Communications of the Association for Information Systems

Volume 55 Paper 10

8-6-2024

"Trigger Warning: This Study Contains Extremist Content." Research Strategies for Investigations of Online Extremism and Terrorism

Kevin M. Blasiak
Center for Technology & Society TU Wien, Austria, kevin.blasiak@tuwien.ac.at

Marten Risius
The University of Applied Sciences Neu-Ulm, Germany

Sabine Matook
The University of Queensland, Australia

Recommended Citation
Blasiak, K. M., Risius, M., & Matook, S. (2024). "Trigger Warning: This Study Contains Extremist Content." Research Strategies for Investigations of Online Extremism and Terrorism. Communications of the Association for Information Systems, 55, 257-278. https://doi.org/10.17705/1CAIS.05510

"Trigger Warning: This Study Contains Extremist Content." Research Strategies for Investigations of Online Extremism and Terrorism

Cover Page Footnote

This manuscript underwent peer review. It was received 11/03/2023 and was with the authors for eight months for two revisions. Babak Abedin served as Associate Editor.

Communications of the Association for Information Systems

Tutorial Article DOI: 10.17705/1CAIS.05510 ISSN: 1529-3181

"Trigger Warning: This Study Contains Extremist Content." Research Strategies for Investigations of Online Extremism and Terrorism

Kevin M. Blasiak
Artifact-based Computing and User Research
Center for Technology & Society
TU Wien
Austria
kevin.blasiak@tuwien.ac.at
0000-0002-2753-688X

Marten Risius
Information Management
The University of Applied Sciences Neu-Ulm
Germany
0000-0002-1859-5351

Sabine Matook
Information Systems
UQ Business School
The University of Queensland
Australia
0000-0001-9520-5743

Abstract:

Scholars studying online extremism and terrorism face major challenges, including finding safe access to hostile environments where members evade law enforcement. Protective measures, such as research ethics, often overlook the safety of investigators. Investigators, including Open-Source Intelligence (OSINT) analysts, encounter emotional harm, abuse from ideologues, consent issues, and legal challenges in data collection. Despite rising awareness of these challenges, scholars lack guidance on starting and navigating research in these areas. This paper identifies challenges and offers strategies for safely, ethically, and legally researching in this environment.

Keywords: Online Extremism, IS Research, Researcher Safety, Research Ethics.

This manuscript underwent peer review. It was received 11/03/2023 and was with the authors for eight months for two revisions. Babak Abedin served as Associate Editor.

1 Introduction

Anyone working on issues such as online extremism or terrorism faces a broad range of challenges to personal safety and well-being. This includes academics and researchers from non-governmental organizations, such as Open Source Intelligence (OSINT) analysts, trust safety specialists, and content moderators of different social media platforms (Pearson et al., 2023; Roberts, 2019). To maintain clarity, we will solely focus on challenges related to extremism research while acknowledging that terrorism investigators also confront similar obstacles. The first challenge that investigators face: How do I gain access to the underworld of online extremism? When successful, investigators face additional hazards on how to handle said content now, ranging from mental health issues over legal concerns to death threats and online abuse (Conway, 2021; Pearson et al., 2023). Threats arise from dealing with the content itself (Roberts, 2019), online activists (e.g., trolls) (Seering et al., 2019), or even governments that - threaten to - arrest content moderators (Harbath, 2023). Indeed, as researchers, we also faced legal intimidation tactics (i.e., a strategic lawsuit against public participation (SLAPP)[1]) by an online personality associated with violent extremism because of our published work (anonymous, 2021[2]). However, investigators are often not aware of the challenges associated with investigating online extremism until they are subject to threats, intimidation, or abuse (Pearson et al., 2023).

Investigators have little guidance on how to safely navigate online extremist environments, often leaving them to their own devices (Winter, 2019). Even content moderators who review extremist content on behalf of large social media companies lack, in many cases, adequate training and awareness of the risks associated with extremist content (Roberts, 2019). The current body of literature finds that investigating sensitive subjects, including online extremism, requires substantial guidance for navigating online extremism environments, as well as knowledge to ensure investigator safety (Conway, 2021; Winter, 2019) and ethical and legal advice on data collection (Lakomy, 2023; Winter & Gundur, 2022). While research acknowledges the importance of these issues, the literature offers little support for online extremism research in practice and the navigation of its challenges. Moreover, current guidelines on researching sensitive topics are inept at capturing investigators' particular challenges in online extremist environments (Conway, 2021). Thus, the study's research questions are:

RQ1: What challenges and risks do investigators face when designing and conducting online extremism research?

RQ2: Which strategies can researchers adopt to master the research challenges in this hostile environment safely, ethically, and legally?

To answer these research questions, we blend insights from the online extremism literature with a detailed account of our online extremism research experience. The study's outcome is a set of strategies for the safe, ethical, and legal conduct of designing and conducting quality online extremism research. Thereby, we follow the approach taken in other 'research method papers,' for example, on online focus group research (Schulze et al., 2023), taxonomy development research (Nickerson et al., 2013), and construct measurement and validation procedures (MacKenzie et al., 2011). We present our strategies and insights on online extremism research as a reflective ethnography (Van Maanen, 2011), thus following the example of other IS researchers who offered practical insights from their research conduct (e.g., Schultze (2000)). The highly transparent reporting of our research experiences has pedagogical value for investigators (Burton-Jones et al., 2021), providing them with a first-hand account of how to undertake online extremism research safely, ethically, and legally (Schulze et al., 2023).

We advance IS research, particularly online extremism research, in five ways. First, by reviewing the relevant literature, we offer a comprehensive overview of challenges pertaining to researchers in this field. The proposed strategies allow others to start designing online extremism research, enter online extremist environments, and conduct the work ethically, legally, and safely. Second, we describe an empirical online extremism study in IS and critically reflect on our challenges and lessons learned. These insights allow other investigators to learn from our experiences instead of repeating mistakes made by us and others (Pearson et al., 2023). Third, we synthesize knowledge on the conduct of online extremism research from other disciplines to inform IS research, which increasingly focuses on socially sensitive issues such as

[1] SLAPP's are lawsuits intended to censor, intimidate, and silence critics by burdening them with the cost of a legal defense until they abandon their criticism or opposition

[2] We removed the reference for the review process to ensure authors' anonymity.

online extremism (Spiekermann et al., 2022). Fourth, we discuss the uniqueness of our empirical context (i.e., online extremist environments) and show how our strategies can benefit other research contexts (e.g., critical gender research) (e.g., Adam (2002)); Howcroft and Trauth (2008)). We hope the strategies also provide value for investigators using ethically and legally precarious research methods (i.e., web scraping (Krotov et al., 2020)). Lastly, we offer hands-on guidance for scholars to deepen their research ethics applications to conduct online extremism research ethically, legally, and safely.

2 The Challenges of Researching Online Extremism

Online extremism research is only just emerging in the field of IS (Risius et al., 2023). The augmentation of extremism by digital technologies (i.e., extremists' use of technology) led extremists to use commercial platforms for their malevolent purposes (Fisher et al., 2019). In response, platforms have become active participants in countering extremism influencing platform operations by, for instance, introducing dedicated counter extremism teams that plan for platform continuity (Borelli, 2023).

Due to the absence of established standards for conducting online extremism research, investigators face many challenges when engaging in online extremism research. These range from challenging ethical approval processes to difficulties obtaining data, over legal concerns to investigator and safety issues. This is similar to other high-risk IS research (e.g., cybercrime and darknet research) (Benjamin et al., 2019) since extremism investigators are often limited in their work by the challenges despite the high societal importance of their work. We draw upon existing suggestions from the literature to inform our approach and mitigate associated challenges (Conway & Macdonald, 2023; Pearson et al., 2023; Reynolds, 2012; Winter & Gundur, 2022). Table 1 summarizes the challenges discussed in the literature and faced by investigators conducting research in this domain. We will elaborate on these issues based on the literature and our experiences in conducting extremism research in further detail below.

Table 1. Challenges to Investigators in Online Extremism Research

Challenge	Description	Example from the literature
Ethical approval		
Investigator safety/legality	Standard research ethics processes do not consider the investigator's safety and legal challenges. Investigators are obliged to rigorously follow ethics standards even if they compromise researcher safety and legality (i.e., by disclosing investigators' names to extremists, with no legal support for accessing extremist content).	Conway (2021); Winter and Gundur (2022)
Study feasibility	Standard ethical approval requirements can jeopardize study feasibility because they raise unjustifiable risks to investigators and thus create obstacles to data collection.	Winter and Gundur (2022)
Data collection		
Inability to access extremist data	Access to online extremist environments is obscured and often hidden, requiring investigators to use grey areas or unethical data collection methods (i.e., based on deception, lack of consent).	Conway (2021); Winter (2019)
Investigator safety		
Emotional and mental health risks	The analysis of sensitive content is a cause of mental and emotional harm to investigators. Analyzing graphic, violent, hateful, or deceptive messages puts investigators at risk of harm to their well-being.	Lakomy and Bożek (2023); Pearson et al. (2023); Winter (2019)
Investigators being targeted	Investigators have repeatedly become the target of abusive users who disagree with the research or research findings. This includes abuse such as cyberbullying, doxing, or death threats.	Massanari (2018)
Legal repercussions		
Lawsuits (e.g., libel, defamation, SLAPP)	Investigators can face legal repercussions for their findings, including lawsuits and legal intimidation to prevent the publication of findings.	Pearson et al. (2023)

Legality of data collection	Data scraping or open-source data collection methods involving presumably public online data put investigators in a legal grey area. These methods may infringe on privacy laws. In extreme cases, data collection that includes prohibited content can put investigators on the wrong side of the law.	Krotov et al. (2020); Lakomy (2023); Reynolds (2012)

2.1 Ethics Approval Challenges in Extremism Research

A rigorous ethics process and approval from a university ethics board (i.e., Research Ethics Committees (REC) or Institutional Review Boards (IRBs)) is an essential part of any investigation involving human subjects. Ethical research is a frequent concern when researching virtual communities (Buchanan & Ess, 2009; Cotton, 2004; Hoser & Nitschke, 2010) such as sensitive virtual communities (e.g., communities that may involve illegal activities) (Benjamin et al., 2019) and involving human subjects in research (Davison et al., 2001). However, ethics guidelines by ethics boards often add to the challenge of accessing such online data. To protect research subjects (e.g., by obtaining consent or full disclosure) (Bassett & O'Riordan, 2002; Bruckman, 2002), ethics boards regularly demand precautions that make sensitive data collection (e.g., extremist data) unfeasible (Winter & Gundur, 2022). For instance, in our research, the ethics board initially demanded full disclosure of our names when collecting consent to enable research subjects to engage with us in case of questions or concerns. We found, supported by literature (e.g., Baele et al. (2017)), that applying such generic ethics rules (e.g., obtaining participants' written informed consent, revealing investigators' identity) is often not feasible or even dangerous to implement in extremism research. Indeed, we agree with the literature that generic ethical rules diminish the feasibility of designing and conducting sensitive research because the suggested ethics rules ignore the speed, scope, and access to data online (Winter & Gundur, 2022). Hence, we faced a dilemma between protecting our own personal safety by not disclosing our names and compliance with ethics.

To resolve the dilemma, we initiated several discussions with the ethics board representatives to ensure our research aligns with national ethical standards. The initial requirements (i.e., full researcher disclosure) were cause for concern within our research team. We argued that there is an elevated risk of harm for the involved researchers and requested an exemption to disclosure rules. We found that the ethics board was open to hearing our concerns when we highlighted the potential risks (e.g., doxing, brigading) and were willing to consider alternatives. However, there is a need for ethics boards to gain more awareness of the potential harm to researchers.

2.2 Data Collection Challenges in Extremism Research

An essential first step in designing and conducting online extremism research is accessing online extremism data. The 'access' challenges include the challenge of investigators seeking access to extremist online environments (Fisher et al., 2019) and obtaining access to extremist content in formats that facilitate analysis, such as machine-readable data (Etudo & Yoon, 2023). The obscure and purposely hard-to-access nature of online extremist environments poses a substantial challenge for online extremism investigators. For example, many online communities offer visitors open access and free user registration. As a result, this data is not considered private and, therefore, of low ethical concern (Hoser & Nitschke, 2010; Liu & Chen, 2013). However, more fringe online forums strive for secrecy and intend to be outside the public domain (Flick & Sandvik, 2013; Martin & Christin, 2016). For this purpose, extremists have developed strategies to hide their traces to prevent legal prosecution (Fisher et al., 2019). Because of the 'access' challenge, online extremism research relies primarily on publicly available online data sources, such as social media platforms, websites, forums, or chat groups (Conway, 2021; Scrivens et al., 2020). For instance, Reddit is a popular source of public data from far-right extremists (e.g., Gaudette et al. (2021)). However, extremists are increasingly moving off these platforms into harder-to-reach, smaller chat groups and platforms such as Telegram (Clifford, 2020). Thus, extremist online data may remain unresearched due to a lack of access.

Accessing extreme groups usually requires in-depth familiarization with how and where extremists operate online. These groups are often semi-public or invite-only and, therefore, require a level of deception to access the data when entering forums or invite-only chatgroups and channels (Conway, 2021). In some instances, this can include rigorous vetting processes by moderators of extremist groups or forums in separate vetting channels distinct from the main channel (Figure 1). Vetting processes may demand pictures of hands to verify skin color, shirtless pictures to prove physical strength, detailed survey-style questionnaires on political ideology, and one-on-one chats with moderators.

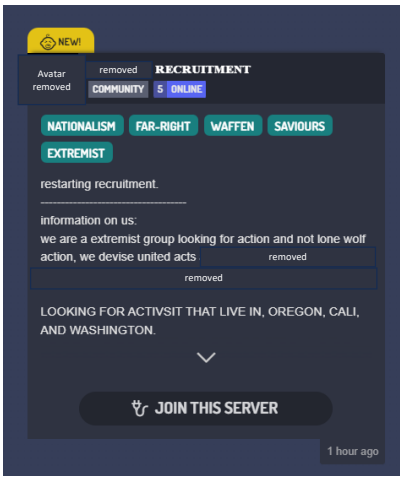


Figure 1. Example of a Public Recruiting Server in Canada, the United Kingdom, Australia, and New Zealand Designated Extremist Group Found on Discord with disboard.org that Leads to Private Chatgroups[3]

2.3 The Potential Harm to Investigators Working with Extremist Material

Exposure to extremist online materials is a vexing challenge in online extremism research (Winter, 2019). Extremist content appears in a variety of forms and includes, among others, graphic depictions of violence, hateful narratives, propaganda, misinformation, or hate speech (Pearson et al., 2023; Winter, 2019). Exposure to this content is common for investigators, which has grave implications for investigators' mental and emotional health and can lead to trauma (Pearson et al., 2023; Winter, 2019). For example, the survey by Lakomy and Bożek (2023) found that extremism investigators experience mental harm from violent extremist content exposure at least once in their careers.

The spectrum of harm caused by extremist content is broad. Extremist propaganda frequently triggers emotional harm, including sadness, anger, and fear (Lakomy & Bożek, 2023; Pearson et al., 2023). Common problems appear regarding concentration, headaches, dreaming related to the analyzed content, and even memory loss, with many of these reactions considered symptoms of trauma or mood disorders (Lakomy & Bożek, 2023; Winter, 2019). In addition, investigators can face intimidation or retaliation by extremists (Massanari, 2018). Initially, we expected these risks to be limited because we did not plan to directly engage with or collect, for instance, potentially harmful extremist content. However, the effects of continuous exposure to online extremist communities had a noticeable mental and emotional effect on the investigators, which was more substantial than expected. For example, while our research did not directly engage with extremist content, we observed chatter, disturbing memes, and glimpses into the individuals' lives, situations, and ideological beliefs. We noticed the pressure that community leaders exerted on other members. This pressure could manifest as either encouragement for daily logins or threats of expulsion for perceived inactivity. Thus, it is important to recognize that no individual piece of particularly disturbing content or interaction solely affects our mental health and emotional well-being. However, the continuous exposure to dark humor, sarcasm, and users' indifference toward human life created a toxic environment.

2.4 Legal Repercussions and Online Abuse

Investigators face various challenges associated with the dissemination of their research findings. These challenges range from online abuse by people or organizations that disagree with the findings to legal challenges that aim to intimidate or prevent scholars from discussing what they found (Massanari, 2018). Doxing is one online abuse and harassment tactic investigators face, which means exposing someone's personal information on the Internet so that others use it for online or offline harassment (Fang et al., 2023). Investigators can also be subject to brigading, a tactic where users work together to target and harass another user. Another harassment tactic is swatting, where adversaries make a fake emergency call to send heavily armed police (e.g., a "SWAT team" in the US) to someone's address (obtained after a doxing incident) (Conway, 2021).

[3] Direct references to or imagery of extremist groups have been removed

The threat of legal repercussions is another tactic to prevent scholars from disseminating their findings. In 2023, we also experienced the threat of legal repercussions after one of our studies appeared in the press (Anonymous, 2023). We received a letter from a senior member of the US Republican party who was legally representing a person also listed on the Southern Poverty Law Centers' list of extremist individuals[4]. Fortunately, our university paid for the expensive legal support, which argued that the research is protected under the United States First Amendment. Unfortunately, the threat of legal repercussions is not uncommon, yet investigators' legal protection often remains limited (Berger, 2019; Pearson et al., 2023). A survey among extremism investigators found that not all institutions recognize online research, such as online extremism research, as a field warranting special protections for investigators (e.g., not requiring full disclosure, providing legal support) (Pearson et al., 2023). Thus, the investigators remain unprotected from attacks by individuals or institutions that intend to intimidate and censor academic discourse.

While researchers may face legal threats from their research subjects, they also encounter significant challenges from the legislative bodies in their country of residence. Engaging in extremist activity (although as an observer) or possessing extremist material (despite it being for research) constitutes serious legal offenses in many countries around the world. Despite having lived in the country where our research was conducted for several years, a lack of familiarity with the legal landscape was a clear obstacle impacting our research. As researchers who grew up overseas, we encountered limitations in understanding what activities might constitute legally prosecutable offenses. This inherent uncertainty posed a considerable challenge throughout the research process, especially as there are many known cases where investigators faced jail time and spent time in detention over possessing research material that was considered illegal in that particular jurisdiction (Reynolds, 2012).

In addition, investigators may face legal repercussions from state actors. For instance, Twitter's former Head of Trust & Safety, Yoel Roth, shares his struggles when assessing whether to flag an Indian state-operated disinformation campaign (which is something Twitter would always disclose per policy) while the Indian government threatened to incarcerate Twitter content moderators situated in India (Harbath, 2023). In a similar case in Brazil, platform employees were incarcerated. Roth argued that governments (or people) may feel they can only control the platforms by targeting their employees. In another notable instance, misinformation researcher Kate Starbird from the University of Washington encountered legal reprisal from political entities in the United States due to her efforts in identifying misinformation on social media (Leingang, 2024). Consequently, some misinformation researchers shifted their research focus or even ended research programs because politicians had constructed a narrative that sought to discredit scientific work in this domain by framing it as acts of censorship (Nix et al., 2023).

Appendix 1 provides a detailed overview of the discussed challenges and our experience.

3 Strategies for Conducting Online Extremism Research in IS

Strategies are plans to overcome particular challenges in specific contexts (Mintzberg, 1987). Based on the literature and our experience, this section presents several strategies to help overcome extremism research challenges. We propose four categories of strategies for others wishing to research online extremist environments. Strategies are categorized by the challenge that they intend to address. The first category of strategies aims to obtain ethics approval for extremism research. The second category aims to address challenges related to data collection and access to online extremist environments. The third category of strategies addresses challenges related to extremism analysis. Finally, the fourth category addresses the reporting of extremism research.

For strategies to be effective, it is essential to consider the specific context in which they were formulated. The extremism research context commonly involves exploring how online extremists use social media platforms for extremist purposes such as propaganda dissemination, recruitment, or radicalization (Anonymous, 2024[5]). This specific type of participant is a hard-to-reach minority population (Wolfowicz et al., 2021) that is unlikely to be sufficiently represented on commercial and academically accepted micro-tasking platforms (e.g., MTurk, Prolific) (Clemmow et al., 2023). Thus, we faced the challenge of contacting extremist participants directly by joining extremist social media platforms and group chat

[4] https://www.splcenter.org/fighting-hate/extremist-files/individual
[5] Reference omitted to maintain anonymity during the peer review process.

environments. Given this research context, we propose strategies for others wishing to conduct online extremism research in IS.

3.1.1 Strategies for Ethical Approval

Use existing extremism guidelines for study design and ethics approval:

Investigators are advised to draw on various resources available to assess the risks and develop a safe study design. The Association of Internet Researchers (AoIR) issued in 2019 its Internet Research - Ethical Guidelines 3.0 to guide informed consent and investigators' safety in digital spaces (Franzke et al., 2020). Without reiterating the detailed guidelines, a notable emphasis is on investigators' safety, which has not been accounted for in traditional ethics guidelines (Conway, 2021). Furthermore, the AoIR guidelines also advise dealing with informed consent online or legally disputed data that can be obtained or crawled as part of online extremism research. This issue is related to the ongoing debate in IS regarding the ethical and legal dilemma of crawling data from online sources in presumably public online spaces without the author's knowledge (Krotov & Johnson, 2023; Krotov et al., 2020).

From our experience, resources such as the AoIR ethical guidelines are great for informed conversations with the ethics boards. They help to highlight the potential risk for investigators and argue for amendments to the ethics rules to protect investigators while respecting subjects' rights to privacy. Ethics boards might need to be made aware of the risks associated with online extremism research, particularly in faculties/schools that typically do less research on sensitive topics (e.g., business schools). For institutions, developing specialized expertise in sensitive research areas (i.e., extremism, misinformation, cybercrime) could be a vital strategic direction to pursue (Winter & Gundur, 2022). Institutions and investigators can build on the AoIR guidelines but also on other well-regarded guidelines about informed consent in online environments and investigators' safety, such as the British Psychological Association's Ethics Guidelines for Internet-mediated Research (2021) (The British Psychological Society, 2021) and the Norwegian National Research Ethics Committee's A Guide to Internet Research (2019) (NESH, 2019). The guidelines from the Data & Society's Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment are particularly well suited to discuss measures to protect investigators from online harassment (Marwick et al., 2016).

A priori assess acceptable risk:

The degree of any investigator's vulnerability depends on the appropriateness and effectiveness of the preparations done before entering the online field (Conway, 2021). Investigators should discuss the acceptable risk of the research with their ethics boards. However, informed reflection by investigators on how far they are willing to go in protecting themselves should predate these discussions. Investigators should note that many novice investigators underestimate the risks and safety concerns before researching online extremism topics (Pearson et al., 2023). Moreover, when intending to work with highly sensible content, discussing the research with appropriate law enforcement might be a risk-mitigating activity worth considering (Reynolds, 2012). In some instances, investigators have come into conflict with the law based on the material collected online for research purposes (Curtis & Hodgson, 2008).

3.1.2 Strategies for Extremism Data Collection and Access to hard-to-reach Online Extremist Environments

Use procedural and technical tactics to prevent or mitigate investigator harm:

Investigators can adopt various tactics during data collection to mitigate privacy and security challenges. The literature distinguishes between technical tactics (e.g., use of online safety technology) and procedural tactics (e.g., processes to avoid revealing one's identity). The tactics are most often self-developed (i.e., "Do-It-Yourself") responses due to the common lack of formal support by institutions and ethics boards (Pearson et al., 2023). Table 2 presents tactics to ensure privacy and security during online extremist data collection.

Table 2. Tactics for (online) Privacy and Security During Data Collection (Based on Pearson et al. (2023))

Tactic	Means
Procedural	Use a specific work-only device (e.g., laptop, PC, mobile telephone) for research.*
Procedural	For accessing messaging services, use a 'burner' or specific work phone that contains no associated contacts so that the number cannot easily be traced back to the investigator.*
Procedural	Avoid conducting research on the same messaging service that researchers also use for their own, private purposes to avoid emotional harm by association.
Procedural	For accessing platforms, use an unaffiliated email address whenever possible or a group email not directly affiliated with any one person.
Procedural	Use a neutral pseudonym and profile picture to avoid raising alarms.
Procedural	Assume an online personality/user for research purposes that is vastly different from one's own (e.g., do not choose a profile picture that you could personally like) to avoid spillover effects into one's private life.
Procedural	Restrict access to data and carefully consider who needs to have access.*
Procedural	Use a combination of a virtual private network (VPN)*, safe operating system (e.g., tails), or browser (e.g., onion browser) to access online entities controlled by extremists.
Technical	Enable 2-factor authentication when possible.
Technical	Store data on work-affiliated cloud space or hard drive.*
Technical	Changed passwords frequently and used a password manager to avoid replication.*
Notes: * Tactics are adapted from Pearson et al. (2023)	

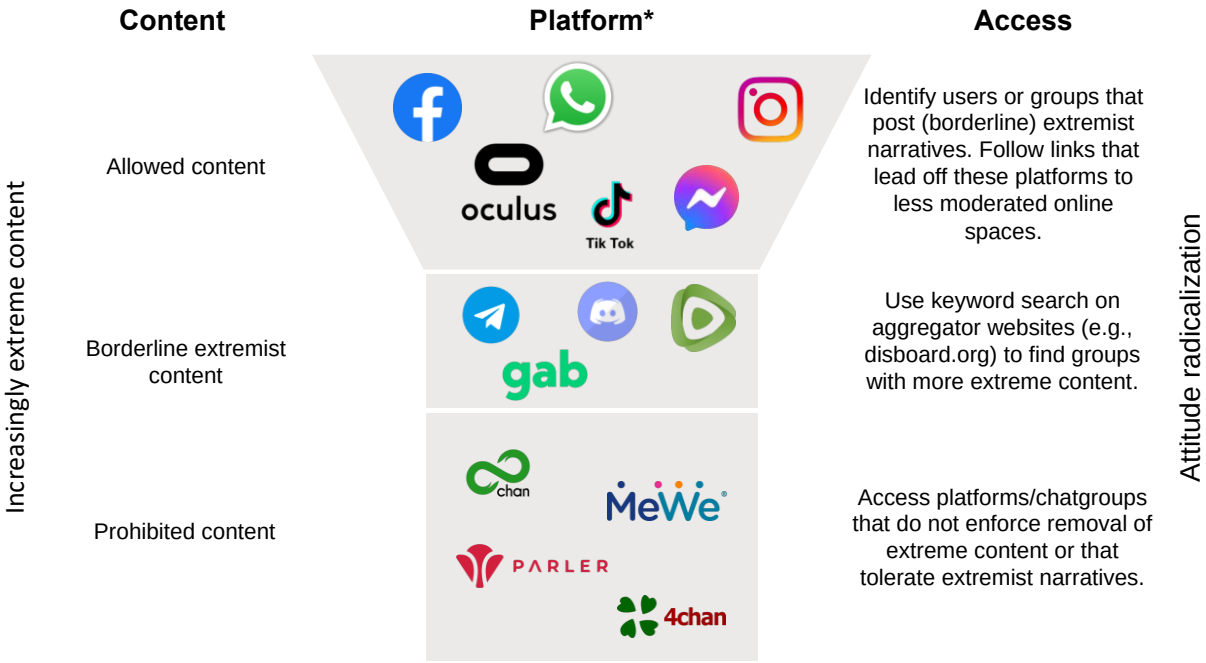
Avoiding the need to access extremist environments for data collection:

Investigators can resort to data collection methods that are significantly less risk-prone (e.g., include only meta-data). Although some risk remains (e.g., a legal grey area, accidental exposure to harmful content), collecting data that requires direct exposure to extremists is significantly riskier. Commonplace is collecting extensive data sets often using (semi-)automated means (e.g., web data scraping, open-source intelligence) of social media postings, user comments, digital trace data, or extremist propaganda materials (Conway, 2021; Krotov et al., 2020; Lakomy, 2023). Much benefit can be derived from exploring extremist communities without interacting with participants, as evidenced by related literature focusing on fraud, terrorism, and other illicit behaviors (Leavitt, 2009; Martin & Christin, 2016). In these alternative data collection methods, the investigators have less exposure to extremist content as much data can be collected safely from a distance (emotional and physical) using these methods (Lakomy, 2023).

Access extremist environments using third-party tools and keyword searches:

Access to extremist environments requires planning. We recommend prior familiarization with how extremist online environments operate. For instance, many extremists seek to radicalize users from mainstream platforms. They use "beacons"[6] to lead users from mainstream platforms onto a more radical platform (Fisher et al., 2019). Figure 2 illustrates how the 'moving-away' path is set up. Familiarization with how extremist environments operate can help investigators identify beacons and, thus, prevent them from entering unprepared into more extreme online environments on often less strictly moderated platforms.

[6] Beacons serve as a constant stream of communication, enabling rapid dissemination of information. Beacons function as the main sources of traffic, essentially acting as 'signposts' directing users to locations where they can access extremist material (Fisher et al., 2019), see also Mapping the jihadist information ecosystem: Towards the next generation of disruption capability (Global Research Network on Terrorism and Technology), retrieved from https://gnet-research.org/wp-content/uploads/2019/12/6.pdf



*Platforms are examples. Popular platforms can in some instances also feature borderline extremist content

Figure 2. Radicalization Funnel: From "beacon" Content on Mainstream Platforms to Extreme Content on Fringe Platforms

Investigators can use third-party tools to identify extremist groups. Extremists increasingly utilize decentralized platforms to avoid detection (Bodo & Trauthig, 2022). Platforms such as Reddit, Discord, or Telegram allow users to create their own platform instances or groups within the main platform. These are, for instance, called Subreddits on Reddit or Servers on Discord. Platforms delegate some responsibility in moderating these spaces. Investigators can use open-source web tools that aggregate public information (e.g., disboard.org for the chat platform discord) to access extreme online environments via simple keyword searches. As shown in Figure 3, investigators find recruitment servers with keywords such as "traditional", "far-right", "nationalism", "nationalist", and "anti-pride".

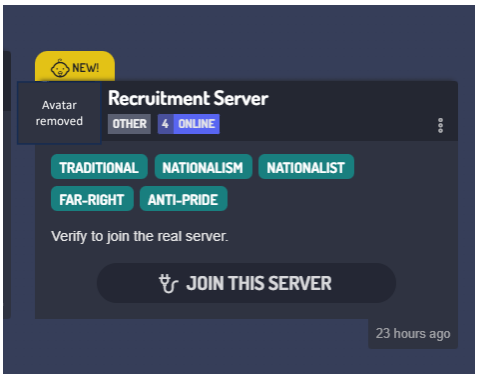


Figure 3. Screenshot from an Extremist Group Recruitment Server with Keywords on disboard.org[7]

Strategies to obtain consent from extremist groups:

When directly accessing these groups for data collection, we suggest obtaining consent. Some platforms might have terms of service that regulate accessing platforms for research. In instances where consent from individual users is impractical, investigators may approach the administrator or moderator of groups. However, investigators should carefully consider the risks when engaging with these groups. We found that some group administrators were open to engaging with research, whereas others have been more

[7] Direct references to or imagery of extremist groups have been removed

hostile. For instance, Reddit moderators within the "Gamergate[8]" community were open to discussing posting a survey invitation after reviewing our experiment and disclosing our university affiliation via a university email address. A group email address affiliated with the university was sufficient to prove our identity as researchers, and we did not need to provide our personal email addresses or names.

3.1.3 Strategies for Analyzing Extremist Data

During data analysis, the goal is to remain emotionally separated from the, at times, harmful content (Pearson et al., 2023; Winter, 2019). The literature proposes various tactics to protect investigators from emotional and mental harm. These tactics can be preventative (e.g., deciding not to collect potentially disturbing data) or mitigating tactics (e.g., increasing the physical distance to the content) to reduce the mental and emotional strain of working with harmful content.

Introduce preventative strategies for investigator's safety:

Extremism research does not necessarily have to involve harmful content or engagement with potentially hostile individuals. Online extremism is a sociotechnical phenomenon that exceeds harmful or violent content (e.g., extremist or terrorist groups delivering humanitarian services) (Risius et al., 2023). Various types of research can be done from a safe distance, for instance, by analyzing metadata (e.g., timestamps, geolocation data) from chat platforms (e.g., Al-Saggaf (2016)). Alternatively, secondary data (e.g., literature) can be drawn on to produce significant insights (e.g., Risius et al. (2023), Aldera et al. (2021)).

Use of mitigation strategies by investigators:

When analyzing extremist content, it is suggested to demarcate "working" and "not working" by limiting exposure to content, for instance, by setting time limits or defining a dedicated physical space from where the extremist environment is accessed (Pearson et al., 2023). Moreover, conscious (regular, time-boxed) breaks from viewing harmful content or engaging in extremist online channels help to prevent harm and keep investigators grounded when handling sensitive materials (Conway, 2021). In addition, the literature reports that some investigators found it helpful not to look at the challenging visual stimuli, as it helped to reduce emotional and mental harm (Lakomy & Bożek, 2023). When viewing emotionally challenging content, compartmentalizing online extremist research as a professional experience separate from the investigator's identity as a private person (Conway, 2021; Lakomy & Bożek, 2023) can help mitigate harm. From our experience, this can be a challenging process due to the toxic nature of the topic, but it can be accomplished through active reinforcement (e.g., mute notification, set reminders).

Investigators working on online extremism can use several mitigating tactics to protect their mental and emotional well-being. Regular meetings with co-workers or colleagues to discuss the impact of their work on cognitive and emotional well-being are helpful. They can contact others through social media or attend relevant conferences when working in isolation. They should also seek professional help, such as counseling, either through their institution or privately. Many investigators in the field found these professional connections with others in similar situations helpful in processing the experience of online extremist research (Pearson et al., 2023). Table 3 provides an overview of how investigators can protect themselves from emotional and mental harm.

Table 3. Protection Tactics of Investigators' Mental and Emotional Well-Being (Based on Pearson et al. (2023))

Tactics	Means
Mitigation	Working during set hours when handling sensitive content (e.g., avoided checking devices in bed, whether in the early morning or late at night; where possible, avoided working outside of 'work hours,' such as in the evenings or at weekends).*
Mitigation	Take breaks from consuming harmful content, including hourly, daily, weekly, or longer, depending on personal needs.*
Mitigation	Worked in a location not used for other purposes (e.g., leisure, sleeping).
Mitigation	Introduce measures that demarcate "working" and "not working" (e.g., changing clothes, switching devices).*

[8] Gamergate has been labeled as a male supremacy online harassment campaign and a right-wing hate group against feminism, diversity, and progressivism in video game culture (https://www.splcenter.org/fighting-hate/extremist-files/ideology/male-supremacy)

Mitigation	Request a workspace in which PC/screen is not easily viewable by others so as not to worry about traumatizing others.*
Mitigation	Minimize screens when viewing extremist content.*
Mitigation	Use a privacy screen to prevent coworkers from seeing the screen
Mitigation	Reduced screen brightness when viewing extremist content.*
Mitigation	Reduced volume when listening to extremist audio/video.*
Mitigation	Watch content on a mobile phone as this has a small screen.*
Mitigation	If working in a team, talk to other team members about their work and its impacts on them.*
Mitigation	If working in isolation, reach out to others working on online extremism, including via social media and/or at relevant conferences and other events.*
Mitigation	Take and reinforce a consciously scientific or analytical approach to content.*
Mitigation	Communicate the specific needs of and risks to online extremism investigators to institutions' press and marketing teams.*
Mitigation	If in a position to do so, promote the inclusion of a budget for investigators' welfare-related services in relevant research planning and proposals.*
Mitigation	Get professional help (e.g., counseling), either via institution or privately. *
Mitigation	Conduct regular self-assessment to reflect on whether the research is causing harm to the investigator
Mitigation	If in a position to do so, promote obligatory or mandatory training to counter the mental and emotional well-being effects of the work
Prevention	Investigators can opt-out from research involving harmful content or exposure to extremist individuals. A conscious choice not to involve harmful data is a legitimate measure to protect oneself.
Note: Tactics marked with an * are adapted from Pearson et al. 2023	

From our experience, significantly limiting exposure to extremist content and online activity was the most helpful strategy. For instance, while observing extremist groups online, we observed changes in our online behavior. We frequently visited the communities and subscribed to "backup" servers on less-regulated platforms such as Telegram. We did this to ensure our connection to the group in case the primary community server on platforms such as Discord faced bans. Accessing these less regulated backup servers on Telegram exposed us to more graphic and disturbing content, resulting in a desensitization effect where content that initially seemed disturbing appeared less so over time. Consequently, we limited our exposure time to the communities to acceptable durations (i.e., about 30 minutes/day for a total duration of 2 weeks), albeit still complying with the community pressure for daily logins (see Figure 4 for an example). In addition, we deactivated any push notifications about activities in extremist chatgroups. This experience is consistent with findings from Pearson et al. (2023), who highlight that extremist investigators underestimate the effects of exposure to extremist (online) environments.

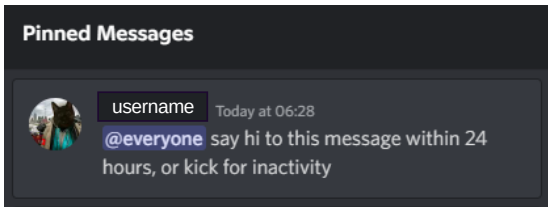


Figure 4. Group Moderators Tracking User Activity

3.1.4 Strategy for Reporting Extremist Research Findings

Investigators face several risks even after completing an online extremism research project. The dissemination and reporting of results are a critical point that can lead to targeted attacks on the investigators (Pearson et al., 2023). The attacks can be verbal abuse, physical threats, or legal challenges. Investigators may be targeted because of their work or public identity, such as ethnicity,

minority, sexual identity, or political activism. Strong ideologically motivated attacks on researchers have ranged from doxing to death threats (Massanari, 2017).

Prevent online abuse:

Online abuse (e.g., hateful comments) was commonplace in a survey among extremism investigators (Pearson et al., 2023). Measures to prevent online abuse should be taken before the start of the project. For instance, investigators should recognize that a public social media presence carries risks. We recommend weighing the costs and benefits of maintaining a social media presence and carefully considering any public information that extremists and other actors could use to launch attacks. Investigators should consider whether they are willing to hide their entire social media presence or use a publishing alias to mitigate challenges, as these could affect their career progression. In a fireside chat at the 2023 Stanford Trust & Safety conference, Yoel Roth warned that if you are working in this space, you should consider yourself already under attack and cautioned to take preventative measures before a personal attack occurs.

Mitigate the risks of legal challenges:

Investigators should clarify legal support from their institution before commencing with the research project. In our experience, legal challenges came unexpectedly and with significant backing from organizations with ties to influential individuals well embedded in politics or society. For instance, it's important to recognize that many extremist individuals or organizations have ties to politically accepted entities. Influential think tanks with specific political leanings, mainstream politicians, or lobbying organizations often serve as mouthpieces for extremist individuals (Stahl, 2023). Therefore, investigators should evaluate their position, especially before publishing results, and if necessary, mitigate risk by, for instance, ensuring appropriate support (e.g., legal representation). At this point, we recognize that legal challenges vary widely across jurisdictions, and in some countries, the likelihood of legal challenges or even state-enforced censorship is more elevated compared to others (George & Youm, 2022).

3.1.5 Summary of Key Challenges and Strategies

We combined our experiences from the field with other investigators who conducted and reported on their experiences. Table 4 summarizes the key challenges and strategies. The strategies provide comprehensive practical suggestions for investigators planning online extremism research.

Table 4. Overview of Strategies and Key Challenges

Challenge addressed	Strategies	Description	Literature
Ethical approval			
Legal challenges, emotional and mental harm to the researcher	Use of existing guidelines in extremism for study design and ethics approval	Use ethics guidelines (e.g., AoIR Guidelines) to inform study design and ethics approval.	Conway (2021); Winter and Gundur (2022)
	A priori assess acceptable risk	Assess the potential risks to researchers and investigators and consider whether a priori measures have been taken.	
Data collection			
Accessing online extremist data	Use of 3rd party aggregator platforms to identify and access extremist groups	Using keywords from reports and the academic literature on online extremism), search for online groups on aggregator websites (i.e., disboard.org for discord) or on the platform itself.	Heslep and Berge (2021)
	Familiarization with extremist online ecosystem	Thorough familiarization with extremist online environments and ideological themes. Be aware of vetting processes and avoid controversy.	Fisher et al. (2019)

Legal challenges and online abuse	Use technical and procedural safety precautions	Consider the use of, for instance, VPN and password managers to prevent harm to investigators.	Pearson et al. (2023)
	Explore safe(r) data collection methods	Some research approaches are significantly safer than others, depending on the investigators' distance from the research subject.	
Investigator safety			
Emotional and mental harm to investigators	Introduce preventative measures for investigators' safety	Various measures can prevent harm from sensitive data. For example, reconsidering the necessity of exposure to extreme content. Exposure can often be reduced to a bare minimum (or no exposure at all) and continuous exposure (e.g., outside a specific research task) might not be necessary at all.	Lakomy and Bozek (2023); Winter (2019)
	Use of mitigation strategies by investigators	Investigators must recognize the effects and risks of the work and introduce measures that minimize them. This includes, for instance, changing screen settings (e.g., size or brightness) when viewing graphic content or strictly limiting the exposure time per day/week.	
Legal repercussion			
Online abuse and legal repercussions	Prevent online abuse	Consider the investigators' vulnerability to abuse (e.g., public social media profiles, publicly accessible information) and consider reducing investigator's online and offline footprint by using intermediaries, aliases, or services that remove online traces.	Massanari (2018)
	Mitigate the risks of legal challenges	Discuss possibilities of legal challenges and defense mechanisms with ethics boards or legal departments before seeking publication.	Reynolds (2012)
		When feasible, avoid using actual names of organizations or persons, replacing them with generic names. In some instances (e.g., when the subject of the study is a particular organization) this might not be practical.	n/a

4 Limitations and Future Research

We also want to discuss the study's limitations related to online extremism research and propose ways in which future research can inform the discussion about rigorous research and investigators' safety.

Our research on online extremism only involved indirect online interactions with human subjects (i.e., extremists). We assume that online extremism investigators, particularly IS scholars, only pursue indirect interactions with extremists and, thus, can regulate many of the challenges. Our proposed strategies might not go far enough when investigators intend to engage with extremists (e.g., conduct interviews). In these cases, investigators must draw on traditional extremism research guides (e.g., Horgan (2012).

We highlight some of the legal challenges investigators face conducting online extremism research. This includes academics, researchers from non-governmental organizations, Open-Source Intelligence (OSINT) analysts, trust and safety specialists, and content moderators on various social media platforms. Many scholars discuss the legal challenges of gathering public social media data (e.g., Krotov et al. (2020); Lakomy (2023)). More research is needed on how to best navigate the legal aspects of extremism data collection and analysis. Investigators need to receive guidance on "when am I working as a researcher and when am I falling on the wrong side of the law?" (Pearson et al., 2023, p. 102) for conducting ethically and legally sound extremist research. Different jurisdictions handle the possession and access to extremist content differently (Reynolds, 2012). Hence, we did not provide generalizable strategies in this regard. Future research is encouraged to support researchers in better understanding their risks (i.e., legal consequences, abusive attacks, consequences of being identified by bad actors) and develop best practices that are tailored to the different legal contexts (e.g., different jurisdictions) or type of data and environments (e.g., extremist content on social media, cybercrime on darknet forums).

Our study provides an overview of the challenges based on our experience and the literature to derive strategies for investigators. However, each challenge warrants a more in-depth consideration to eventually derive rigorously tested best-practice recommendations. We highlight the precarious legal context researchers face (e.g., Reynolds (2012)), data scraping (e.g., Krotov et al. (2020)), emotional stress and trauma (e.g., Winter (2019)), investigators' reflexivity (e.g., Necef (2020)), and difficulties of ethical approval processes. These issues, on their own, are topics worth exploring. For example, research highlights the perspective of the ethics boards, their inherent challenges, and suggestions for structural change (e.g., dedicated or specialized ethics boards) are important future directions that could significantly advance the debate.

5 Conclusion

Online extremism research is a noble endeavor that poses serious challenges to investigators (Conway, 2021; Pearson et al., 2023). We outline the associated challenges and present strategies to reduce their impact. As IS researchers, we focused on research design, ethics approval, data collection, analysis, and dissemination of results of online extremism research in IS. The strategies equip others with practical knowledge on researching online extremism environments. The prospect of an increasing number of online extremism research in IS is exciting. We hope to have contributed to the conversation about this important topic and supported the advancements of online extremism research. Notably, we hope to have motivated others to reflect on questions such as: What is our role as a discipline to influence the ethical practice of working with sensitive data? As a discipline, are we currently equipped to research sensitive sociotechnical issues safely and ethically? The answers and our study contribute to an enhanced use of digital technologies and a better society.

Acknowledgments

Kevin Blasiak's research was supported by an RTP scholarship from the University of Queensland, for which he is deeply grateful.

Marten Risius receives generous funding support from Bavarian State Ministry of Science and the Arts through the Distinguished Professorship Program as part of the Bavarian High-Tech Agenda. He is the recipient of an Australian Research Council Australian Discovery Early Career Award (project number DE220101597) funded by the Australian Government.

Sabine Matook benefited from support from the Australian Research Council (DP210100341).

Declaration of AI

During the revision of this work, the author(s) used ChatGPT to improve the writing for language and grammar.

References

Adam, A. (2002). Exploring the gender question in critical information systems. *Journal of Information Technology*, *17*(2), 59-67.

Al-Saggaf, Y. (2016). Understanding online radicalisation using data science. *International Journal of Cyber Warfare and Terrorism (IJCWT*), *6*(4), 13-27.

Aldera, S., Emam, A., Al-Qurishi, M., Alrubaian, M., & Alothaim, A. (2021). Online extremism detection in textual content: A systematic literature review. *IEEE Access*, *9*, 42384-42396.

Baele, S. J., Lewis, D., Hoeffler, A., Sterck, O. C., & Slingeneyer, T. (2017). The ethics of security research: An ethics framework for contemporary security studies. *International Studies Perspectives*, *19*(2), 105-127.

Bassett, E. H., & O'Riordan, K. (2002). Research ethics in internet-enabled research: Human subjects issues and methodological myopia. *Ethics and Information Technology*, *4*(3), 233-247.

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting darknet identification, collection, evaluation with ethics. *MIS Quarterly*, *43*(1), 1-22.

Berger, J. M. (2019). *Researching violent extremism the state of play*. Researching Violent Extremism Series, Issue. R. Network. https://www.resolvenet.org/research/researching-violent-extremism-state-play

Bodo, L., & Trauthig, I. K. (2022). Emergent technologies and extremists: The DWeb as a new internet reality? *Global Network on Extremism and Technology (GNET), July.* https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf

Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society*, *25*(11), 2877-2897.

Bruckman, A. (2002). Studying the amateur artist: A perspective on disguising data collected in human subjects research on the Internet. *Ethics and Information Technology*, *4*(3), 217-231.

Buchanan, E. A., & Ess, C. M. (2009). Internet research ethics and the institutional review board: Current practices and issues. *ACM Sigcas Computers and Society*, *39*(3), 43-49.

Burton-Jones, A., Boh, W. F., Oborn, E., & Padmanabhan, B. (2021). Editor's comments: Advancing research transparency at MIS Quarterly: A pluralistic approach. *MIS Quarterly*, *45*(2), iii-xviii.

Clemmow, C., van der Vegt, I., Rottweiler, B., Schumann, S., & Gill, P. (2023). Crowdsourcing samples for research on violent extremism: A research note. *Terrorism and Political Violence*, *36*(3), 267–282.

Clifford, B. (2020). *Migration moments: Extremist adoption of text-based instant messaging applications*. GNET Report. https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf

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.

Conway, M., & Macdonald, S. (2023). Introduction to special issue: The practicalities and complexities of (regulating) online terrorist content moderation. *Studies in Conflict & Terrorism*, 1-4.

Cotton, A. H. (2004). Ensnaring webs and nets: Ethical issues in Internet-based research. *Contemporary nurse*, *16*(1-2), 114-123.

Curtis, P., & Hodgson, M. (2008). *Student researching al-Qaida tactics held for six days.* The Guardian. https://www.theguardian.com/education/2008/may/24/highereducation.uk

Davison, R. M., Kock, N., Loch, K. D., & Clarke, R. (2001). Research ethics in information systems: Would a code of practice help? *Communications of the Association for Information Systems*, *7*, 1-40.

Etudo, U., & Yoon, V. Y. (2023). Ontology-based information extraction for labeling radical online content using distant supervision. *Information Systems Research*, *35*(1), 203-225.

Fang, Y., Risius, M., & Cheung, C. (2023). *Understanding the current state of knowledge and future directions of doxing research: A social cognitive theory perspective*. 56th Hawaii International

Conference on System Sciences (HICSS 2023) 56th Hawaii International Conference on System Sciences (HICSS 2023), Hawaii, USA.

Fisher, A., Prucha, N., & Winterbotham, E. (2019). *Mapping the jihadist information ecosystem: Towards the next generation of disruption capability*. Global Research Network on Terrorism and Technology. https://gnet-research.org/wp-content/uploads/2019/12/6.pdf

Flick, C., & Sandvik, R. A. (2013). *Tor and the darknet: Researching the world of hidden services*. Proceedings of the Thirteenth International Conference, the Possibilities of Ethical ICT,

Franzke, A. S., Bechmann, A., Zimmer, M., Ess, C., & Association of Internet Researchers. (2020). *Internet Research: Ethical Guidelines 3.0*. https://aoir.org/reports/ethics3.pdf

Gaudette, T., Scrivens, R., Davies, G., & Frank, R. (2021). Upvoting extremism: Collective identity formation and the extreme right on Reddit. *New Media & Society*, *23*(12), 3491-3508.

George, C., & Youm, K. H. (2022). Media freedom in Asia: Challenges from below. *Asian Journal of Communication*, *32*(3), 194-199.

Harbath, K. (2023). *Yoel Roth on hard tradeoffs, speaking publicly and the future of trust and safety*. Impossible Tradeoffs. https://anchorchange.substack.com/p/yoel-roth-on-hard-tradeoffs-speaking

Heslep, D. G., & Berge, P. (2021). Mapping Discord's darkside: Distributed hate networks on Disboard. *New Media & Society*, 534-555.

Horgan, J. (2012). Interviewing the terrorists: Reflections on fieldwork and implications for psychological research. *Behavioral Sciences of Terrorism and Political Aggression*, *4*(3), 195-211.

Hoser, B., & Nitschke, T. (2010). Questions on ethics for research in the virtually connected world. *Social Networks*, *32*(3), 180-186.

Howcroft, D., & Trauth, E. M. (2008). The implications of a critical agenda in gender and IS research. *Information Systems Journal*, *18*(2), 185-202.

Krotov, V., & Johnson, L. (2023). Big web data: Challenges related to data, technology, legality, and ethics. *Business Horizons*, *66*(4), 481-491.

Krotov, V., Johnson, L., & Silva, L. (2020). Tutorial: Legality and ethics of web scraping. *Communications of the Association for Information Systems*, *47*, 539 – 563.

Lakomy, M. (2023). Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. *Media, War & Conflict*, 1-18.

Lakomy, M., & Bożek, M. (2023). *Understanding the trauma-related effects of terrorist propaganda on researchers*. GNET. https://gnet-research.org/wp-content/uploads/2023/05/GNET-35-Researcher-trauma_web.pdf

Leavitt, N. (2009). Anonymization technology takes a high profile. *Computer*, *42*(11), 15-18.

Leingang, R. (2024). *'Stakes are really high': Misinformation researcher changes tack for 2024 US election.* The Guardian. https://www.theguardian.com/us-news/2024/jan/01/misinformation-trends-2024-election-right-wing

Liu, X., & Chen, H. (2013). *AZDrugMiner: An information extraction system for mining patient-reported adverse drug events in online patient forums*. Smart Health: International Conference, ICSH 2013, Beijing, China, August 3-4, 2013.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293-334.

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, *35*, 84-91.

Marwick, A. E., Blackwell, L., & Lo, K. (2016). Best practices for conducting risky research and protecting yourself from online harassment. *Data & Society*, 1-10.

Massanari, A. (2017). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society*, *19*(3), 329-346.

Massanari, A. (2018). Rethinking research ethics, power, and the risk of visibility in the era of the "Alt-Right" gaze. *Social Media + Society*, *4*(2), 1-9.

Mintzberg, H. (1987). The strategy concept I: Five Ps for strategy. *California Management Review*, *30*(1), 11-24.

Necef, M. Ü. (2020). Research note: Former extremist interviews current extremist: Self-disclosure and emotional engagement in terrorism studies. *Studies in Conflict & Terrorism*, *44*(1), 74-92.

NESH. (2019). *A guide to internet research ethics*. (NESH). https://www.forskningsetikk.no/en/guidelines/social-sciences-and-humanities/a-guide-to-internet-research-ethics/

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336-359.

Nix, N., Zakrzewski, C., & Menn, J. (2023). *Misinformation research is buckling under GOP legal attacks*. The Washington Post. https://www.washingtonpost.com/technology/2023/09/23/online-misinformation-jim-jordan/

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*. VoxPol. https://voxpol.eu/wp-content/uploads/2024/01/Online-Extremism-and-Terrorism-Researchers-Security-Safety-Resilience.pdf

Reynolds, T. (2012). Ethical and legal issues surrounding academic research into online radicalisation: A UK experience. *Critical Studies on Terrorism*, *5*(3), 499-513.

Risius, M., Blasiak, K., Wibisono, S., & Louis, W. (2023). The digital augmentation of extremism: Reviewing and guiding online extremism research from a sociotechnical perspective. *Information Systems Journal*, *34*(3), 931-963.

Roberts, S. T. (2019). *Behind the screen. Content moderation in the shadows of social media*. Yale University Press.

Schultze, U. (2000). A confessional account of an ethnography about knowledge work. *MIS Quarterly*, *24*(1), 3-41.

Schulze, L., Trenz, M., Cai, Z., & Tan, C.-W. (2023). Conducting online focus groups-practical advice for information systems researchers. *Communications of the Association for Information Systems*, *52*, 385-428.

Scrivens, R., Gill, P., & Conway, M. (2020). The role of the internet in facilitating violent extremism and terrorism: Suggestions for progressing research. In *The Palgrave handbook of international cybercrime and cyberdeviance*. Palgrave Macmillan.

Seering, J., Wang, T., Yoon, J., & Kaufman, G. (2019). Moderator engagement and community development in the age of algorithms. *New Media & Society*, *21*(7), 1417-1443.

Spiekermann, S., Krasnova, H., Hinz, O., Baumann, A., Benlian, A., Gimpel, H., Heimbach, I., Köster, A., Maedche, A., Niehaves, B., Risius, M., & Trenz, M. (2022). Values and ethics in information systems. *Business & Information Systems Engineering*, *64*(2), 247-264.

Stahl, L. (2023, 24.03.2024). *Supreme court grapples with online first amendment rights as social media teems with misinformation*. 60 Minutes. https://www.cbsnews.com/news/scotus-grapples-with-online-first-amendment-rights-as-social-media-teems-with-misinformation-60-minutes-transcript/

The British Psychological Society. (2021). *Ethics guidelines for internet mediated research*.

Van Maanen, J. (2011). *Tales of the field: On writing ethnography*. University of Chicago Press.

Winter, C. (2019). *Researching jihadist propaganda: Access, interpretation, and trauma.* Resolve Network: Researching Violent Extremism Series. https://www.resolvenet.org/system/files/2019-09/RSVE_RVESeries_ResearchingJihadistPropaganda_CWinter_May2019.pdf

Winter, C., & Gundur, R. V. (2022). Challenges in gaining ethical approval for sensitive digital social science studies. *International Journal of Social Research Methodology*, 1-16.

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews*, *17*(3), 1-90.

Appendix A:

Table A1. Reporting on Our Online Extremism Research Process

Description	Tactics
Access to online extremist environment	
How did we access online extremist environments?	We used the literature to familiarize ourselves with how extremist online environments operate and then targeted specific platforms to search for extremist pages, groups, or chats: We took all steps outlined with regards to assuring investigator privacy and safety (outlined in this table below) We identified platforms that we were interested in based on the literature (i.e., Reddit, discord) Based on the literature and specialized reports (e.g., Global Network on Extremism and Technology) from which, we developed keywords that would lead us to extremist sources (e.g., nationalism, boogaloo, great replacement) We identified third party websites that track known or banned groups on these platforms, as well as websites that allow to search for groups using keywords (e.g., disboard.org) Using our keywords, we identified several leads to extremist groups
How did we behave in extremist online environments?	We tried to keep a low profile and, to some extent, assimilate to how other users would interact. We used limited means of deception and presented ourselves as someone who might be very early in the radicalization process, mainly driven by curiosity. We created user profiles that were relatively neutral, not tied to an identity, and stayed clear of any behavior that would directly associate us with the extremist online culture and activities (i.e., do not post offensive memes, do not use offensive or hateful language) When approached by other users, we presented ourselves as curious and interested in these chatgroups. Oftentimes disclosing that we do research out of curiosity in the topics was received well in the chatgroups In vetting processes to enter groups, we remained as neutral as possible, hoping to be granted access because of our curiosity about the topic rather than agreement with the extremist themes. We familiarized ourselves with the underlying ideology of the extremist groups (e.g., nationalism, ethnonationalism, anarchism) in order to avoid controversial topics
Ethical approval	
How did we obtain ethical approval for our research?	We employed the standard ethics procedures for research with human subjects but negotiated some amendments: Recruit participants without full disclosure of investigators' identities but point to an unspecified group of investigators at, for instance, the school of business. Create and use a generic university group email alias (socialmedia-research@domain) as a point of contact for participant inquiries while protecting the investigators' identity. Ensure we only include/show safe material to participants (i.e., not breaching laws or platform content policy) by using only material we found on moderated social media platforms. Display the suicide helpline along questions that assessed participants' (vulnerable) emotional state (e.g., loss of significance (Kruglanski et al., 2018), the meaning of life (Jasko et al., 2017)) Provide a debrief on the harms of extremist material with contact numbers to authorities or groups that deal with radicalization.
Legal aspects of data collection	
How were participants recruited and data collected?	Based on our ethical approval and to maintain legality, we selected a recruitment process that is not based on deception (i.e., participants were aware that we were investigators and collected data for a lab experiment). We attracted participants via messages in social media communities that are typically (semi) anonymous (i.e., Discord, Reddit) and that are highly popular among or associated with extremist ideas (e.g., far left/right political discussion groups, gun enthusiasts, public recruitment server of known extremist groups). We identified subjects and groups using keyword searches on public group registries (e.g., disboard.org). We, therefore, implemented the following measures: In moderated groups, approached the moderator of these groups for permission to post participant invitations (the request was declined in most cases). Offer an anonymous way for participants to receive the study incentive (~3 USD). Disclose the purpose and intent of our research without biasing our findings by framing our research as research on social media content usage. Collected (anonymous) consent from all participants and assured that we did not collect identifying data. Offered additional details (i.e., that we conducted an objective study on social media usage with the intent to cover a broad spectrum of different user groups with a focus on non-

	mainstream groups) and were open to discussion on request, which led to some moderators accepting our invitation to participate. Remained ideologically neutral and did not engage in any discussion on extremist topics.
Investigator online safety	
How did we ensure researcher safety online?	We took several measures to protect investigator safety by preserving our identities. We used a VPN[9] to mask our IP address and prevent tracking throughout our data collection. We used exclusively newly created social media accounts, some of which had to be created in advance as some groups required accounts to be older than a particular number of days (e.g., 30 days) All accounts were only linked to anonymized email addresses or burner accounts/phone numbers when possible. When applicable, use the Onion browser (TOR network) or a safe operating system run on a flash drive to avoid spyware or being tracked.[10]
Emotional and mental harms	
What measures did we take to address potential emotional and mental harm?	An inherent consequence of joining extremist online communities was the exposure to extremist materials and, to some extent, partaking in the extremist environment. We took several measures to reduce the ramifications of exposure to extremist environments. Limit the duration of exposure to these environments to a set period of time per day (e.g., 1 hour per day). Disable notifications/emails (e.g., Discord server message notification). Weekly group meetings to discuss the experiences of being in these extremist chatgroups. Credible supervisor assurance that it is okay to stop or interrupt the research whenever necessary.

[9] Virtual Private Network (VPN) adds security and anonymity to users by hiding the user's actual public IP address
[10] Tails (The Amnesic Incognito Live System) is a security-focused operating system aimed at preserving privacy and anonymity by It connecting exclusively through the anonymity network Tor

About the Authors

Kevin M. Blasiak. Kevin M. Blasiak is a Postdoctoral Researcher at TU Wien and the Center for Technology & Society (CTS) in Austria. He received his doctoral degree from the University of Queensland in Brisbane, Australia. Dr. Blasiak's research focuses on addressing online harms, such as online extremism, and developing measures to mitigate these issues. His work is rooted in the field of information systems, with a particular emphasis on responsible computing and platform trust & safety. His research has been published in outlets such as the Information Systems Journal and presented at conferences such as the International Conference on Information Systems and the European Conference on Information Systems. Dr. Blasiak has also contributed reports to the Global Internet Forum to Counter Terrorism (GIFCT). Currently, he leads the responsible computing circle at CTS and is a member of the Stanford Internet Observatory Trust & Safety Teaching Consortium. He has a background in management consulting with companies such as CGI and PwC.

Marten Risius. Marten Risius is Professor for Digital Society and Online Engagement at The University of Applied Sciences Neu-Ulm, Germany. His position receives generous funding support from the Bavarian State Ministry of Science and the Arts through the Distinguished Professorship Program as part of the Bavarian High-Tech Agenda. He is member of the Stanford Internet Observatory Trust & Safety Teaching Consortium. His articles have been published in several journals, such as MIS Quarterly, Strategic Management Journal, Information Systems Journal, Journal of Strategic Information Systems, Journal of Information Technology, MISQ Executive, Business Information Systems Engineering, AIS Transactions on Human Computer Interaction, and Communications of the AIS. He has written reports for the Global Internet Forum to Counter Terrorism (GIFCT) and Global Network on Extremism and Terrorism (GNET). He has been recognized with the Australian Research Council Discovery Early Career Researcher Award, the Early Career Award from the Association of Information Systems, and the German Academic Association for Business Research Young Talent Award.

Sabine Matook. Sabine Matook is a Professor in Information Systems at the UQ Business School, The University of Queensland, Brisbane, Australia. She received her doctoral degree from the Technische Universität Dresden, Germany. Dr. Matook’s research focuses on connecting people with technology safely and seamlessly. Her research on socio-technical connections is embedded in the context of information systems development and social media environments. Her work has appeared in MIS Quarterly, Journal of Management Information Systems, European Journal of Information Systems, Information Systems Journal, Journal of Strategic Information Systems, and others. Dr. Matook is a Senior Fellow of the Higher Education Academy (HEA) and recipient of numerous teaching excellence awards.