In *Terrorism and Political Violence* 2021 special issue on 'Ethics and Terrorism,' 33(2): 367 – 380.

Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines

Maura Conway

Abstract

This article reflects on two core issues of human subjects' research ethics and how they play out for online extremism and terrorism researchers. Medical research ethics, on which social science research ethics are based, centers the protection of research subjects, but what of the protection of researchers? Greater attention to researcher safety, including online security and privacy and mental and emotional wellbeing, is called for herein. Researching hostile or dangerous communities does not, on the other hand, exempt us from our responsibilities to protect our research subjects, which is generally ensured via informed consent. This is complicated in data-intensive research settings, especially with the former type of communities, however. Also grappled with in this article therefore are the pros and cons of waived consent and deception and the allied issue of prevention of harm to subjects in online extremism and terrorism research. The best path forward it is argued—besides talking through the diversity of ethical issues arising in online extremism and terrorism research and committing our thinking and decision-making around them to paper to a much greater extent than we have done to-date—may be development of ethics guidelines tailored to our sub-field.

Introduction

The study of extremism and terrorism raises significant ethical issues in their own rights as, separately, does online research; the combination of these poses particular ethical quandaries. Not having a problem-solving purpose *per se*, this article reflects on two core issues of human subjects' research ethics and how they play out for extremism and terrorism researchers in the Internet age. At the center of medical research ethics, on which social science research ethics are based, is the protection of research subjects from harm. This is appropriate given both the history of egregious violations of persons for purposes of medical research and the inherently risky nature of medical experimentation on humans overall. There is global consensus that the surest way to guarantee the protection of human subjects in medical research is via obtaining their full and free consent to their participation in any such research. In universities, this and other research ethics requirements are overseen by what are generally termed Research Ethics Committees (REC), Institutional Review Boards (IRBs), or similar, which govern not just medical research, but the ethics aspects of all research taking place within their institutions. The protection of research subjects via obtaining informed consent is thus now also a central pillar of social science research ethics as governed by RECs/IRBs.

Explored herein are two of the ways in which these, at first glance eminently reasonable, ethical requirements are complicated when applied in a specific non-medical research setting. The article reflects first on the domination of discussion around protection and harms by the potential for harm to research subjects to, in many cases, the almost total exclusion of potential harms to researchers. Concerns for researcher welfare are an important missing factor in contemporary research ethics governance it is argued herein, which have been gaining greater attention among online extremism and terrorism researchers since approximately 2018, and warrant much closer attention from RECs/IRBs than they have received to-date. Second, if researcher safety is all-but-missing from research ethics discussions, the same cannot be said as regards informed consent and related issues, which dominate contemporary research ethics approval processes. A wide variety of issues complicate the fulfillment of this requirement by online extremism and terrorism researchers, however. Chief amongst these is researchers' desire to engage in incognito data collection for primarily safety, but also other reasons, which raises issues around the ethical permissibility of deception or even just concealment in our sub-field.

Regarding audience, this article is largely targeted at university-based researchers and PhD students. It is not directly addressed therefore at those outside of the academy, though many of the issues raised are certainly germane to, for example, those undertaking the same or similar research in think tanks or other settings. In addition, because the majority of the scholarly research undertaken in this sub-field to-date has been carried out in Western liberal democracies, and it is within these countries that RECs/IRBs are most commonplace, it is the norms obtaining in these countries that this article is concerned with. It is worth noting here too that this article is neither exhaustive nor comprehensive, a raft of additional broadly ethics issues merit attention, including legal and jurisdictional issues (e.g. GDPR, U.K. Terrorism Acts, platforms' Terms of Service), data collection and processing beyond the public-private debate (e.g. around leaked, hacked/stolen, and otherwise "dumped" data; data sharing), and publication and knowledge communication ethics (e.g. circulation of terrorism content by researchers on social media; the influence of universities' impact agendas on online extremism and terrorism researchers' engagements with news media and the ethical implications of these).

The above caveats notwithstanding, this article addresses a series of core and interconnected ethics issues within online extremism and terrorism research, namely researcher safety, informed consent and the closely related matter of harm to subjects, and, stemming from these discussions, the need for ethics guidelines tailored not just to terrorism studies—though these would doubtless be beneficial—but to our specific sub-field. The article is divided into three sections. The first and second sections take up researcher safety in "online field" research and the interrelated issues of informed consent, deception, and protection of research subjects respectively. Section three addresses the pros and cons of the currently available guidelines for engaging in ethically informed online research and advocates for the development of ethics guidelines tailored to our sub-field. In the conclusion, a case is made for committing our ethical thinking and decision-making to paper to a much greater extent than we have done to-date.

Researcher safety in online "field research"

Numerous texts supply guidance to security researchers on *Danger in the Field, Surviving Field Research*, and *Conducting Terrorism Field Research*,[1] but with most of these having little-to-nothing to say about the Internet. For online extremism and terrorism researchers, the Internet *is* the "field," however.[2] Per Barratt and Maddox therefore, "the safety of researchers working in digital spaces needs to be properly considered and safeguarded with the same care as is applied to conventional research engagements."[3] While texts solely concerned with online extremism and terrorism research ethics are still relatively rare,[4] articles and reports that include some reflection on ethics issues in online extremism and terrorism research are increasing in number.[5] A hallmark of this emergent literature is an emphasis on researcher welfare, especially researchers' mental and emotional wellbeing.[6] Many of these analyses mirror discussions that had begun to appear in media at about the same time regarding wellbeing issues among social media companies' content moderator workforce,[7] which may have laid the groundwork for researchers to relate their experiences.

Fortunately for Western scholars, "[t]o date, jihadist extremists have not systematically targeted researchers for potential violence outside of conflict zones. Indeed, groups such as al Qaeda have often sought to benefit from adversary research."[8] But as also pointed out, "[a]s research increases on right-wing movements with a larger and more diffuse presence, researchers may need to be more conscious of potential [physical] threats closer to home."[9] Aside from posing physical dangers to researchers, both jihadist and right-wing extremists have been known to engage in networked forms of abuse, some of which also has the potential to spill over into "real world" settings. Researcher online harassment and other forms of networked abuse can take a variety of forms, including "doxxing" (i.e. posting individuals' private information online oftentimes accompanied by implicit or explicit requests to use it for online and/or "real world" harassment), "brigading" (i.e. a group of users coordinating to "pile on" another user for harassment purposes), and "swatting" (i.e. making a hoax telephone call to emergency services in an attempt to have them dispatch heavily armed police—in the US, a "SWAT team"—to a particular address), which may also be used in combination. In fact, the extreme right has a long history of this type of behavior, having carried out "perhaps the world's first instance of doxxing" in the 1980s,[10] and employing swatting in their much more recent online harassment campaign against women in computer gaming known as "Gamergate."[11] Unfortunately, there is no way when researching online extremism and terrorism, to definitively avoid becoming the subject of such harassment and abuse. This may occur whether in the course of your research you identify yourself as a researcher, or engage in anonymous participant or non-participant online observation and are "outed" by research subjects or others, or arising from publication of your research findings.

While mental and emotional distress arising from exposure to certain types of online content might very well be "softer" than the challenges raised by being directly targeted by extremist and terrorist actors or those adjacent to them, "it is nonetheless far more frequent and should therefore be taken seriously" too.[12] From 2014, IS's online propaganda increased in both volume and goriness, with videos depicting beheadings and other atrocities delivered in a steady high definition content stream for maximum impact. It was arising from repeated and prolonged consumption of this content that some researchers began to reflect on its potential negative effects on them.[13] Winter was the first online terrorism researcher to comment in writing on the potential damage to researchers of a steady diet of hateful and often violent content:

> Jihadist propaganda can be extremely distressing, as its intent is to upset viewers. However, even the most violent materials are in need of consideration by researchers, because they not only help us understand what drives terrorism at an organizational and individual level, but also contain valuable intelligence insights on jihadist activities. The potential harm inflicted upon practitioners working on issues associated with violent extremism—those employed by law enforcement agencies or technology companies—are increasingly well-known. However, there is less awareness of how those same issues are or could be affecting academic researchers psychologically.[14]

Other researchers concurred in their comments to NPR journalist Hannah Allam whose piece on the topic included comments such as "You look at violent imagery all day, and it gets to you. And you want to tell yourself it doesn't, but it does" and "I look at my colleagues and myself, and I see slightly angrier, more cynical people than I saw a year ago or two years ago, and that makes me sad … And I think a lot of that is to do with having to, day in and day out, face up to the worst of humanity."[15]

Very welcome, in this context, is the emphasis in the 2020 iteration of the Association of Internet Researchers' (AoIR) ethics guidelines on "the growing need for ***protecting the researchers***, as well as our subjects and informants" [emphasis in original].[16] Interestingly, the bulk of the paragraph-long section is addressed to extremism and terrorism research, with "Gamergate" referred to and "simply reviewing and curating, e.g., videos of beheadings and other forms of extreme violence" described as potentially having "serious consequences for researchers' psychological health and well-being … "[17] While such acknowledgment in these globally respected guidelines is certainly positive, elsewhere it is pointed out that whereas others professionally tasked in relation to online extremism and terrorism content "benefit from a certain level of welfare," academia is increasingly lagging behind in this respect, with one interviewee observing the following to Mahlouly:

> Researcher welfare is an important thing that I personally spend a lot of time thinking about. I know that other people spending their time looking at propaganda think about [it] as well. Especially in this area, because you have exposure to law enforcement, government and military people, social media corporations … All of us doing kind of the same sort of thing. We are all looking at propaganda a lot. But there is a sliding scale of welfare for these people. So, at the top of that you get social media people that get flexible hours, free yoga (literally free yoga [laugh]) and 24-hour therapy, all that stuff. Then you have law enforcement and they don't have free yoga, but they have flexible hours to a degree, football on Thursdays, that kind of thing … And then academia, where you have nothing.[18]

Agreed upon by virtually all contributors on researcher safety issues in this space is thus the necessity for additional knowledge generation around the issues, dedicated resources to mitigate some of the potential risks and harms, and increased training for all researchers (and decisionmakers, such as REC/IRB members, funders, etc.) active in our sub-field.[19]

Cross-cutting identity-related issues

Unfortunately, certain online extremism and terrorism researchers' identities can cause both the negative security and privacy implications and mental and emotional wellbeing issues associated with their research to be exacerbated. Drawing attention to this is emphatically not for purposes of burdening certain researchers with additional responsibilities on the basis of their identities but highlighting instead, as already widely recognized,[20] that researcher safety issues are not uniform. While nobody is *a priori* exempt, depending on the online extremist or terrorist community they are focused upon, researchers with certain identity markers are more likely to be the targets of online hate and harassment than others.[21] For example, sections of the extreme right evince hatred for various people of color, including particularly black people, Jewish people, Muslims, immigrants, refugees, LGBTQI+ individuals, and women. In general, a researcher that is publicly identifiable as falling into one or more of these categories is likely to prove a more attractive and persistent target for extreme right online harassment than those who do not. In addition, a tactic of online harassers is to communicate false or private information about their targets, which could negatively impact researchers reputations and/or careers, to their employers. While, again, this could be unpleasant for established scholars, it could have profoundly negative consequences for those Massanari describes, in a slightly different context, as "untenured, and/or a member of a marginalized community, and/or facing a precarious professional situation (such as being an adjunct, a graduate student, on the job market, or in a university where their research was not valued)."[22]

Winter makes a number of useful suggestions for how online terrorism researchers may maintain their mental and emotional wellbeing, one of which is that "researchers should try to keep grounded when handling [online terrorist] materials, even if this means actively trying to remain detached from them." He goes on to say that "[w]hile a researcher's empathy is important, so too is their ability to separate themselves from the subject of study; it means they remain analysts and avoid becoming participants."[23] Prolonged and repeated exposure to content that denigrates or otherwise egregiously offends one or more of researchers' core identity characteristics renders detachment effectively out of the hands of some researchers, however; they are always already "participants." Examples of this could include female researchers doing work on incel forums or black, Jewish, LGBTQI+, or Muslim researchers focused on extreme right online activity. Having more than one of these characteristics may also be expected to intensify the negativity of the experience (e.g. exiled Iraqi or Syrian Muslim researchers consuming IS content, black female researchers consuming increasingly racist incel content, etc.). Another upshot of this is that researcher crossover from a focus on one type of online extremism or terrorism, say violent jihadism, to another, say white supremacism, may be experienced vastly differently by the same researcher. On the other hand, for many people who fit into one or more of the discussed identity categories, it is precisely these aspects of their identities that impels them to do this work and "keeps them going." The potential for identity characteristics to compound the negative effects of researching online extremism and terrorism is worth paying attention to nonetheless.

As regards privacy and security, the degree of any particular researcher's vulnerability will depend on the appropriateness and effectiveness of the preparations they have made before entering the "field," including the level of security they have implemented to reduce risks. According to Mertus, "[e]ach researcher should decide for themselves how far they are willing to go in protecting themselves and the threshold of acceptable risk."[24] In fact, what constitute appropriate protections and acceptable risks should ideally be discussed and agreed with experienced and well-informed RECs/IRBs; in the absence of this, careful risk assessment on the part of researchers, based on the nature of the online space(s) they plan on entering, their level of research experience, and similar, is warranted. In terms of researchers' maintenance of their mental and emotional wellbeing, this too varies from person to person. And while identity markers may affect the level and nature of some types of harassment, it does not necessarily determine how it is received. Some researchers' life and/or professional experience may have prepared them for these negative externalities while others have not. Ultimately, it is for each individual to continually evaluate their own positioning, identity, experience, and other factors, ideally in consultation with colleagues, others close to them, and/or relevant professionals—as sometimes individuals have difficulty identifying their own struggles with coping—in order to determine the best course for them at any given time. Finally, it is worth pointing out, in closing this section, that "[i]f your experiences become too difficult, give yourself permission to move on to other projects."[25] Ultimately, we are all of us, as individuals, more important than our research.

Informed consent, deception, and harm to subjects

One of the ways in which online extremism and terrorism researchers seek to protect their safety "in the field" and limit potential harms to themselves from their research subjects is not to request consent, but instead to lurk in extremist and terrorist online spaces for data collection purposes. Concerns about the attitudes of RECs/IRBs to these types of practices prompted Baele and colleagues to layout "An Ethics Framework for Contemporary Security Studies" in 2018 to seek to "prevent the kind of incongruous situations produced by the blind application of generic ethics rules (e.g., obtaining participants' written informed consent, avoiding deception) to research projects in which these commandments appear impossible or even dangerous to implement."[26] This section is divided into four sub-sections that address some of these "generic ethics rules"—"public" versus "private" online data collection, challenges around informed consent requirements in data-intensive online research, the ethical permissibility of deception and concealment, and the "do no harm" principle—and their application to online extremism and terrorism research.

The "public" versus "private" data debate

One of the first questions that often arises in discussions of online data collection is whether the content is "public" or "private." Why? Because this is a way of determining whether it is necessary for researchers to obtain the consent of the data's creators or not.[27] This question is much more difficult to answer than it may first appear, however. It is regularly argued that content posted in wholly open online settings, such as non-passworded discussion forums or unlocked Twitter accounts, is in the public domain and thus comparable to, say, a letter in a newspaper. This is because a letter in a newspaper is viewed as text and not thereby subject to the same ethical considerations as human subjects research. The use of such content by researchers poses minimal risk for the posters, on this view, because—like the newspaper letter writer—they are assumed to have an awareness that their content is public, which is underlined by users' ability to conceal their identities online to varying extents via the employment of pseudonymous screen and/or user names, which many do, and in the case of Twitter, the option to easily make their tweets private, which most do not.[28]

A more nuanced approach to this discussion seeks to dispense with public-private distinctions and determine instead whether the research subjects' are likely to expect that their consent will be requested before their data is collected. But nor is this approach without its challenges:

> Researchers … may not be equipped to determine the expectations for privacy of individuals participating in these forums, and not all individuals will share the same expectation of privacy. The question is then to determine whether researchers should set the bar according to the most open or the most private individual.[29]

Rosenberg makes a useful suggestion in this respect however, pointing researchers to the norms of the online community being studied for guidance.[30] Décary-Hétu and Aldridge explain, for example, that it is routine for users of illegal cryptomarkets, to "explicitly espouse 'crypto-anarchist' and radical libertarian principles," leading Décary-Hétu and Aldridge and other researchers to determine that those particular online communities viewed their content as usable without consent.[31] Some online spaces in which, especially, varieties of the extreme right are active share this libertarian orientation. Having said all this, the only type of extremist and terrorist content that is uncontestably public is that which, like branded extremist and terrorist group propaganda, is produced and circulated online with the express purpose that it be widely disseminated, copied, downloaded, and similar. This segues with Article 9.2(e) of the EU's General Data Protection Regulation (GDPR), one of the bases on which it allows processing of what it terms "special categories of personal data" being that these have been "manifestly made public by the data subject."

Determining the necessity of informed consent in data-intensive online research

Additional issues arise around informed consent in online "big data" research. The first such issue is the practicability of seeking consent from all research subjects in a large to very large to, potentially, massive dataset. This would require not just disproportionate efforts, due to the number of subjects, but the very act itself could, secondly, increase potential harm to subjects. The overwhelming majority of online spaces in which extremists and terrorists are currently active do not have "real name" policies, which means that most posters are pseudonymous but not anonymous. In some spaces, such as 4chan and 8kun however, posts are overwhelmingly anonymous (i.e. the platforms do not allow users to create unique usernames). In either case, potential harms, including firstly invasion of privacy, would stem directly from researchers' efforts to contact individual research subjects for the purposes of acquiring consent. Not all the online spaces in which extremists and terrorists are currently active have administrator and/or moderator roles, but some do, including the latter two spaces. A suggested compromise, in the absence of being able to obtain the informed consent of all users of a particular forum or board, might therefore be for researchers to obtain consent for a data crawl or the use of other data collection methods from the appropriate administrator or moderator.[32] Any online radicalization research based on open sources has the potential to be biased by a requirement that the subjects of such research, including administrators or moderators, be provided with such information however, even absent consideration of the likelihood of such permission being forthcoming. Outreach to research subjects for informed consent purposes in large-scale online research is thus oftentimes not in the interests of either the research subjects or the research.

Deception and concealment

There is a spectrum of revelation possible online, including by online researchers. This ranges from full formal disclosure by researchers of their identities and research purposes on one end to wholesale deception as to one's identity and purposes on the other. The former approach is generally accompanied by the receipt of full informed consent from these researchers' subjects, in the latter case the research subjects generally remain fully in the dark that any research is taking place and, in fact, are often led to believe that the researcher is a fellow traveler of whatever variety (e.g. a right-wing extremist, jihadi, drug dealer, etc.). The work of Barratt and Maddox is an example of the former and Ebner—a non-university-based researcher—of the latter.[33] While online interviews and interview-like interactions in which researchers fully disclose their identities and research purposes to their research subjects are not wholly unknown in extremism and terrorism studies,[34] much more commonplace in our sub-field is the collection of medium to large to very large or even massive—the latter generally using (semi-)automated means—of digital trace data and/or extremist and terrorist propaganda materials, which generally requires a measure of deception. Is this ethically permissible? There are, very broadly, two schools of thought on the ethical permissibility of deception in online research: one that takes a benign view when researching hostile or dangerous communities and another that views it as largely impermissible regardless of the nature of the online communities being researched.

Safety is the chief reason that deception is generally employed by online extremism and terrorism researchers. The most common way in which this occurs is researchers concealing their identities in online spaces via the use of a pseudonym, oftentimes a *Kunya* in online jihadi circles, and sometimes also the use of a profile picture communicating familiarity with whatever ideology dominates in the community they are researching. This is more ethically defensible than it may first appear as the use of "real names" is uncommon in these spaces, so a pseudonym is expected and it is usually possible to employ both a relatively neutral pseudonym and profile picture without raising alarms. A *kunya*, for example, is an honorific utilized in the Arab world, which is composed of either the term *abu* (i.e. father) or *umm* (i.e. mother) plus commonly the name of the user's eldest son or sometimes daughter (e.g. Umm Layth) and/or place of origin (e.g. Abu Talha al-Almani). In terms of profile pictures, it is increasingly common for these to be mundane in order to avoid the attention of content moderators. Ebner gives the example of a female Indonesian IS supporter: "I told my fellow

Indonesian IS supporters to change or delete their IS profile pics and change their account names to something funny."[35]

A requirement of gaining ethical approval for research utilizing such concealment practices however, is commonly a commitment to non-engagement with research subjects; that is permission to "lurk" only. As far back as 2015, Décary-Hétu and Aldridge discussed Russian-language online hacker communities requiring potential members to prove their Russian origin by answering questions that only those deeply familiar with Russia could be expected to know.[36] Display of knowledge of the Koran and Sunnah has also been requested for purposes of admittance to some jihadi online spaces, while Ebner too discusses an instance in which users on a neo-Nazi online forum were requested to "send a hand or wrist photograph with a piece of paper reading MAtR—your username—timestamp" to verify their whiteness.[37] The ethical permissibility of these types of engagements are more difficult to construe than concealment—or even low-level deception?—and warrant further discussion and debate.

While it is possible to present in a gender-neutral fashion online, gender-switching (i.e. deceiving other users as to whether one is male or female) is easy and thus commonplace, including amongst online extremists and terrorists.[38] But what of its ethicality amongst researchers? In a previous article on the role of the internet in extremism and terrorism, I wrote that:

> … in the past jihadi online forums were often segregated on the basis of gender. Anecdotal evidence collected by the author suggests that female researchers accessing extremist forums of various sorts are wont to adopt male personae, including screen names and avatar images, in those settings, but that male researchers retain male identities in the same circumstances. This is a potentially interesting phenomenon facilitated by the Internet that could mean that female users are more influential in extremist cyberspaces than previously thought. (Switching in the other direction is a possibility too, of course, and also has the potential for interesting findings).[39]

This points implicitly or explicitly to at least three reasons for online gender switching amongst extremism and terrorism researchers, the first is safety, the second is access, and the third is for research into online gender dynamics. As regards safety, many female researchers represent themselves as male in not just jihadi but also extreme right online spaces in order to avoid the gendered harassment common in both types of online locales, but that is especially severe in extreme right online settings. Second, regarding access to especially jihadi online spaces, many of the channels, groups, and chats in messaging and other services currently in use by IS supporters and others are gender segregated, with many more spaces accessible to users representing as males than females. Female-only extreme right online spaces, although much less numerous, are also inaccessible to researchers representing as male. Third, empirical research into the similarities and differences in the experiences of users representing as male versus those representing as female in extremist and terrorist cyberspaces may also require deception in this regard (e.g. an individual PhD student carrying out an online ethnographic study of the experiences of male versus female users).

Alternatively, Barratt and Maddox provide strong reasons supporting their commitment to conducting active participatory digital research, including:

> … that active engagement through digital ethnography with hidden populations online forms an integral complement to digital trace analyses, for both methodological and ethical reasons. Active engagement adds richness, context and an opportunity for deliberate research participation by members of the community of interest, with which we can better interpret the findings of studies based solely on the analyses of their digital traces.[40]

While empowerment of extremists and terrorists may strike us as generally unwarranted, richer and more accurate analyses would certainly be welcome and could, eventually, be expected to feed into the development of more effective responses to online extremism and terrorism. As opposed to deception, Barratt and Maddox's research, and other similar studies,[41] illustrate that full disclosure by researchers as regards who they are and what they want is possible even in hostile online spaces. Full disclosure may moreover ensure a degree of legal protection in the event of a researcher's online activity falling within the ambit of the authorities.[42] It's worth pointing out too that the widespread use of fake accounts is likely to skew metrics, especially in smaller or newer forums, channels, chats, and the like (i.e. giving the impression to other researchers, law enforcement, or journalists that a channel or group has a greater following than it does), which may in itself be considered an ethical—in addition to a methodological—issue.[43] Thus "the decision to use fake identities for safety reasons needs to be carefully justified and weighted against the epistemic value of the research," say Eppert *et al*.[44]

"Do no harm": Parsing harm to subjects in online extremism and terrorism research

Easily the most commonly acknowledged issue in the literature on the ethical dimensions of "real world" conflict and security field research is potential harm to research subjects. Neither the impracticability nor inadvisability of seeking consent for much online extremism and terrorism research nor the researchers' role as a non-participant observer in extremist and terrorist online spaces removes researcher's ethical responsibilities to their research subjects and, some might say, increases them. For the avoidance of doubt, requirements to avoid harm to research subjects do not, in most jurisdictions, extend to information obtained about past or present illegal activity. In many EU member states, for example, it is a criminal offense not to report planned crimes, which includes terrorist attack plotting.

The identification of individual users as extremists (or even terrorists) or as being popular, or even influential among extremists, or otherwise online extremist-adjacent raises significant ethical issues, which are alluded to by numerous authors, but most comprehensively treated by Berger.[45] Such identification is almost never necessary, but when might it be useful and ethically allowable? The two main reasons forwarded by Berger for identifying users are the:

> obvious value for replication of social media studies and more broadly for a public understanding of the drivers of extremism—the individuals who are influential or popular within an extremist network shed light on many aspects of a movement, including its key issues and important leaders.[46]

The potential harms to those so identified can be significant, however. Media coverage of online extremism and terrorism research, which is increasingly prevalent, "may be sensationalized or politicized, omitting nuance or misrepresenting facts."[47] A related problem is when analyses and subsequently media identify users as extremists, including just via online pseudonyms, who are not public figures and who may, as a result face serious harms (e.g. unemployment, loss of social media access).[48] Of course, some users relish being identified as it raises their profile within the extremist movement and more widely; Berger referred to this in his alt-right Twitter census: " … after a past study of white nationalist activity on Twitter by the author, users identified as being influential subsequently exploited their rankings for self-promotion."[49] The way to avoid all of this is simply not to publish usernames or any personally identifying information. Is this always and without exception the best route to take however, or are there instances in which it might be ethically permissible to publish such details?

There is a general feeling that public figures should be open to identification and scrutiny. So, Berger explains, for example, that as regards identifying users in his alt-right Twitter census:

> One exception was made, based on the fact that the user's connection to the alt-right is extremely public and uncontroversial, and whose ranking is unsurprising. The most influential user in the dataset was @richardbspencer, the Twitter account of Richard Spencer, founder of the now-defunct website, alternativeright.com, which gave the alt-right its name. Spencer is the primary public face of the alt-right movement … .[50]

In fact, the term "public figure" is usually used in the context of legal actions for libel and defamation to refer to persons known to the general public, such as politicians, actors, or sportspeople. Outside of "famous" people, publicness can be quite difficult to empirically discern however, especially on the Internet. We are probably all agreed that a Twitter user with 10 followers is not a public figure, but how about 10,000 followers? Or is publicness only reached with 10 million followers? What is the appropriate rubric, in other words, or can such even be determined, and is this instead a decision best taken on a case-by-case basis? Might it not be the case that a "real life" public figure only has, for whatever reason, 10 Twitter followers; must that account then be anonymised? If this matter is truly context-dependent, which it may very well be, an important factor to keep in mind for extremism and terrorism researchers is avoidance of harm to research subjects to the extent possible.

A research cohort that scholars are held to owe an increased level of responsibility to are children and minors (i.e. individuals below the age of legal responsibility). Some researchers oppose identification in research of any Internet users who have not given their explicit consent, except public figures already known to us in "real life," due to the possibility that any other users may be minors. This is not an outlandish concern even in online extremism and terrorism research. In July 2020, Feuerkrieg Division (FKD) became the sixth extreme right group to be banned in the UK. The now-dissolved heavily online group was allegedly established by a 13-year-old Estonian boy and had other teenage adherents too.[51] Even younger children featured prominently in IS propaganda materials,[52] which showed some of them carrying out atrocities that they had no capacity to consent to. While visual ethics remains a considerably underdeveloped area,[53] researchers should be mindful of sharing unblurred pictures of so-called "cubs of the Caliphate," which may contribute to their re-victimization. Nor, I would submit, is the already wide circulation of these unblurred images online and in mass media an ethically defensible reason for their continued circulation.

Where do we go from here? The need for tailored guidelines

No code of ethics for terrorism research has yet been developed, despite calls for same dating back over at least a decade, and probably much longer.[54] There are however, a number of useful guidelines and codes of practice for undertaking ethically informed Internet research. The most well-known and widely relied upon documents are the aforementioned AoIR ethics guidelines, the third and most recent version of which, "Ethical Decision-making and Internet Research," appeared in 2019, but which should be consulted in conjunction with their first (2002) and second (2012) iterations.[55] Other well-regarded guidelines, and both now appearing in their second editions, are the British Psychological Association's *Ethics Guidelines for Internet-mediated Research* (2017) and the Norwegian National Research Ethics Committee's *A Guide to Internet Research* (2019).[56] Also worth mentioning, given the focus herein on both researcher safety and tailored advice, is Data & Society's *Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment*.[57]

A problem, such as it is, with generalized internet research ethics codes is that they are difficult to devise due to, among other things, the very fast changing nature of the online ecosystem they are developed to "govern" and the wide variety of types of research they are expected to cover, even when they are discipline-specific. This requires, in effect, that Internet research ethics guidelines focus on core ethical commitments—what AoIR refers to as "a basic ethical approach"[58]—while leaving enough room to account for new types of online spaces, data collection and other tools and methods, research topics, and so on. This, unsurprisingly, has both positives and negatives. Some scholars view the open-ended nature of various guidelines as vital given "a research and ethical landscape that continues to change and transform, often in dramatic ways, over a very short period of time"[59] (e.g. Facebook's pivot to private groups; extremist and terrorists forced migration from social media platforms to messaging applications). Nor does this type of "researcher-led, case-by-case approach"[60] make "*a priori* judgements whether some research per se is unethical"[61] and can be viewed as an opportunity for scholars to develop context-specific ethics practices and inform RECs/IRBs as to the appropriateness of these in scholars' particular (sub-)disciplinary context. Such non-prescriptive approaches are viewed as "less than adequate" by other researchers however.[62] This is due to the adoption in many available guidelines of a bottom-up rather than a top-down approach, which entails acknowledgment of "the messiness and complexity" of Internet research, description and discussion of the ethical issues thereby arising, and suggested ethical questions for researchers to ask themselves, but little to no instruction as to "how to act."[63] This caused many of the UK-based researchers, from a variety of disciplines, interviewed by Samuel, Derrick, and van Leeuwen to view such guidelines as "vague and unhelpful" and thereby placing too great a burden for ethical decision-making on individual researchers.[64]

Ultimately, Samuel, Derrick, and van Leeuwen's interviewees advocated for a discipline or analysis-specific approach to Internet research ethics as "a better way to ensure that, rather than having all-encompassing guidelines useful to no-one … having more, but more specific guidelines useful to everyone."[65] I too am inclined to favor the development and deployment of sub-discipline and analysis-specific guidelines. Marwick, Blackwell, and Lo's best practice document for conducting research likely to attract online harassment illustrates the utility of narrowly tailored advice albeit on a topic, researcher online safety, that is much less divisive than some others. How are we to arrive at guidelines that grapple with more contested issues? The best avenue is probably via the process-based bottom-up approach advocated by AoIR, which is:

> … first of all reflective and dialogical as it begins with reflection on [one's] own research practices and associated risks and is continuously discussed against the accumulated experience and ethical reflections of researchers in the field and existing studies carried out. This further means an emphasis on the fine-grained contexts and distinctive details of each specific ethical challenges [sic] [italics in original].[66]

There is no fast or easy way to arrive at even a basic agreed level of prescription, in other words. Ultimately, "the best we can do is develop 'guidelines, not recipes' … the issues raised by Internet research are *ethical* problems precisely because they evoke more than one ethically defensible response to a specific dilemma or problem. *Ambiguity, uncertainty, and disagreement are inevitable*" (emphasis in the original).[67] While some of the more obvious ethics issues pertaining to online extremism and terrorism research are treated herein, ongoing and systematic identification of and intensive discussion around the whole range of ethical ambiguities, uncertainties, and disagreements arising in our particular sub-field are, I submit, vital next steps if we're eventually to develop tailored guidelines that respect RECs/IRBs functions and criteria, but shaped to more closely correspond to and improve online extremism and terrorism scholars' research practice, which should, in turn, result in more thorough and considered REC/IRB evaluations and decisions.[68]

Conclusion(s)

There are myriad ethical issues facing extremism and terrorism researchers who undertake online "field work." Two of the most important of these were treated herein, researcher safety, which is oftentimes overlooked in discussions of ethics, and informed consent, which is generally at the core of ethics discussions, but can be complicated not just in online settings, but particularly when it comes to hostile or dangerous (online) communities. What should certainly be clear at this stage is that these issues are certainly not new but have not been systematically discussed in our sub-field to-date. While colleagues in a variety of other fields—including directly related ones, such as Internet studies—have engaged publicly with ethics issues for many years, (online) extremism and terrorism researchers have, when we have done so at all, more often discussed such matters informally among ourselves. This has to change; our nascent formal discussions on these issues must continue and develop. AoIR's most recent ethics guidelines are eloquent on the necessity for dialogue, including that "one of the most important ethical techniques to be recommended is one of the simplest: talk things over with colleagues and friends."[69] I want to go a step further, however; both informal and formal "talks" are crucial but not enough; we must, as individual researchers and research groups, commit our ethical decisions and decision-making processes to writing more often and fully than we have to-date so that a store of usable knowledge is built up over time that is then usable by us in our own and others' decision-making, including especially that of RECs/IRBs. Perhaps the greatest contribution this article can make therefore is the spurring of more discussion, the contribution of further written analyses, of both ethical successes and mistakes, and maybe ultimately, if appropriate, a formal set of ethics guidelines tailored for online extremism and terrorism research.

Acknowledgments

Many thanks to especially Elizabeth Buchanan and Charles Ess for all their work on ethics in VOX-Pol, and from whom I learned an enormous amount. Thanks too to everybody who discussed online extremism and terrorism research ethics with me at the International Studies Association's (ISA) annual convention in Baltimore in 2017, our 2018 workshops in Swansea and Amsterdam, and our 2019 VOX-Pol summer school at DCU and sponsored panel at the Society for Terrorism Research's (STR) annual conference in Oslo.

Notes

[1] Geraldine Lee-Treweek and Stephanie Linkogle (Eds.), *Danger in the Field: Risk and Ethics in Social Research* (London and New York: Routledge, 2000); Chandra Lekha Sriram, John C. King, Julie A. Mertus, Olga Martin-Ortega and Johanna Herman (Eds.), *Surviving Field Research: Working in Violent and Difficult Situations* (London and New York: Routledge, 2009); Adam Dolnik (Ed.), *Conducting Terrorism Field Research: A Guide* (London and New York: Routledge, 2013).

[2] Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 86; see also, Stephane J. Baele, David Lewis, Anke Hoeffler, Oliver C. Sterck, and Thibaut Slingeneyer, "The Ethics of Security Research: An Ethics Framework for Contemporary Security Studies," *International Studies Perspectives* 19, no. 2 (2018): 112.

[3] Monica J. Barratt and Alexia Maddox, "Active Engagement with Stigmatised Communities Through Digital Ethnography," *Qualitative Research* 16, no. 6 (2016): 711–2.

[4] Ted Reynolds, "Ethical and Legal Issues Surrounding Academic Research into Online Radicalisation: A UK Experience," *Critical Studies on Terrorism* 5, no. 3 (2012): 499–513; Elizabeth Buchanan, "Considering the Ethics of Big Data Research: A Case of Twitter and ISIS/ISIL," *PLoS ONE* 12, no. 12 (2017); Adrienne L. Massanari, "Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the 'Alt-Right' Gaze," *Social Media + Society* 4, no. 2 (2018): 7; Dounia Mahlouly, *Reconciling Impact and Ethics: An Ethnography of Research in Violent Online Political Extremism* (Dublin: VOX-Pol, 2019).

[5] Baele et al., "The Ethics of Security Research"; J. M. Berger, *Researching Violent Extremism: The State of Play* (Washington DC: RESOLVE Network, 2019); Simon Cottee and Jack Cunliffe, "Watching ISIS: How Young Adults Engage with Official English-Language ISIS Videos," *Studies in Conflict & Terrorism* 43, no. 3 (2020): 183–207; Kerstin Eppert, Lena Frischlich, Nicole Bögelein, Nadine Jukschat, Melanie Reddig, and Anja Schmidt-Kleinert, *Navigating a Rugged Coastline: Ethics in Empirical (De-)Radicalization Research* (Bonn: CoRE—Connecting Research on Extremism in North Rhine-Westphalia, 2020); Joe Whittaker, *Building Secondary Source Databases on Violent Extremism: Reflections and Suggestions* (Washington DC: RESOLVE Network, 2019).

[6] Baele et al., "The Ethics of Security Research"; Peter King, "Building Resilience for Terrorism Researchers," *VOX-Pol Blog*, 19 September 2018; Michael Krona, "Vicarious Trauma from Online Extremism Research: A Call to Action," *GNET Insights*, 27 March 2020; Massanari, "Rethinking Research Ethics"; Whittaker, *Building Secondary Source Databases*; Charlie Winter, *Researching Jihadist Propaganda: Access, Interpretation, and Trauma* (Washington DC: RESOLVE Network, 2019).

[7] See, for example, Isaac Chotiner, "The Underworld of Online Content Moderation," *The New Yorker*, 5 July 2019; Casey Newton, "The Trauma Floor: The Secret Lives of Facebook Moderators in America," *The Verge*, 25 February 2019; Benjamin Powers, "The Human Cost of Monitoring the Internet," *RollingStone*, 9 September 2017. See also Ellen Silver, "Hard Questions: Who Reviews Objectionable Content on Facebook—And Is the Company Doing Enough to Support Them?" *Facebook Newsroom*, 26 July 2018. In fact, the "unseen toll" of online extremism and terrorism researchers' work has itself attracted journalistic coverage; see Hannah Allam, ""It Gets to You." Extremism Researchers Confront the Unseen Toll of Their Work,' *NPR*, 20 September 2019; Paris Martineau, "The Existential Crisis Plaguing Online Extremism Researchers," *Wired*, 2 May 2019.

[8] Berger, *Researching Violent Extremism*, 9.

[9] *Ibid*.

[10] Maura Conway, Ryan Scrivens, and Logan McNair, *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends* (The Hague: ICCT, 2019), 3.

[11] Svana M. Calabro, "From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting," *Suffolk University Law Review* 51, no. 1 (2018): 55–75.

[12] Baele et al., "The Ethics of Security Research," 115.

[13] King, "Building Resilience for Terrorism Researchers"; Krona, "Vicarious Trauma from Online Extremism Research."

[14] Winter, *Researching Jihadist Propaganda*, 3.

[15] Allam, "It Gets to You"; see also Krona, "Vicarious Trauma from Online Extremism Research."

[16] Aline shakti franzke, Anja Bechmann, Michael Zimmer, and Charles M. Ess, *Internet Research: Ethical Guidelines 3.0* (AoIR, 2019), 11.

[17] *Ibid*.

[18] Interviewee quoted in Mahlouly, *Reconciling Impact and Ethics*, 24; see also Zoey Reeve, "Repeated and Extensive Exposure to Online Terrorist Content: Counter-terrorism Internet Referral Unit Perceived Stresses and Strategies," *Studies in Conflict & Terrorism*, [Online First], 14.

[19] Allam, "It Gets to You"; Berger, *Researching Violent Extremism*, 9–10; Krona, "Vicarious Trauma from Online Extremism Research."

[20] Stephen Brown, "Dilemmas of Self-representation and Conduct in the Field," in *Surviving Field Research*, eds. Sriram et al.; Julie A. Mertus, "Maintenance of Personal Security: Ethical and Operational Issues," in *Surviving Field Research*, eds. Sriram et al., 172. See also Reeve, "Repeated and Extensive Exposure to Online Terrorist Content," 19; Chaseedaw Giles, "Op-Ed: I'm a Black Social Media Manager in the Age of George Floyd. Each Day is a New Trauma," *Los Angeles Times*, 23 June 2020.

[21] Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 11.

[22] Massanari, "Rethinking Research Ethics," 3.

[23] Winter, *Researching Jihadist Propaganda*, 11–2.

[24] Mertus, "Maintenance of Personal Security," 172.

[25] Alice Marwick, Lindsay Blackwell, and Katherine Lo, *Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment* (New York: Data & Society Research Institute, 2016), 6.

[26] Baele et al., "The Ethics of Security Research," 107.

[27] Annette Markham and Elizabeth Buchanan, *Ethical Decision-Making and Internet Research (Version 2.0)* (AoIR, 2012), 6–10.

[28] David Décary-Hétu and Judith Aldridge, "Sifting Through the Net: Monitoring of Online Offenders by Researchers," *The European Review of Organised Crime* 2, no. 2 (2015): 132.

[29] Décary-Hétu and Aldridge, "Sifting Through the Net," 133.

[30] Åsa Rosenberg, "Virtual World Research Ethics and the Private/Public Distinction," *International Journal of Internet Research Ethics* 3, (2010): 23–36; see also, Robert W Gehl, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network," *New Media & Society* 18, no. 7 (2016): 1221.

[31] Décary-Hétu and Aldridge, "Sifting Through the Net," 133.

[32] Décary-Hétu and Aldridge, "Sifting Through the Net," 133–4.

[33] Barratt and Maddox, "Active Engagement with Stigmatised Communities"; Julia Ebner, *Going Dark: The Secret Social Lives of Extremists* (London: Bloomsbury). It should be noted that the combination of activity undertaken by Ebner—online and offline deception and engagement with extremists—is unlikely to be permitted by any university REC/IRB.

[34] Aysha Navest, Martijn de Koning, and Annelies Moors, “Chatting About Marriage with Female Migrants to Syria,” *Anthropology Today*, 32 no. 2 (2016): 22–25; Lorne L. Dawson and Amarnath Amarasingam, “Talking to Foreign Fighters: Insights into the Motivations for Hijrah to Syria and Iraq,” *Studies in Conflict & Terrorism* 40, no. 3 (2017): 192.

[35] Ebner, *Going Dark*, 81.

[36] Décary-Hétu and Aldridge, “Sifting Through the Net,” 134.

[37] Ebner, *Going Dark*, 9. See also, Lorraine Bowman-Grieve and Maura Conway, “Exploring the Form and Function of Dissident Irish Republican Online Discourses,” *Media, War & Conflict* 5, no. 1 (2012): 75.

[38] Lizzie Dearden, “Safiyya Shaikh: How an Unemployed London Mother Ran an International ISIS Propaganda Network,” *Independent* (UK), 3 July 2020; Meili Criezis, “Online Deceptions: Renegotiating Gender Boundaries on ISIS Telegram,” *Perspectives on Terrorism* 14, no. 1 (2020): 67–73. See also, Adam Bermingham, Maura Conway, Lisa McInerney, Neil O’Hare, Alan F. Smeaton, “Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation,” in *ASONAM 2009: Advances in Social Networks Analysis and Mining* (IEEE Computer Society: Digital Library, 2009), 234–5.

[39] Conway, “Determining the Role of the Internet in Violent Extremism and Terrorism,” 91.

[40] Barratt and Maddox, “Active Engagement with Stigmatised Communities,” 715.

[41] Navest et al., “Chatting About Marriage”; Dawson and Amarasingam, “Talking to Foreign Fighters.”

[42] Universities UK, *Oversight of Security-Sensitive Research Material in UK Universities: Guidance* (London: Universities UK, 2019).

[43] Eppert et al., *Navigating a Rugged Coastline*, 9.

[44] *Ibid*.

[45] Berger, *Researching Violent Extremism*.

[46] *Ibid*., 6.

[47] *Ibid*., 7.

[48] *Ibid*.

[49] J. M. Berger, *The Alt-Right Twitter Census: Defining and Describing the Audience for Alt-Right Content on Twitter* (Dublin: VOX-Pol, 2018), 21; see also, Carolyn Gallaher, “Researching Repellent Groups: Some Methodological Considerations on How to Represent Militants, Radicals, and Other Belligerents,” in *Surviving Field Research*, eds. Sriram et al., 128.

[50] Berger, *The Alt-Right Twitter Census*, 22.

[51] Daniel de Simone, “Neo-Nazi Group Led by 13-year-old Boy to be Banned,” *BBC News*, 13 July 2020; see also Ebner, *Going Dark*, 10.

[52] Amy-Louise Watkin and Seán Looney, “The Lions of Tomorrow”: A News Value Analysis of Child Images in Jihadi Magazines,” *Studies in Conflict & Terrorism* 42, no. 1–2 (2019): 102–40.

[53] Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 23.

[54] Tora K. Bikson, Ricky N. Bluthenthal, Rick Eden, and Patrick P. Gunn (Eds.), *Ethical Principles in Social-Behavioral Research on Terrorism: Probing the Parameters* (California: RAND, 2007).

[55] Franzke et al., *Internet Research: Ethical Guidelines 3.0*; Markham and Buchanan, *Ethical Decision-Making and Internet Research (Version 2.0)*; Charles Ess, *Ethical Decision-making and Internet Research* (AoIR, 2002). Links to all versions of the guidelines are available on the AoIR website at https://aoir.org/ethics/.

[56] British Psychological Society, *Ethics Guidelines for Internet-mediated Research* (Leicester: British Psychological Society, 2017); National Committee for Research Ethics in the Social Sciences and the Humanities (NESH), *A Guide to Internet Research Ethics* (Oslo: NESH, 2019). For listings of additional relevant guidelines, see Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 12–14; Massanari, "Rethinking Research Ethics," 7; Gabrielle Samuel, Gemma E. Derrick, and Thed van Leeuwen, "The Ethics Ecosystem: Personal Ethics, Network Governance and Regulating Actors Governing the Use of Social Media Research Data," *Minerva* 57, no. 3 (2019): 324.

[57] Marwick, Blackwell, and Lo, *Best Practices for Conducting Risky Research*.

[58] Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 3.

[59] *Ibid*.

[60] Samuel, Derrick, and van Leeuwen, "The Ethics Ecosystem," 329.

[61] Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 4.

[62] Samuel, Derrick, and van Leeuwen, "The Ethics Ecosystem," 325.

[63] *Ibid*., 329.

[64] *Ibid*., 338.

[65] *Ibid*., 339.

[66] Franzke et al., *Internet Research: Ethical Guidelines 3.0*, 4.

[67] *Ibid*., 6.

[68] Baele et al., "The Ethics of Security Research," 123.

[69] *Ibid*.