). Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the "Alt-Right" Gaze. *Social Media + Society, 4*(2). https://doi.org/10.1177/2056305118768302

Mattheis, A. A., & Kingdon, A. (2021). Does the Institution Have a Plan for That? Researcher Safety and the Ethics of Institutional Responsibility. In A. Lavorgna & T. J. Holt (Eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches* (pp. 457–472). Springer International Publishing. https://doi.org/10.1007/978-3-030-74837-1_23

Molas, B. (2024). Doxing: A Literature Review [ICCT Project Report]. International Centre for Counter-Terrorism. https://icct.nl/sites/default/files/2025-01/Molas_Doxing%20A%20Literature%20Review.pdf.

Moran, R. J., & Asquith, N. L. (2020). Understanding the vicarious trauma and emotional labour of criminological research. *Methodological Innovations, 13*(2). https://doi.org/10.1177/2059799120926085

Murguía Burton, Z.F. & Cao, X.E. (2022). Navigating mental health challenges in graduate school. *Nat Rev Mater 7*, 421–423. https://doi.org/10.1038/s41578-022-00444-x

Newman, E., Simpson, R., & Handschuh, D. (2003). Trauma exposure and post-traumatic stress disorder among photojournalists. *Visual Communication Quarterly, 10*(1), 4–13. https://doi.org/10.1080/15551390309363497

Nicholls, H., Nicholls, M., Tekin, S., Lamb, D., & Billings, J. (2022). The impact of working in academia on researchers' mental health and well-being: A systematic review and qualitative meta-synthesis. *PLOS ONE, 17*(5). https://doi.org/10.1371/journal.pone.0268890

Ortutay, B. (2021). Facebook shuts out NYU academics' research on political ads. *AP News* August 4, 2021.
https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18

Payne, R., Martin, B. A., Tuzovic, S., & Wang, S. (2023). Defining biometrics with privacy and benefits: A research agenda. *Australasian Marketing Journal, 31*(4), 294-302.

Pearson, E., Whittaker, J., Baaken, T., Zeiger, S., Atamuradova, F., & Conway, M. (2023). *Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field*. Vox-Pol Researcher Security, Safety, and Resilience Project (REASSURE).

Rager, K.B. (2005). Compassion Stress and the Qualitative Researcher. *Qualitative Health Research, 15* (3), 423-430. doi:10.1177/1049732304272038

Rager, K. B. (2005). Self-Care and the Qualitative Researcher: When Collecting Data Can Break Your Heart. *Educational Researcher, 34* (4), 23-27. https://doi.org/10.3102/0013189X034004023

Rentschler, C. (2017) Bystander intervention, feminist hashtag activism, and the anti-carceral politics of care. *Feminist Media Studies, 17*(4), 565-584, DOI: 10.1080/14680777.2017.1326556

Schulz, P., Kreft, A.-K., Touquet, H., & Martin, S. (2023). Self-care for gender-based violence researchers – Beyond bubble baths and chocolate pralines. *Qualitative Research, 23*(5), 1461–1480. https://doi.org/10.1177/14687941221087868

Segers, I. B., Gelashvili, T., & Gagnon, A. (2024). Intersectionality and care ethics in researching the far right. *Feminist Media Studies, 24*(5), 1219–1224.
https://doi.org/10.1080/14680777.2023.2280884

Sobieraj, S. (2020). *Credible Threat: Attacks Against Women Online and the Future of Democracy*. Oxford University Press.

Steadman, C. (2023). Remembering and anticipating researcher vulnerability: an autoethnographic tale. *Journal of Marketing Management, 39* (9–10), 807–828.
https://doi.org/10.1080/0267257X.2022.2158905

Sun, H., Yuan, C., Qian, Q., He, S., & Luo, Q. (2022). Digital resilience among individuals in school education settings: a concept analysis based on a scoping review. *Frontiers in psychiatry*, 13, 858515.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online. *Policy & Internet, 11*(1), 84–103. https://doi.org/10.1002/poi3.185

Vaughan, A. (2021, September 15). Problematising Ethics and Individual Responsibility for Researchers Studying the Far Right. *AoIR Selected Papers of Internet Research.* AoIR 2021. https://doi.org/10.5210/spir.v2021i0.12135

Vera-Gray, F. (2017) 'Talk about a Cunt with too Much Idle Time': Trolling Feminist Research." *Feminist Review 115*(1), 61-78.https://doi.org/10.1057/s41305-017-0038-y

Wolf, L. E., Dame, L. A., Patel, M. J., Williams, B. A., Austin, J. A., & Beskow, L. M. (2012). Certificates of Confidentiality: Legal Counsels' Experiences with and Perspectives on Legal Demands for Research Data. *Journal of Empirical Research on Human Research Ethics, 7*(4), 1–9. https://doi.org/10.1525/jer.2012.7.4.1

Acknowledgements

Thank you to our expert reviewers, Adrienne Massanari and Beatrys Rodrigues; the Center for Information, Technology, and Public Life at the University of North Carolina (CITAP) for funding Dafna Kaufman and Jacob Smith's work on this project; and the Center for Information Technology Policy at Princeton University for funding Alice Marwick's work on this project. Editing support was provided by Kiara Childs at the Data & Society Research Institute. Layout and design was done by Felicity Gancedo and Ifeoma Obioha at CITAP; we thank both Data & Society and CITAP for donating this time. Thanks especially to the entire AoIR community for inspiring this work and all the members of the Risky Research Working Group past, present, and future.

Citation

AoIR Risky Research Working Group (2025). *Risky Research: An AoIR Guide to Researcher Protection and Safety.* The Association of Internet Researchers. https://aoir.org/riskyresearchguide/

Creative Commons License