Data&Society

Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment

Authors: Alice E. Marwick, *Data & Society Research Institute*

Lindsay Blackwell, *University of Michigan School of Information*

Katherine Lo, *University of California Irvine, Information and Computer Sciences*

Citation: Marwick, A., Blackwell, L., & Lo, K. (2016). *Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment* (Data & Society Guide). New York: Data & Society Research Institute.

Introduction

Researchers conducting research into sensitive topics may face online harassment, social shaming, or other networked forms of abuse. The potential negative effects are myriad. It may be emotionally taxing for the researcher. More severe forms of harassment may pose physical danger to the researcher and their loved ones. False, misrepresented, or private information propagated by harassers may negatively impact the researcher's reputation and/or career. If the researcher goes to their institution seeking help, their concerns may be ignored, misunderstood or not taken seriously. Ultimately, fear of harassment may have a chilling effect on the type of research that is conducted and the capabilities of individual researchers.

This document is a set of best practices for researchers—especially junior researchers—who wish to engage in research that may make the researcher susceptible to online harassment.

NOTE: This document focuses specifically on best practices for academic researchers. We have provided a number of cybersecurity guides in the resources that have detailed instructions for protecting yourself from online harassment. For example, the Speak Up and Stay Safe project has meticulous directions on how to remove your personal information from online databases. We highly recommend following these recommendations, which are general cybersecurity best practices when dealing with online harassment.

What is online harassment?

Online harassment is the use of networked technologies to threaten, maliciously embarrass, or attack another individual. It includes behaviors that range from merely irritating to life-threatening. Some typical techniques include "doxing," or revealing personal information publicly; "brigading," or when a group of people work together to harass an individual; "revenge porn," or disseminating private photos (real or falsified) without the individual's consent; and "swatting," or reporting a false threat to local police, prompting an emergency response team to the individual's home.

What legal remedies are available?

It is hard to convict someone of online harassment. This is due to a variety of reasons, including jurisdiction (the harasser and harassed may be in different cities, states, or countries); a lack of technical knowledge or resources on the part of local police; use of anonymous and pseudonymous accounts; and (in the United States) First Amendment protections, which make it difficult to regulate online speech. While there are some accounts of people successfully suing or prosecuting online harassment, this is very rare.

What does this have to do with research?

Scholars who research and write about a wide variety of topics are finding that their work has an audience beyond the academy. This public interest can be highly beneficial, but it can also cause problems for individual researchers and their institutions. Work that may not seem controversial within one's discipline can spark public discussion, criticism, or outrage. In the worst case scenario, a scholar may become the target of repeated harassing behavior. This is particularly true for members of marginalized groups, including women, people of color, and LGBT people.

NOTE: The following case studies are fictional, but based on real incidents.

Michael is a postdoc studying African-American experiences of police brutality. An editorial he writes on the topic is published online and receives dozens of racist comments. For weeks afterward, Michael receives death threats on Twitter from pseudonymous accounts. His home address is posted and shared, and his colleagues receive calls demanding that Michael be fired. His advisor tells him to stay off the internet. His university has no experience with targeted harassment and is unable to help him cope with or respond to these threats. Michael calls the local police, who are unhelpful. Afraid and angry, Michael deletes his Twitter account and changes his phone number.

Grace is a graduate student working on a project about healthcare equity for transgender people. Her research is covered by a local newspaper. She receives several threatening emails, which she ignores. A picture of Grace from a university website—easily found online—is Photoshopped onto a pornographic image, which is emailed to her parents, romantic partner, and department chair.

Grace feels humiliated and ashamed. While her department is supportive, she regrets ever having begun her project.

Susan is an assistant professor who publishes a study comparing the supporters of three popular political candidates. She begins receiving online threats from supporters of one candidate, who feel that they were portrayed unfairly in her analysis. A student at her university, who campaigns for this candidate locally, is seen loitering outside her classroom and office on multiple occasions. Shortly after this begins, there is an influx of negative reviews about Susan on teaching evaluation websites, and the volume of online threats directed at Susan increases. She reports the individual student to her school's dean, but the university does not understand how the student's actions may be connected with online harassment and is slow to investigate. Susan is nervous and fears for her and her students' safety.

Why does this document exist?

We believe the academy needs to recognize that researchers conducting sensitive or risky research—particularly research about controversial topics—may be susceptible to online harassment and related threats. We also believe that institutions are responsible for ensuring that their employees, whether graduate students, postdocs, faculty, or staff, enjoy safe and secure working environments—which includes internet and social media use.

Recommendations for Departments and Institutions

For institutional leadership, department chairs, and other administrators:

- Have a proactive communications plan for dealing with online harassment, involving university and department public relations and social media personnel.
- Appoint a point person(s) who is knowledgeable about cybersecurity, social media, and harassment whom researchers or students can rely on for support.
- Educate department and university personnel about these issues.
  - Create a one-sheet guide that can be easily disseminated across campus. Include definitions of online harassment, links and contact information for security, counseling services, IT, and relevant resources.
  - *Example:* Rutgers University guide to offline harassment *(PDF)*
- Harness university resources (e.g., IT, campus police) to protect the researcher: filter email accounts, secure websites, provide additional security (if necessary), etc.
- Do not give out any additional information about the researcher(s) without their explicit consent and communicate suspicious activity to them if requested.

- Investigate the merit of claims or threats and discuss them with the researcher for further context and clarification before acting.
- Acknowledge that online harassment is a real and significant problem, and that it cannot be solved by simply "staying off the internet." (A helpful analogy: if a student were being stalked, would you suggest they never go outside?)
- Recognize the psychological harm that can result from online harassment and make emergency counseling services available, should harassment occur.

Recommendations to Advisors and Senior Faculty

For those with a student in their department who wishes to undertake potentially risky research:

- Have a frank discussion with the student about the possible risks of such research.
- Be aware of available university resources, such as counseling services, campus police, information technology experts, and policies to protect students from harassment and harm, and share them with your student.
- Help the student connect with other researchers doing similar work, using your personal network, relevant mailing lists, professional organizations, etc.
- Support the student if they are harassed; if others in the department are dismissive of their experiences, advocate for their needs and the validity of their work.
- Give the student opportunities to discuss their experiences with you, should they choose.

Recommendations to Supervisors

For those conducting risky research that requires research assistants, postdocs, etc.:

- Consider removing student names from public websites and documents about the project. *NOTE: it is also important that all project participants are recognized for their work. Ask the student what they prefer. Consider restricting student names to published papers.*
- Give students opportunities to participate in other projects. Do not penalize them for choosing not to work on controversial topics.
- Give students opportunities to discuss their experiences with you, should they choose. Let students debrief after any research experience that may be difficult.
- Serve as a point person for all media inquiries and public discussion of your research.

Recommendations to Researchers

Before beginning research:

- Notify your institution that you are engaging in research that may be susceptible to online backlash, and that your advisor, PI, department, university marketing team, etc. may receive negative messages or false information about you.
  - Use our information sheet to educate your institution about online harassment.
  - Talk to campus security about the options available in case you experience harassment.
  - Instruct colleagues and department administrators not to reveal any personal information about you over the phone or via email.
- Explain online harassment to your friends and family, and warn them about the possibility of your research making you vulnerable to online attacks.
  - If you live with a roommate or partner, make sure they are aware that your research activities may make them vulnerable as well, particularly if your home address is compromised.
- Follow the steps in a cybersecurity guide such as the Speak Up and Stay Safe project or Crash Override's interactive guide C.O.A.C.H. to remove personal information (such as your phone number or address) from the internet, protect cloud storage, secure passwords, and so forth.
- Reach out to people doing similar research. Be proactive about building community and having conversations with people who understand your experiences. Invest time and attention into building offline friendships and relationships.
- Take breaks. Switch to less taxing projects. Recharge yourself by enjoying life outside of work.

If you are harassed:

- Recognize that this is a traumatic experience and that counseling or therapy may be appropriate. Prioritize your mental health.
- If you are harassed on social media, turn off mobile notifications. Ask a trusted friend to read your emails, DMs, Twitter mentions, comments, etc. and let you know if they see anything that requires your attention.
- If you are concerned about swatting, call your local police and proactively explain the situation. They may have procedures in place to deal with threats.
- Engage strategically. If people begin to contact you about your work, you may choose not to engage with anyone, or to engage only with select individuals.
- If your experiences become too difficult, give yourself permission to move on to other projects.
- If you are overwhelmed or need help managing harassment, Crash Override and CyberSmile have trained agents who understand online abuse.

Prevention Strategies and Tactics

Anyone can be harassed online, even if they take every possible measure to protect themselves. It is important not to blame or criticize a person who is experiencing harassment, even if you feel that they could have done more to protect their online safety.

Research-Specific

- **Public email aliases***:* Consider creating an email alias on your institutional or professional domain that points to your primary email address. List this alias anytime you must publish your email address online (e.g., on your website or CV).
  - You can also create mail filters so that messages sent to this alias are routed to a designated folder separate from your primary inbox.
  - If you are a frequent target of harassment, consider creating different aliases to publish on particular channels, which may help you track where harassing messages originate.
- **Project email aliases**: For project recruitment messages and consent forms, consider creating a project email alias to allow participants to contact the research team without publicly disclosing the identities of individual researchers.
- **Contact information**: Remove your personal phone number and home address from any public CVs or resumes.
  - When an address is required, list your university's main address. Consider removing your office address from university directories, published syllabi, or course websites.
  - Consider creating a Google voice number that forwards to your personal phone; list this number anytime you must publish your phone number online. This makes it possible to disconnect, if necessary, without compromising your personal phone number.
- **Public talks and videos**: Consider refusing to have talks filmed and broadcast online unless they are password protected.
  - If you are giving a talk with a recorded Q&A, consider making your audience aware of the potential risks.
- **Personal websites:** If you have domains registered under your name, your information may be publicly available (including your full name, mailing address, telephone number and email address) through the domain name registrar or WHOIS database.
  - Look up your domains through whois-search.com. If your information is public, purchase domain privacy services from the company where you registered your domain name.

Basic Cybersecurity Measures

- Google yourself.
  - Be especially aware of whether your physical address and phone number are publicly available online.
  - Search for pseudonyms you currently use or have used in the past (e.g., a Twitter handle), which may be linked to your full name or other information about your identity.
  - Check sites like LinkedIn or Facebook, which may appear in search results for your full name, to see how much of your contact information is publicly available. Tailor the privacy settings of these accounts to only display information you wish to share publicly.
  - Check inactive accounts on websites you used in the past, such as MySpace, Flickr, or LiveJournal, to see if they retain traces of your digital information. Consider deleting posts and accounts with information that would make you uncomfortable if it were made public.
  - Check your account names and email addresses with Have I been pwned? to determine if your account passwords have been compromised in known data breaches. Immediately change account passwords that have been— or that you suspect may have been— compromised.
- Set up two-factor authentication on your primary email account; if this is compromised, an attacker can potentially access many other accounts.
  - While email is the most important, consider setting up two-factor authentication on all platforms that support it, such as Facebook, Twitter, PayPal, and Google. Two Factor Auth has a comprehensive list.
- Secure your passwords.
  - Use a password manager (such as LastPass, DashLane or 1Password) and use a different, strong password for each site.
  - Your Facebook, Apple, and Google passwords should be particularly strong.
  - NEVER share your password, especially over the phone or via email.
- Beware of phishing. There are many ways in which your accounts can be compromised, some of which look "official."
  - Always manually check that the website's URL is correct before you enter your password (paypal.com instead of fakesite-paypal.com).
  - Never open attachments or install software from unknown sources.
- Regularly scan your computer for malicious software (malware), using a program like Malwarebytes.
- Be aware of different online accounts and how they are connected.

- Check whether your username on one site (for example, a dating profile) can be connected to other accounts. Be aware of personal or identifying details that are associated with these accounts.
- Check which apps and sites have permission to access each other.
  - Delete links between Facebook and Twitter. Unlink a Twitter account from Facebook at https://www.facebook.com/twitter/. View applications that have permission to access your Twitter account—and revoke any unwanted access—at https://twitter.com/settings/applications.
  - In general, do NOT use Facebook or Twitter to log into other sites.

A Word About Twitter Blocklists

One way that some users choose to avoid harassment is to use a blocklist. Before using a blocklist, make yourself aware of the pros and cons of this approach.

- Blocklists are often created based on criteria such as who a user follows or what they have retweeted, and often capture users who have never participated in harassing behaviors.
- Blocking a user (or set of users) on Twitter prevents the user from:
  - Following you
  - DMing you
  - Tagging you in a photo
  - Adding you to a list
  - Seeing your tweets, followers, likes, or lists (when logged into Twitter)
  - Viewing your tweets in search (when logged into Twitter)
- Blocking a user (or set of users) on Twitter does NOT prevent the user from:
  - Viewing your profile, including your bio
  - Mentioning you in a tweet (though it *will* prevent you from seeing any tweet that they send)
  - Logging out of Twitter—or logging into another Twitter account—to see your tweets, follow you, etc.
- A Twitter user who is blocked will, if they visit your profile, see that you have blocked them. If a user is harassing you, seeing that you have blocked them could incite further attacks.
- Blocklists may upset users who wish to contact you (depending on your status as a public researcher, non-partisan non-profit, non-advocacy group, activist, etc.).
- Blocklists are preventative, but they cannot prevent online harassment—they simply block a predefined set of users from contacting you (with significant limitations, as outlined above).

Resources for Experiencing & Combating Harassment

Crash Override
Crash Override is a crisis helpline, advocacy group and resource center for people experiencing online abuse. They are a network of experts and survivors who work directly with individuals, tech companies, media, security experts, and law enforcement to educate and provide direct assistance.

A DIY Guide to Feminist Cybersecurity
Excellent, in-depth guide to securing your data online from Safe Hub Boston, an activist group working to make public spaces safer for everyone.

HeartMob
A private platform that provides community support for people experiencing online harassment.

National Network to End Domestic Violence Technology Safety Resources
A collection of resources to help individuals and agencies respond effectively to the many ways in which technology impacts victims of domestic and dating violence, sexual violence and stalking.

The Online SOS Network
A nonprofit that serves and supports people experiencing online harassment. Provides free crisis consultations with mental health professionals, referrals to appropriate resources and services, and contingency funds.

Recommendations for Dealing With Vicarious Trauma from Digital Media
Researchers may undertake projects that involve viewing content that is violent, offensive, or disturbing. Researchers experiencing harassment may also be sent such content. This study includes some "best practices" for dealing with such images and videos.

Violet Blue, **The Smart Girl's Guide to Privacy** (No Starch Press, 2015)
A great short book that covers many of the issues in this document in more depth.

Speak Up and Stay Safe: A Guide to Protecting Yourself from Online Harassment
A fantastic, detailed guide on how to protect yourself online from the creators of Feminist Frequency and Women, Action and the Media.

Without My Consent
Without My Consent is a non-profit organization seeking to combat online invasions of privacy. Their resources are intended to empower individuals to stand up for their privacy rights and inspire meaningful debate about accountability, free speech, and the internet.

Zen and the Art of Making Tech Work For You
A manual for managing online presence and creating safe spaces online, by the Tactical Technology Collective.

Academic Resources on Conducting Risky Research

Many disciplines have a body of literature on how to conduct research that is sensitive, stressful, or psychologically difficult. Depending on your home discipline, these resources may or may not be helpful.

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. Online here

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

Lee, Raymond M. (1993). *Doing research on sensitive topics*. London: Sage.

McCosker, H., Barnard, A., & Gerber, R. (2001). Undertaking Sensitive Research: Issues and Strategies for Meeting the Safety Needs of All Participants. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *2*(1). Online here

Moncur, W. (2013, April). The emotional wellbeing of researchers: considerations for practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1883-1890). ACM. Online here

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

Acknowledgements

This document originated from the MIT Workshop on High Impact Research on Online Harassment and Moderation at the MIT Media Lab, funded by Jigsaw and coordinated by J. Nathan Matias and Camille François. Thank you also to Nicole Ellison, Cliff Lampe, Zara Rahman, Sarah Sobieraj, Jonathan Stray, and TL Taylor for their contributions.

The authors welcome feedback on this document. Please email us at riskyresearch@datasociety.net.