CARR'S ONLINE SECURITY GUIDE

CARR

Centre for
Analysis of the
Radical Right

Authors:
CARR's Associate Director, Dr William Allchorn
CARR's Head of Doctoral Fellows, Bàrbara Molas

Date:
October 2020

Important Note:

This is an EMBARGOED GUIDE designed for CARR Fellows only.

If you wish to distribute outside of CARR, please contact the authors at: socialmedia@radicalrightanalysis.com.

Contents

Introduction

CARR's Online Security Guide brings researchers at the 'coal face' of studying the radical right the practical tools and strategies needed to mitigate and react to potential security threats (such as harassment, intimidation and abuse) that might arise during the course of such research. It takes a threat-modelling approach – starting with the positionality of the researcher, the problem that might have occurred and the counter-strategies that might be employed in reacting to such threats.

The guide is ordered from what could be considered more 'benign' threats (e.g. negative comments and intimidation) through to 'more serious' threats that might impinge on the physical security of a researcher. (There is also a useful branch diagram in Appendix C to help with practical decision-making and a set of tips in Appendix A about accessing security sensitive content.) Such an approach is especially taken to inform Early Career Researchers about the escalating severity of such threats but also to give individuals the ability to target information most relevant to their situation. The core takeaway from this guide is to remain aware, ready and vigilant but also to put in place measures that give researchers sufficient distance from their research subject that they don't become unnecessarily worried, anxious or overwhelmed in their field of research.

Keeping a Check on Harassment

Incident Log

An incident log is a highly helpful device to maintain a record of all aggressions and micro-aggressions by radical-right actors. Try to incorporate each event into your own personal incident log book, along with a screen shot or similar material that might add relevant information to the incident. You can use this information to establish patterns of attacks against you and to assess whether they are escalating. Most importantly, all this gives you confidence when reporting it either to CARR, who can help to offer advice, or to the relevant authorities (e.g. police and internet platforms). It can also serve as a monitor of what does and does not work when reporting such malicious incidents.

Figure 1: Example Incident Log

Incident No.	Date	Time	Description	Evidence	Outcome
#1	3/10/20	10:42	Intimidation via Social Media	Screenshot of incident	Successfully reported to Platform & Police
#2	4/10/20	16:43	Harassment in the street	Mobile Phone Footage	Successfully reported to Police

#3	5/10/20	17:08	Death threats via Email	Screenshot of Incident	Successfully reported to Police

Typology of Threats

Threat 1: Negative Comments

Negative Comments (such as slurs, defamatory comments and name-calling) might come up in the course of maintaining an online presence as a researcher studying the radical right. At its most benign, this might simply involve name-calling and heated discussions online but at the harder end this might also entail racist, misogynistic or abusive comments that will need to be reported – either to the relevant platform or law enforcement. Below is a list of counter-strategies to help you know how to react in these situations:

- **RESPONDING TO ATTACKERS** is not recommended. As American anthropologist from New York University explains, responding to accusations from groups whose ideals are antagonistic to ours may only cause "anger and grief", often triggering further polemic and trauma.
- The dictum of '**DON'T FEED THE TROLLS**' is therefore helpful in this instance. (Unless your research requires you to interact with the radical right, in which case you might wish to have a separate set of social media accounts for fieldwork activity.)
- In any case, think about **BLOCKING OR 'SOFT BLOCKING' SUSPICIOUS ACCOUNTS OR AGGRESSORS** but obviously as a last resort, in case of blowback or further escalation effects.

Threat 2: Intimidation Campaigns

Intimidation campaigns (e.g. sharing of name and/or photos on public forums) might occur where radical-right online communities or networks share your name and/or publicly available photos on public forums. This can be as benign as discussing your research about them (in some cases they laud the attention given by researchers to their tiny organizations!) or a more sinister step down the road of listing you as a potential target for more concerted harassment further down the line. Below is a list of counter-strategies to help you know how to react in these situations

- **CHECK THE SEVERITY OF THE THREAT.** As with the above threat, it is good to keep a check on the severity of such attempts at intimidation and 'go silent' (e.g. erasing profiles, pictures and posts) online when the attention gets too much as well as reporting any signs of concerted harassment to your University, research institution or trusted authorities.
- **CHANGE YOUR PRIVACY SETTINGS.** Make your posts on social media sites private so that only select people can view them, and if public make sure you de-activate geo-tagging and only report on your location after you've left the disclosed location.
- **GET A TARGETED HARASSMENT POLICY ADDED TO YOUR FACULTY HANDBOOK.** As one senior researcher at CARR has suggested, it is

advisable to get a targeted harassment policy added to your faculty handbook so that the administration knows how to react and what processes to follow to safeguard yourself and loved ones.

At this time, it might be also advisable to seek self-care strategies that help you mentally and emotionally. Below are some tips if you are this situation:

- **FIGHT ISOLATION.** Engage with study groups and associations that allow you to connect with scholars and professionals engaged in similar work. Sharing your experiences with them will allow you to find advice both through their websites and social media groups as well as comfort.
- Examples of study groups and associations dedicated to the study of the far right include: Berkeley Centre for Right-Wing Studies, Centre for Research on Extremism (CREX) Oslo, ECPR Standing Group on Extremism & Democracy, Institute for Research on Male Supremacism, International Association for Comparative Fascist Studies (COMFAS), and Researchers of Historical and Neo-Fascism.
- **ADDRESS YOUR EMOTIONS.** Dealing with far-right material might lead you to develop feelings related to anger or frustration. Taking several breaks throughout your working day and engaging in activities that allow you to release such feelings is crucial. A PhD candidate, whose work includes the misogynistic incel movement, explains that she enjoys playing videogames after interacting with particularly difficult material. In such videogames, she can fight the "bad guys" and feel she has accomplished what she ultimately wants: "defeating evil".

  SEEK PSYCHOLOGICAL SUPPORT. Exposure to harassment campaigns and extremist content can have traumatizing effects that stay with you. By talking to a trained counsellor or therapist, you will be able to come to terms with these experiences and have time to heal from them.

Threat 3: Harassment

Harassment (e.g. targeted and sustained forms of malicious messaging) might be at the level of more targeted and sustained forms of malicious messaging and attention by radical-right actors. This might involve frequent abuse and negative comments on social media or forms of paper terrorism (e.g. signing you up to illicit mailing lists and other attempts at defamation). In many ways, you will follow the same actions as above but the frequency of your contact with law enforcement, platforms and your research institution will increase – mainly to shield you from the worse effects of these campaigns and to provide support.

Threat 4: Hacking

Whilst not diminish the above, material threats such as hacking or doxing (e.g. phishing and/or breaking into personal online accounts) represent perhaps a level up from more 'garden variety' intimidation that you see online. This might include phishing and/or breaking into personal online accounts to post malicious information or message, and to further escalate physical security threats again a researcher. In this case, there are a number of preventative and reactive strategies that you can employ to minimize this threat:

- **CHANGE ALL OF YOUR PASSWORDS EVERY SO OFTEN**. Online passwords to your email and other personal sites may be changed once a month to once every three months, depending on how active your research and online presence might be. Visit this website to find out if your email is part of any recent hacks.
- **PHISHING EMAILS.** Hackers might use phishing scams to trick you into disclosing your home address, Social Security/National Insurance numbers or even passwords. Be wary whenever you receive a message that supposedly comes from a bank or credit card company and requests your personal information. Financial institutions will never ask for this information by email or text message.
- **OPT-OUT OF ALL DATA ON BROWSER-BASED SITES** when presented with the choice of accepting cookies.
- **REQUEST ADDRESS REMOVAL FROM PUBLIC SITES/DOCUMENTS.** This will differ according to jurisdiction and site
- **TRY TO 'HACK' OR 'DOX' YOURSELF** through a simple search Engine Search or sites such as Duck-Duck-Go.
- **RUN A GOOGLE REVERSE IMAGE SEARCH OF YOURSELF.** This will throw up images out there of yourself and different versions of that image that are available on the web.
- Also, add **TWO-STAGE VERIFICATION** for all accounts to reduce the likelihood of malicious activity.

Threat 5: Doxing

Doxing (e.g. sharing of home or work address on public forums) might be linked to hacking but comes with its own suit of concerns and issues. If you find your personal details shared publicly by radical right actors, it is recommended that you report this to a platform or law enforcement immediately and log information related to it straight away. Below are some strategies to prevent doxing – either by hacking or through malicious surveillance by a third party:

- **DON'T OVERSHARE** on social media or online forums and message boards. Sharing personal information could easily give those who wish to expose your location and address (i.e. doxers) too much to work with.
- **EXERCISE GOOD 'SOCIAL MEDIA HYGEINE'** by setting up separate research-focused accounts and only checking those during research active periods. As noted further below, this will mitigate the blurring of what is research and what is not – with a separate account affording a firewall between you research and private life.
- **DON'T PROVIDE PERSONAL INFORMATION** when signing up for social media platforms, don't provide personal details, such as your date of birth, hometown, high school, or employer information. This especially goes for fringe or alternative platforms (such as Gab, VK and Telegram) It is worth noting that Telegram does not recognize Internet generated numbers, so the use of a burner phone is advised if this particular platform is to be used. You can also browse VK without an account.
- **FIND OUT WHAT INFORMATION TROLLS CAN FIND OUT ABOUT YOU**. Search for yourself on DuckDuckGo and try doing this search using Google Chrome's incognito mode (or a similar high privacy setting for your browser). This will give you a sense of how much data exists about you online to people who are not in your network. After that initial search, you

can go on to looking at all of the data brokers' sites that trade in our personal lives.

- **NEVER SHARE** certain pieces of information online, such as your Social Security number, home address, driver's license number, and any information regarding bank accounts or credit card numbers. Remember, hackers could intercept email messages, so you shouldn't include private details in yours.

Threat 6: Threats to Personal Security

Though separate from the online space, it is hard to separate offline incidents of harassment and intimidation from escalated online campaigns that might have started them. Again, it is imperative that you report offline incidents or even death threats to law enforcement or your University's security department **immediately** and log information related to it straight away. Below are some strategies to minimize offline harassments incidents:

- **CHECK OUT THE OFFLINE FIELD YOUR GOING INTO FOR POTENTIAL SECURITY RISKS.** As one senior CARR researcher relays, "I just have the habit of giving a call to the organizer and asking for his opinion. If I'm told it is safe, I go. If the answer is like " You can attend but I cannot keep an eye on everybody", I abstain from going. It 's as simple as that."
- **TRY NOT TO GIVE RADICAL RIGHT PROTEST ORGANISERS GROUNDS TO EXPOSE YOUR IDENTITY.** As one senior CARR researcher relays, "I am safe because all the guys on the scene know that I do not take pictures. Never. Most XRW militants are extremely suspicious of any outsider taking pictures and think you might be an informant or an antifa activist. The other side of the coin is that I immediately object if any participant of an XRW event takes a picture of me."
- **COMPLAIN TO ORGANISERS IF YOU ARE HARASSED.** As one senior CARR researcher relays, **"…**if you are ever threatened in real life, do not stay silent. Complain to the organizer. I've had a few shovings with Front national thugs who threatened me and when they see you do not stay still, they usually stop bothering you."

Preventive strategies

Appendix A: WORKING WITH RADICAL-RIGHT CONTENT

Here are some points of advice of working with particularly traumatic or security sensitive materials online:

- **LIMITING THE AMOUNT OF INTERACTION WITH TRAUMATIC IMIGARY** is key to protect our mental health as researchers of the radical right. Visit the following page for practical ways to reduce the impact such material may cause to you: https://dartcenter.org/content/working-with-traumatic-imagery
- **REPORTING THE NATURE OF YOUR RESEARCH TO YOUR UNIVERSITY OR RESEARCH INSTITUTION.** In the UK and other contexts, it is also imperative for your own safety and legal protection that your University is aware of the security-sensitive nature of your research and the content and materials you might be accessing – especially when it is of a terroristic nature. Several Universities in the UK have published guidance on this matter – in line with the 2015 Prevent Duty (University of Surrey, University of Glasgow, University of Durham & City University, London).
- **GAINING PROPER ETHICAL APPROVAL FOR YOUR RESEARCH.** It goes without saying that such reporting is obviously in addition to ethical approval and correct ethical procedures in obtaining, storing and reporting such data. This is to protect yourself in case you need to report illegal or illicit activities, and will vary according to your country-context (i.e. some countries do not have ethics approval boards.)
- **ACCESSING AND STORING SECURITY-SENSITIVE CONTENT** should also been done (where possible) on University equipment with the knowledge of your University's IT Department and stored securely on a University drive. It is also recommended that data is stored on specific devices that are password protected or encrypted e.g. research specific laptops, encrypted memory sticks.
- **INSTALL A VIRTUAL PRIVATE NETWORK (VPN)** on your phone and computer to protect your network access. This helps to privatize your network traffic and bypass filtering happening at your internet service provider. It also makes sure that trolls cannot find you by using your IP address. We recommend Private Internet Access and Vypr VPN, but whatever VPN you use be sure to **always read the privacy policy** to make sure your service does not sell, store, or share your data, and that they will protect it if engaged by the state. If you are in the United States, the government now has permission to collect your browsing data without a warrant. Private Internet Access , in particular, enables you to correspond your location to the pseudonym accounts that you may create to further protect anonymity
- **USE THE TOR BROWSER.** A VPN is great because it can offer privacy, but only the TOR Browser offers a high level of anonymity. Tor is a system for anonymous information exchange via the easily downloadable onion browser which uses onion routing, a form of layered encryption where traffic is processed through at least three nodes, encrypted at each stage so that the sender and destination are unknown. It is important to note that Tor should not be downloaded unless you have activated a VPN first and are using a burner laptop, it is also advised this browser is only used to

access information on the Deep or Dark Web and not for general surface Web browsing).

- **PRACTISING GOOD RESEARCHER 'HYGEINE'** is also essential to keeping separation between your work and private life. By storing and keeping content on a separate drive and set of computer equipment, you reduce the blurring of boundaries and therefore compartmentalize risk. This also minimises the risk of hackers accessing personal files
- **LIMITING THE REPORTING OF TERRORISTIC CONTENT** is vital such that you don't inadvertently publicize the propaganda of certain individuals and groups. Blurring or dialing down the resolution of posters and only using select excerpts of terrorist manifestoes when reporting on a groups activity is key here, as well as thinking about how much the reader needs to know in order to grasp your analysis and argument.
- **LIMIT THE PUBLLISHING OF TRIGGERING CONTENT** is also vital given the racist, misogynistic and homophobic nature of such content.

Appendix B: EXISTING SAFETY GUIDES

Association of Internet Researchers' Internet Research: Ethical Guidelines 3.0.

Internet Research: Ethical Guidelines 3.0
Association of Internet Researchers

Unanimously approved by the AoIR membership October 6, 2019

This work is licensed under a Creative Commons Attribution-NonCommercial-Share Alike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/

aline shakti franzke (University of Duisburg-Essen), Co-Chair
Anja Bechmann (Aarhus University), Co-Chair,
Michael Zimmer (Marquette University), Co-Chair,
Charles M. Ess (University of Oslo), Co-Chair and Editor

The AoIR IRE 3.0 Ethics Working Group, including: David J. Brake, Ane Kathrine Gammelby, Nele Heise, Anne Hove Henriksen, Soraj Hongladarom, Anna Jobin, Katharina Kinder-Kurlanda, Sun Sun Lim, Elisabetta Locatelli, Annette Markham, Paul J. Reilly, Katrin Tiidenberg and Carsten Wilhelm.[1]

Cite as: franzke, aline shakti, Bechmann, Anja, Zimmer, Michael, Ess, Charles and the Association of Internet Researchers (2020). *Internet Research: Ethical Guidelines 3.0.* https://aoir.org/reports/ethics3.pdf

[1] A complete list of the EWG members is provided in **Appendix 7.2**. Contributions from AoIR members are acknowledged in footnotes. Additional acknowledgements follow **4. Concluding Comments.**

Equality Labs' Anti-Doxing Guide

ANTI-DOXING GUIDE FOR ACTIVISTS FACING ATTACKS

Equality Labs Follow
Sep 2, 2017 · 11 min read

We're Equality Labs: a feminist digital security, technology, political organizing startup dedicated to progressive power-building. We provide practical tools for communities to make new interventions in longstanding systems of oppression and advocate for themselves. You can learn more about us by visiting our website.

Marwick, Blackwell, L & Lo's Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment.

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

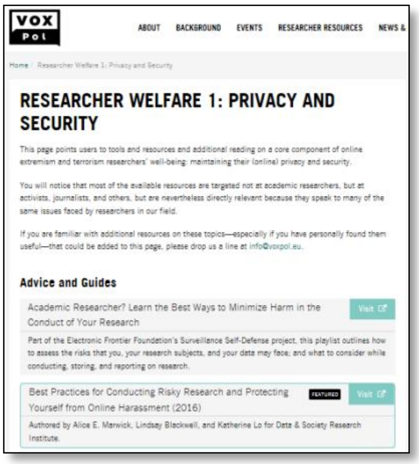
Researchers conducting research into sensitive topics may face online harassment, social shaming, or other networked forms of abuse. The potential negative effects are myriad. It may be emotionally taxing for the researcher. More severe forms of harassment may pose physical danger to the researcher and 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.

RESEARCH INSTITUTE

Vox Pol Privacy & Security Guide



RESEARCHER WELFARE 1: PRIVACY AND SECURITY

This page points users to tools and resources and additional reading on a core component of online extremism and terrorism researchers' well-being: maintaining their (online) privacy and security.

You will notice that most of the available resources are targeted not at academic researchers, but at activists, journalists, and others, but are nevertheless directly relevant because they speak to many of the same issues faced by researchers in our field.

If you are familiar with additional resources on these topics—especially if you have personally found them useful—that could be added to this page, please drop us a line at info@voxpol.eu.

Advice and Guides

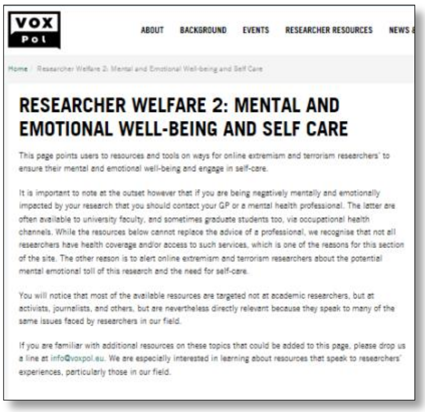
Academic Researcher? Learn the Best Ways to Minimize Harm in the Conduct of Your Research

Part of the Electronic Frontier Foundation's Surveillance Self-Defense project, this playlist outlines how to assess the risks that you, your research subjects, and your data may face; and what to consider while conducting, storing, and reporting on research.

Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment (2016)

Authored by Alice E. Marwick, Lindsay Blackwell, and Katherine Lo for Data & Society Research Institute.

Vox Pol Wellbeing Guide


VOX Pol
ABOUT
BACKGROUND
EVENTS
RESEARCHER RESOURCES
NEWS &
Home / Researcher Welfare 2: Mental and Emotional Well-being and Self Care

RESEARCHER WELFARE 2: MENTAL AND EMOTIONAL WELL-BEING AND SELF CARE

This page points users to resources and tools on ways for online extremism and terrorism researchers' to ensure their mental and emotional well-being and engage in self-care.

It is important to note at the outset however that if you are being negatively mentally and emotionally impacted by your research that you should contact your GP or a mental health professional. The latter are often available to university faculty, and sometimes graduate students too, via occupational health channels. While the resources below cannot replace the advice of a professional, we recognise that not all researchers have health coverage and/or access to such services, which is one of the reasons for this section of the site. The other reason is to alert online extremism and terrorism researchers about the potential mental emotional toll of this research and the need for self-care.

You will notice that most of the available resources are targeted not at academic researchers, but at activists, journalists, and others, but are nevertheless directly relevant because they speak to many of the same issues faced by researchers in our field.

If you are familiar with additional resources on these topics that could be added to this page, please drop us a line at info@voxpol.eu. We are especially interested in learning about resources that speak to researchers' experiences, particularly those in our field.

Winter’s Guide to Researching Jihadist Propaganda: Access, Interpretation, and Trauma.

OVERSIGHT OF SECURITY-SENSITIVE RESEARCH MATERIAL IN UK UNIVERSITIES

GUIDANCE

Universities UK

Appendix C: SECURITY GUIDE TREE DIAGRAM