Global Network
on Extremism & Technology

Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities

Manjana Sold, Julian Junk

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The authors of this report are
Manjana Sold and Julian Junk

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Executive Summary

The nexus between terrorism and technology is socially and politically more relevant than ever. Almost every mobilisation and radicalisation process and every violent attack, whether carried out or prevented, has an online component to it. Researchers, not least those involved in GNET, are meeting head on the challenge of analysing these processes in difficult empirical online environments. Even when taking into account ever changing platforms and policies, as well as the shift towards ever more closed and encrypted spaces, there is abundant empirical data. This abundance creates challenges and opportunities of its own,[1] yet there are also hard limits to and grey zones around what a researcher dealing with extremist online content can and is allowed to do, which brings in ethical and data protection considerations. Discussions of such topics gained much relevance in recent years and are particularly lively in international research consortia.

While summarising the state of these discussions around ethics and privacy, this GNET report identifies the limits of and opportunities for research and formulates related recommendations for researchers and tech companies. It proceeds in three steps: first, it summarises some of the main ethical considerations that a researcher in this academic field should bear in mind; second, it provides an overview of the main data protection principles that are to be observed and highlights the opportunities for and balancing acts required of researchers in this regard; and third, it discusses the interplay between researchers, data sources and the policies of platforms, condensing in this context some key recommendations for researchers, tech companies and regulators. The most important points are: first, more cross-platform access points and databases would provide incentives for a broader and more vibrant research field; second, badly needed international research collaboration around analysing extremist online content would benefit from greater international harmonisation and a convergence of data protection rules; third, data protection regimes should not be seen as inconveniences but as enabling research by providing a clearer demarcation of what is and is not possible; and, lastly, the dynamic empirical field requires regular mechanisms of exchange between tech companies, researchers and regulators to adapt policies, habits and legal frameworks in a way that does justice to the social and political relevance of the nexus between extremism and technology.

1 Abdullah Alrhmoun, Shiraz Maher, and Charlie Winter, *Decoding Hate: Using Experimental Text Analysis to Classify Terrorist Content*, ICSR King's College London (2020).

Contents

1 Introduction

The digital space played a central role in the radicalisation processes of many perpetrators of past attacks:[1] extremists including Anis Amri (Berlin, Germany), Brenton Tarrant (Christchurch, New Zealand) and Stephan Balliet (Halle, Germany) took advantage of social media platforms not only to gather and distribute information, and to network and stage, but also to exchange ideas with like-minded people and sometimes even to share an attack live for thousands of viewers. It is through this communication by radical or extremist actors that we can learn much about the radicalisation processes that take place in the virtual world. The content and its presentation, as well as the way in which these actors communicate, are of central importance in that regard and can serve as a background against which to develop the most appropriate preventative and demobilising measures.

In the context of this research field, data retrieved from social media naturally has become increasingly important.[2] This is exemplified by numerous scientific publications based on data from social media: for instance, Facebook,[3] Twitter,[4] YouTube[5] and Instagram.[6] An extremely large pool of data can now be accessed and used to develop and test hypotheses.[7] These opportunities go hand in hand with limitations and pitfalls. This relates to potential ethical and data protection requirements, which certainly provide challenges for researchers but also many opportunities. While transparency and the guideline "maximising benefits and minimising harm" are essential throughout the entire research process, there are further principles and guidelines that need to be considered. In the first two sections, we summarise some key ethical considerations that a research process in this academic field should include and we provide insights

1 We are immensely grateful for the comments from Sebastian Golla on earlier versions of this report and his skilful legal guidance through so many of our research endeavours in the last years. Thanks go as well to Clara-Auguste Süß for her comments and Leo Bauer and Klara Sinha for their support in finalising this report.

2 Sebastian J. Golla, Henning Hofmann, and Matthias Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," *Datenschutz und Datensicherheit – DuD* 42, no. 2 (2018): 89, http://link.springer.com/10.1007/s11623-018-0900-x; Manjana Sold, Hande Abay Gaspar, and Julian Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 2020.

3 Agata Błachnio, Aneta Przepio´rka, and Patrycja Rudnicka, "Psychological Determinants of Using Facebook: A Research Review," *International Journal of Human-Computer Interaction* 29 (2013), https://doi.org/10.1080/10447318.2013.780868; Ralf Caers et al., "Facebook: A Literature Review," *New Media & Society* 15 (2013), https://doi.org/10.1177/1461444813488061; Stefania Manca and Maria Ranieri, "Is It a Tool Suitable for Learning? A Critical Review of the Literature on Facebook as a Technology Enhanced Learning Environment," *Journal of Computer Assisted Learning* 29 (2013), https://doi.org/10.1111/jcal.12007; Ashwini Nadkarni and Stefan G. Hofmann, "Why do People Use Facebook?," *Personality and Individual Differences* 52, no. 3 (2012), https://doi.org/10.1016/j.paid.2011.11.007; Robert E. Wilson, Samuel D. Gosling, and Lindsay T. Graham, "A Review of Facebook Research in the Social Sciences," *Perspectives on Psychological Science* 7 (2012), https://doi.org/10.1177/1745691612442904.

4 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (2015); Amandeep Dhir, Khalid Buragga, and Abeer A. Boreqqah, "Tweeters on Campus: Twitter a Learning Tool in Classroom?," *Journal of Universal Computer Science* 19 (2013); Shirley Ann Williams, Melissa Terras, and Claire Warwick, "What Do People Study When They Study Twitter? Classifying Twitter Related Academic Papers," *Journal of Documentation* 69 (2013).

5 Chareen Snelson, "YouTube Across the Disciplines: A Review of the Literature," *MERLOT Journal of Online Learning and Teaching Journal of Qualitative Methods* 7, no. 14 (2011), http://jolt.merlot.org/vol7no1/snelson_0311.htm; Raphael Ottoni et al., "Analyzing Right-wing YouTube Channels: Hate, Violence and Discrimination," (2018); Kostantinos Papadamou et al., "Understanding the Incel Community on YouTube," (2020).

6 Tim Highfield and Tama Leaver, "A Methodology for Mapping Instagram Hashtags," *First Monday* 20, no. 1 (2015); Asuncion Bernardez-Rodal, Paula Requeijo Rey, and Yanna G. Franco, "Radical right parties and anti-feminist speech on Instagram: Vox and the 2019 Spanish general election," *Party Politics* (2020); Lena Frischlich, "#Dark inspiration: Eudaimonic entertainment in extremist Instagram posts," *new media & society* (2020).

7 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 89.

into the main data protection principles to be observed.[8] We then highlight the opportunities available to and balancing acts required of researchers in this regard. In the third section, we discuss the interplay between researchers, data sources and policies of platforms, and give some key recommendations.

8 In Sold, Abay Gaspar, and Junk, "Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities" we discuss some of these elements in greater depth, as do the chapters from de Koning et al. "On Speaking, Remaining Silent and Being Heard: Framing Research, Positionality and Publics in the Jihadi Field," in *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations*, ed. Christoph Günther and Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) and "Ethics in Gender Online Research: A Facebook Case Study," in *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations*, ed. Christoph Günther and Simone Pfeifer (Edinburgh: Edinburgh University Press, 2020) in the same volume by Günther and Pfeifer *Jihadi Audiovisuality and its Entanglements. Meanings, Aesthetics, Appropriations* (Edinburgh: Edingburh University Press, 2020).

2 Central Ethical Considerations

Ethical considerations play a role in almost every research project. Research ethics thereby "seeks to protect the people involved, not solely ensuring compliance with the legalities".[9] When analysing content from social media platforms, personal data is ubiquitous.[10] While it neither raises completely new ethical issues nor invalidates "recognised norms and values of research ethics",[11] the oftentimes fairly easy access to and the sheer quantity of this kind of data, as well as the speed in which platforms, contexts and events change, make it not only a necessity but also quite a challenge to provide enough space for ethical considerations and adapt such considerations to changing platforms, visualities and policies. Thus, as in any research project, societal and scientific interests need to be balanced against an individual's right to privacy. However, the use of data from social media raises some particular challenges and can "present a potential minefield".[12]

Even though there is no generally accepted guideline that declares that ethical principles must be considered mandatory, some ethical principles have been repeatedly emphasised as particularly relevant in the literature. We can divide these principles into three categories: first, those that concern the relationship between the researcher and individual research subjects. Second, principles concerning the societal dimension. Third and last, those that are self-reflective and concern the researchers themselves. We summarise those findings below with the aim of making them easily accessible for future research on extremism and technology.

Ethical principles that concern the individual research subject

Principles that concern the individual research subject cover *confidentiality* or *respect for persons*, and *beneficence.* Ensuring *confidentiality* means that researchers who know the identity of a research subject need to take steps to ensure that this identity is not revealed to or by others. Whenever possible, consent should be obtained when using a person's data for research purposes.[13] Informed consent ensures that a person's personal rights and right to informational self-determination are guaranteed. Consequently, researchers are obliged to be transparent and ensure that subjects

9 NESH*A Guide to Internet Research Ethics* (2019), 3, https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.
10 Personal data is any information relating to an identified or identifiable natural person (a "data subject") see article 2 (1) GDPR.
11 National Committee for Research Ethics in the Social Sciences and the Humanities NESH, *A Guide to Internet Research Ethics*, 2.
12 Sold, Abay Gaspar, and Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 52; see also: Farina Madita Dobrick et al., *Research Ethics in the Digital Age: Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization*, ed. Farina Madita Dobrick, Jana Fischer, and Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 1.
13 NESH, *A Guide to Internet Research Ethics*, 2.

know that they are being researched, that they are informed about the upcoming research project in a comprehensible format and that they are given the opportunity to agree to participate voluntarily or to decline to do so. However, asking for informed consent is far from an easy task when dealing with extremist content, as seeking to obtain the research subjects' consent may jeopardise the research: knowing that their data will be observed or even analysed often leads people to modify their behaviour. For example, if individuals knew that they (or their online threads, posts and comments) were being observed, they may act differently, communicate through other channels, stop expressing their opinions virtually or adapt them.

Further problems arise when data from many different people is to be used for research purposes.[14] For example, it can hardly be guaranteed that users of 100,000 Twitter accounts, for example, will give their consent in a timely fashion to researchers to use their data. In such cases, researchers may offer an opt-out approach, allowing individuals to withdraw their consent at any time during the research project. The advantage of this approach is that researchers do not have to obtain the consent of all individuals in advance. This option can also be employed if the amount of personal data is relatively small or if the data is anonymised. Researchers should always treat data collected during a study and after its completion confidentially. Whether or not individuals have given their consent to the analysis has no impact. In all cases data should be pseudonymised or made anonymous by researchers. However, anonymisation is often difficult[15] and people can often still be identified after anonymisation.[16] Researchers thus must ask themselves where and how the data is stored, whether the software used is trustworthy, how comprehensive a software vendor's privacy policy is and whether, for example, there is a need for an encryption program.

Furthermore, the principle of *beneficence* applies: researchers are required to ensure that no harm is done to participants and that the benefits of the study are maximised. For example, in a study on foreign combatants, the researcher must guarantee that all data is made anonymous in such a way that the person cannot be re-identified, as this could possibly result in prosecution or public condemnation. If such anonymisation cannot be guaranteed (for example, due to the constant monitoring of the researcher during meetings with the participant or because the omission of a participant's personal data would make it impossible to test hypotheses), the study may have to be discontinued or redesigned.

As far as maximising the benefits and minimising the risks are concerned, the latter in particular is still a complex undertaking.[17] However, the benefits of data collected online can be maximised with less effort while researching digital topics. Reasons for this include low-threshold possibilities for providing data and codes for reproducibility (for example, Harvard Dataverse or GitHub) or high-quality open-access journals that can reach a large audience (such as the newly founded *Global Studies Quarterly* by ISA or *Texas National Security Review* by UT Austin).

14 Elizabeth Buchanan, "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," *PLoS ONE* 12, no. 12 (2017): 2, https://doi.org/10.1371/journal.pone.0187155.
15 Buchanan, "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," 4.
16 Matthew J. Salganik, *Bit by Bit. Social Research in the Digital Age* (New Jersey: Princeton University Press, 2018), 40. Ideally, and according to Rectical 26 GDPR, persons need to be completely unidentifiable.
17 Salganik, *Bit by Bit. Social Research in the Digital Age*, 298.

Ethical principles that concern the societal dimension

The principles relating to the societal dimension of a research project refer to *justice*, *respect for law and the public interest*. The *justice* principle points to the fact that scientists must ensure a balance of the costs and benefits to different social groups affected by a given research project. Minorities and vulnerable groups must not bear the costs while at the same time majorities and wealthy groups enjoy benefits.[18]

The principle *respect for law and the public interest* stipulates that laws and site policies relevant to research (for example, of social media companies) must generally be observed.[19] A central problem with digital research is the wide range of responsibilities that have to be observed, such as when collecting data on political extremists in different countries. In very rare cases, however, it is also possible to violate the conditions of use. For instance, New York University made a conscious decision to violate Facebook's terms of use to collect data on Facebook's political advertising strategy, presumably because Facebook continues to refuse to provide researchers with that data.[20] Since political advertising and misinformation in the digital domain are important issues for electoral integrity and the improvement of democracy, and since data should be used exclusively for the common good, the company's terms of use could be violated in this case. Furthermore, in order to satisfy the public interest, researchers must discuss their decisions transparently in public.[21] It is only then that the public is able to hold ethical debates about what scientists do and opinions from such debates can be fed back into research designs, making research projects not only more accountable but also more focused in terms of content. *Transparency* refers both to disclosing and explaining the research project to research participants and to being open about data collection and processing methods when presenting or publishing research results.

Ethical principles with regard to researchers themselves

Researchers are obviously part of any research process – their wellbeing should be of concern for any academic as well as for institutional environments. This relates to the *safety and/or security of the researcher*. In particular, when the topic is as sensitive as that of radicalisation, research must be designed in such a way that researchers themselves are protected. Dangers could entail physical threats and intimidation by others but researcher safety should also include psychological support as well, as there are limits to coping with the potentially harrowing content to be analysed. These aspects need to be taken into account before a project is started, but are all too often forgotten or not fully ensured by the institutions involved in research.

18 Salganik, *Bit by Bit. Social Research in the Digital Age*, 298; NESH*A Guide to Internet Research Ethics*, 5–6; British Psychological Society, *Ethics Guidelines for Internet-mediated Research* (2017), 17, www.bps.org.uk/publications/policy-and-guidelines/ research-guidelines-policy-documents/research- guidelines-poli.
19 Salganik, *Bit by Bit. Social Research in the Digital Age*, 300.
20 "Facebook to researchers: Stop using our data," 2020, https://edition.cnn.com/2020/10/24/tech/facebook-nyu-political-ad-data/index.html.
21 Salganik, *Bit by Bit. Social Research in the Digital Age*, 300–01.

Another issue concerns *trust*, which operates from the perspective of both the researched and the researchers. For example, researchers must question whether an online profile is a fake. There are limits to what can be verified, as well as to the transparency of one's own identity (safety and security might mean concealing one's identity). Many users employ fictitious names, provide incorrect location information or choose different languages. Often contributions are written in English, which makes it difficult to assign users nationalities.

Moreover, platform shifts, in which a thread on one platform is linked to another on a different platform, are challenging for researchers. Abbreviations, neologisms, the mixture of different languages and incomplete sentence structure are characteristics of internet conversations and pose further challenges.[22] Automated content analysis by programs is thus more difficult and poses an additional set of challenges.[23] One way of coping with these intricacies is embedded research. The role, whether active or passive, that researchers adopt during the data collection process can have serious consequences for the internal validity of a research design and raises a subset of ethical questions. If researchers manage to assume a completely passive/observational role in the data collection process at all times, they will presumably not influence the observed communication processes – which might be of utmost importance for the validity of the research findings. However, there are often limits to observational roles (for instance, via targeted questions to the researcher's profile) and there is a fine line to walk between non-intrusive and intrusive observations.

From an ethical perspective, privacy settings are also relevant for the implementation of a research project. If settings are chosen that make content publicly viewable, a researcher's analysis of such data is seen to constitute less of an invasion of the subject's privacy than if the data was only shared among 'friends' or an even smaller user-defined subset of selected persons. Ethical questions that arise when conducting research with data from social media are accompanied by legal questions. Since possible damage can be neither completely avoided nor comprehensively anticipated, the aim of both ethical reflection and legal requirements is to establish a balanced relationship between expected benefits of research and privacy interests.[24] Even if legal requirements and ethical considerations are interdependent and can only be understood as a package, both need to be addressed separately by researchers. Below we address legal recommendations we have extracted from the literature.

22 Albert Bifet and Eibe Frank, "Sentiment knowledge discovery in Twitter streaming data," in *Discovery Science*, ed. Bernhard Pfahringer, Geoff Holmes, and Achim Hoffmann, Lecture Notes in Computer Science (Heidelberg: Springer VS, 2010); Simon Carter, Wouter Weerkamp, and Manos Tsagkias, "Microblog language identification. Overcoming the limitations of short, unedited and idiomatic text," *Language Resources and Evaluation* 47, no. 1 (2013).

23 See Alrhmoun, Maher, and Winter, *Decoding Hate: Using Experimental Text Analysis to Classify Terrorist Content*.

24 Anne Lauber-Rönsberg, "Data Protection Laws, Research Ethics and Social Sciences," in *Research Ethics in the Digital Age. Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization*, ed. Farina M. Dobrick, Jana Fischer, and Lutz M. Hagen (Wiesbaden: Springer VS, 2018), 41.

3 Central Data Protection Principles – Legal Limits, Challenges and Opportunities for Researchers

In social media in general, but particularly in social networks, individuals (and groups) often reveal a great deal of information about themselves. They may provide personal information such as their ethnic origin, political opinions, religious and ideological convictions, sex habits, sexual orientation, health and affiliations, such as trade union membership. Some of this personal information may be of interest to researchers conducting studies in various fields. If, in whatever context, personal data is to be collected or used, data protection regulations must be observed. In the following, we provide an overview of the data protection legal framework of observational empirical social research in social media based on the General Data Protection Regulation (GDPR).[25]

Although the regulation contains several important privileges for scientific research, it gives no special grounds for processing. The legality of processing for research purposes is often assessed on the basis of a balance of interests in each individual case. Some personal data is particularly sensitive and is therefore subject to increased protection (for example, religious beliefs or political views that are of great relevance for examining extremist content on social media platforms). Depending on the research project, researchers may also be confronted with limits, challenges and opportunities. These will be discussed below, divided between whether consent was obtained or not, since this is of crucial importance.

Legal regulations for research with personal data with the consent of the persons concerned'

Much of the data available in social media is personal. Even if this information can be accessed online without significant barriers and was deliberately posted by the persons concerned, it is still protected as personal data by the GDPR. The collection and analysis of personal data is inevitable in many research projects. In the European Union, the legal protection applicable to such personal information is set out in the regulation.[26] Since the GDPR does not provide for specific authorisation for the processing of personal data for the purposes of scientific research, the permissibility of data processing is governed in particular by articles 5, 6 and 9. According

25 The GDPR is applicable as of 25 May 2018 in all EU member states. The goal is to harmonise data privacy laws across Europe.

26 The scope of the regulation includes all kinds and forms of "handling" data and thus the collection, storage, structuring and so on. See article 4 (2) GDPR.

to the GDPR, the processing of personal data is generally prohibited unless this is expressly permitted by law or with the consent of the person concerned.

By giving or refusing consent, a person can decide on the disclosure and use of their personal data. They must be given the opportunity to decide in each individual case whether and under what conditions their data may be processed. In order to ensure this, the data protection regulations for consenting to the processing of personal data specify certain content and formal requirements for consent. According to the GDPR, these are in particular the specific designation of the intended purpose of the use of the data, sufficient information of the data subject about the intended processing of their data, the voluntary nature of the consent and the possibility of revoking the consent to any time of the research process.

In addition to the declared consent of a person, data may also be used by researchers if the data subject has consciously published sensitive data. In such a case, article 9 (2) (e) of the regulation lifts the processing prohibition under paragraph 1 and the data subject has no special need for protection. The conscious publication of the data by the data subject can be seen as a kind of waiver of the special protection of article 9. Nevertheless, even if the data is published by the person concerned, the data is not completely removed from the GDPR's protection.[27] In particular, article 6 applies and the data still requires a legal basis for processing, even if article 9 has been waived.[28]

This leads to a question: what is meant by data that has been "made public"? Data is considered to be made public if it is made available to the public by an unspecified number of persons without any significant barrier to admission. Consequently, another central aspect in relation to data protection requirements concerns the type of social media from which the data originated. Does it come from open or closed (parts of) social media, or from social media set up specifically for research purposes? The primary demarcation criterion here is the "access hurdle through registration and login".[29] Depending on the platform, users have the possibility to limit the addressees of their content. Some social media is set up specifically for research purposes, wherein user consent to the processing of personal data proves to be a practicable solution, but this is not the case with other social media. Consequently, the legal requirements for the processing of personal data become relevant. This also applies if the data collected stems from publicly available sources.[30] Moreover, "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities".[31] In addition, individuals also have a right to privacy even when they willingly enter the public arena. Data from semi-public or even closed communication spaces is even more in need of protection than data from public spaces.

27 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 92.

28 At this point it should be noted that article 6 GDPR is also applicable at the same time as article 9 GDPR. The two then stand side by side and must both be fulfilled.

29 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 96.

30 Ian Brown and Josh Cowls, *Check the Web. Assesing the Ethics and Politics of Policing the Internet for Extremist Material*, Oxford Internet Institute (2015), 46. Public spaces are characterised by unrestricted access with the co-presence of strangers. In contrast to this, "[p]rivate spaces are characterized by restricted access … and the absence of strangers" Nicolas Legewie and Anne Nassauer, "YouTube, Google, Facebook: 21st Century Online Video Research and Research Ethics," *Forum: Qualitative Social Research* 19, 32, no. 3 (2018).

31 European Court of Human Rights Application, "Rotaru v Romania no. 28341/95," (2000): § 43.

However, as mentioned above, obtaining consent may often jeopardise research or is simply impossible due to the sheer number of people whose consent would have to be obtained. This is not only the case in research on radicalised or extremist individuals or collectives, but also in many other sensitive research areas. For this reason, below we turn to the legal regulations for research with personal data without the consent of the persons concerned.

Legal regulations for research with personal data without the consent of the persons concerned

Since research often has to rely on personal data in order to achieve research objectives, legislators have laid down eligibility criteria for research. This allows restrictions to be placed on the right to informative self-determination for the purpose of scientific research. If data is used for an investigation that does not fall into the specific categories of article 9 of the GDPR, the lawfulness of its processing is governed exclusively by article 6 instead. Accordingly, at least one of the bases set out in this article must apply when personal data is processed. Consequently, the processing of personal data without consent is only permissible in limited circumstances: for example, if either the data subject's legitimate interests are not affected at all or the public interest in carrying out the research project outweighs the data subject's legitimate interests and the research purpose cannot otherwise be achieved or only with disproportionate effort. If such a condition is met, the research may be carried out without the consent of the person(s) concerned. The lawfulness of processing without consent often depends on a balance between the right to privacy and the benefits of the research. In any case, it is necessary to weigh the research interest against the data subject's legitimate interests.

In accordance with article 9 (2) (j) of the GDPR, there are also statutory provisions for the processing of special categories of personal data for research purposes: first, the existence of a *specific research question and concept*. For the purpose of scientific research, researchers must show that the respective research project meets scientific requirements in terms of its structure and content. Second, researchers must prove *the impracticability of the project* without the concrete personal data. Researchers need therefore to explain in detail why it is urgently necessary for the research project to collect the relevant personal data. For example, scientists should ask themselves whether research could be conducted with less data or other types of data. Third, interests must be balanced again, such as the quantity of data and the special circumstances of subjects. Thus, in order to legitimise data processing for research purposes without the consent of the data subject, it must be shown why the research interest (significantly) outweighs the interest of the data subject in the protection of their data.

To this end, the *principles of necessity, appropriateness and proportionality* of the processing of personal data must be observed and access regulations must be established to ensure that personal data is used in accordance with data protection regulations: first, researchers must demonstrate that the project pursues a *legitimate purpose*. It is true that research in general may be viewed as a

legitimate purpose.[32] Nevertheless, the processing of personal data for a research project without the consent of the data subjects should only be considered if the research purpose cannot be achieved by other means.[33] *Necessity* is to be understood as another precondition for proportionality. A measure is necessary if no milder – that is, less intrusive – measure could achieve the same goal. The necessity test should be considered the first step with which a proposed measure involving the processing of personal data must comply. Should the respective measure not pass the necessity test, there is no need to examine its proportionality. A measure that is not proven to be necessary should be modified to meet the requirement of necessity.

The processing of data obtained online without consent of the data project must also be *appropriate*. The principle of appropriateness requires that the content and form of action not exceed the necessary level to achieve the objectives. In order to examine the appropriateness of the intervention, researchers must weigh up the legal justification for carrying out the intervention (often based on the perceived societal benefit of the research) against the obligation to protect the individual whose privacy is violated by the intervention. After this consideration, researchers must also demonstrate that, according to article 89 of the GDPR, measures and safeguards to protect data subjects, such as, for example, pseudonymisation, are respected.

Another relevant aspect when considering the research project from a data protection perspective refers to the researcher's activity or passivity. The question of whether the researchers are passive observers when collecting the data – that is, whether they have chosen a non-reactive collection method – also has an impact on data protection requirements. In the case of such a procedure, the researcher does not take an active role at any time and does not enter into the discourse. Although such passive observation also rules out obtaining consent from the outset,[34] the intervention is kept to a minimum in that no influence is exerted on what is commented on or posted. Meanwhile, engaging in research with an active approach means that it is possible to obtain consent for the collection and analysis of personal data, but this also introduces the risk of producing interfering content, (further) advancing the discourse or potentially influencing the posting behaviour of others.

Individuals whose consent cannot be obtained should be offered further protection. According to article 89 (1) of the GDPR, technical and organisational measures must be taken to ensure, in particular, that the principle of data economy is respected. Important aspects in this respect are the reduction in the amount of data collected and limiting the scope of processing solely to the extent necessary for the purpose, the specification of a storage period, and a regulation on the accessibility of the data. Insofar as the purposes pursued can also be achieved with anonymised or pseudonymised data,

32 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 90.

33 Sold, Abay Gaspar, and Junk, Designing Research on Radicalisation using Social Media Content: Data Protection Regulations as Challenges and Opportunities, 62–63.

34 Kerstin Eppert et al., *Navigating a Rugged Coastline: Ethics in Empirical (De-)Radicalization Research*, core-nrw Netzwerk für Extremismusforschung in Nordrhein-Westfalen (Bonn, 2020), 9, https://www.bicc.de/fileadmin/Dateien/Publications/other_publications/Core-Forschungsbericht_1/CoRE_FP_1_2020.pdf.

article 89 (1), sentences 3 and 4, of the GDPR stipulates that this needs to be the case. As far as data archiving is concerned, role concepts and secure access solutions are obvious.[35]

Furthermore, even if personal data may be processed (by virtue of consent or a legal provision), technical and organisational measures must be taken to ensure that the purposes of data protection are met. For example, this could be achieved by storing identifiers and data separately. In addition, the data should be earmarked for a specific purpose. Information therefore will only be held and examined for the purpose for which it was collected.

35 Golla, Hofmann, and Bäcker, "Connecting the Dots: Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu," 94.

4 Data Source, Platform Policies and Researchers – Overview, Interplay and Recommendations

In addition to ethical principles and data protection regulations, users and researchers must comply with and take into account the legal agreements of the respective platform, as well as other individual restrictions when using third-party programs. The fact that, on the one hand, leading platforms utilise different policies and, on the other, such policies are often long or difficult to understand poses a challenge of its own. Below we provide a brief overview of the most relevant policies of leading tech companies and derive some general recommendations.

Twitter

With Twitter's new privacy policy, which is in accordance with the GDPR and came into effect in May 2018, Twitter gives its users more control over their data. Since it applies to every user regardless of their location, it appears that GDPR protection will be extended to all users around the globe. Twitter collects information about the IP address and device type from users as soon as they are look at tweets. Of course, data is also generated and collected when a user sends tweets, interacts with other users, retweets, likes and more. According to Twitter's privacy policy, direct messaging content is excluded from data collection and processing. The collected data is used to suggest tweets, track accounts and target advertising. To a certain extent, Twitter offers its users controls about what kinds of data are allowed to be collected. For instance, users can set their accounts to public or private and turn on or off photo-tagging by others. Users can also download information that was shared by the user on Twitter. For example, in addition to public tweets, which "are immediately viewable and searchable by anyone around the world", users are also given the opportunity to use "non-public ways to communicate on Twitter too, through protected Tweets and Direct Messages".[36] Additionally, it is also possible to use Twitter under a pseudonym and "data is kept for up to 18 months, or until account deletion".[37] With the launch of its API v2 in August 2020, "Twitter is making it easier for businesses, academics, and third-party developers to build on its platform":[38] it offers third-party developers access to features long absent from their clients, including "conversation threading, poll results in Tweets, pinned Tweets on

36 Twitter, *Twitter Privacy Policy* (2020), https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-18th-2020/Twitter_Privacy_Policy_EN.pdf.

37 Identity Guard, "What You Need to Know About Twitter's Privacy Policy," (2018), https://www.identityguard.com/news/twitter-privacy-policy.

38 "Twitter launches new API as it tries to make amends with third-party developers," 2020, https://www.theverge.com/2020/8/12/21364644/twitter-api-v2-new-access-tiers-developer-portal-support-developers.

profiles, spam filtering, and a more powerful stream filtering and search query language".[39] In addition, there is also access to a real-time tweet stream.

API access has been reorganised by Twitter on three levels: during the early access period it was possible "to listen and to analyse the public conversation".[40] However, since only the free, basic access level has been launched, which limits the number of API calls developers can make, it remains to be seen what changes and opportunities will arise for researchers. A central advantage of Twitter compared to other social networks is its open communication. Individual tweets as well as entire conversations can be searched and viewed by anyone, regardless of whether they are a user or have a Twitter mutual following with the person in question. Thus researchers have access to not only comprehensive and unfiltered data but also data protection. One limitation of researching Twitter is that data use must not harm its economic interests. The creation, enrichment and distribution of large databases with tweets is prohibited, even for non-commercial purposes.[41] Results cannot be weighed or compared because researchers do not have information about overall Twitter activity.

Facebook

Similar to Twitter, Facebook has not only revised its data protection policy in accordance with GDPR but also made it applicable to its customers worldwide. Facebook, Instagram, Messenger and other products and features offered by Facebook collect different types of information depending on a user's interactions with Facebook products. This includes information and uploaded content, data of a user's social networks (such as the accounts, groups, hashtags and so on with which they interact), usage information and data on internal platform purchases, as well as data on other users' interactions with a user's content and profiles. In addition, data is collected on devices connected to Facebook or Instagram, including device attributes, cursor movements, internet providers, phone companies and device settings. Facebook uses this data to refine its own products and customise content and account recommendations. It also makes the data available to third party customers. In addition, data is not only shared with advertisers, but also with third parties who run apps on Facebook or otherwise use its services. As with other social media platforms, users can restrict data collection through their settings, as well as download and access the user data collected on them. Some data is subject to special protections: users can choose to provide Facebook information about their religious or political views, health, racial or ethnic origins, philosophical beliefs or trade union membership.[42] Although Facebook recently has made some improvements in terms of privacy,[43] the user interface is still not transparent enough. Furthermore, in contrast to personalised advertising, users can barely limit data collection. Facebook gives its users the possibility to access their Facebook information, including

39 "Twitter ändert APl zugunsten von Third-Party-Entwicklern," 2020, https://onlinemarketing.de/technologie/twitter-api-third-party-entwicklern.
40 "Twitter API v2: Early Access," 2020, https://developer.twitter.com/en/docs/twitter-api/early-access.
41 Michael Beurskens, "Legal questions of Twitter research. Twitter and society," in *Digital Formations*, ed. Katrin Weller (New York et al.: Peter Lang, 2014).
42 "Data Policy," 2020, https://www.facebook.com/policy.php.
43 "Mit mehr Kontrolle über die eigene Privatsphäre ins neue Jahrzehnt," 2020, https://about.fb.com/de/news/2020/01/mehr-kontrolle-uber-die-eigene-privatsphare/.

photos, posts, reactions and comments using the so-called "Access Your Information" tool. Additionally, users are able to download a copy of their Facebook information using the "Download Your Information" tool.

Facebook also provides researchers and academics information and content to conduct research.[44] In response to the Cambridge Analytica debacle in 2018, Facebook promised a research initiative to give academics access to its data while keeping user information private. Despite launching a new data access hub to give researchers the opportunity to see all the Facebook datasets available to them, Facebook continues to be criticised[45] for failing to support researchers sufficiently.

Google

Google, unlike Facebook and Twitter, seems to have so far refrained from applying its revised privacy policy, which is in line with the GDPR, to regions outside the EU. For example, it has been reported that users in the UK will lose GDPR protection and now have to accept that, unlike in the EU, where it must be stored on servers in accordance with GDPR rules, their data is stored in the USA – and this means that data protection levels vary according to guidelines that service provides by and large set themselves. As YouTube is only one part of Google's empire, which consists of dozens of apps, services and a mobile operating system, the company is therefore likely to collect more data about its users than, for example, Twitter or Facebook. Among other things, YouTube collects data on user interaction, comments, video uploads, video consumption and much more. While YouTube does share user data with third parties who post ads on the site and provides an API, it is explicitly stated that YouTube does not sell data to third parties, such as other social media companies. YouTube offers users who want access to their data numerous options to review and even delete data.

TikTok

Unlike many large social media companies, TikTok takes a regionally segmented approach to privacy policy. In Europe, for example, there is a directive that takes certain GDPR requirements into account. For the USA and other countries, separate guidelines apply. In addition to the usual data points (usage activities, device information, location data, phonebook when accessed, information on third-party content shared on the platform), content is also collected and analysed. TikTok does not appear to provide researchers with access to an API or other means to collect data legally. Instead, IT specialists have found ways to create unofficial APIs to collect data on users, views and interactions.[46]

44 For further details see "Facebook Research. Supporting exciting and innovative research through meaningful engagements," 2020.
45 See "Facebook needs to share more with researchers," World View, 2020, https://www.nature.com/articles/d41586-020-00828-5, for instance.
46 "How to Collect Data from TikTok," 2020, https://towardsdatascience.com/how-to-collect-data-from-tiktok-tutorial-ab848b40d191.

Telegram

Similar to TikTok, Telegram also maintains a separate privacy policy for European users. As communication platform, Telegram only stores basic information about users (telephone number, email address, username, and so on). Regular chats (which are called "cloud chats") between users and group chats are also stored. Secret chats are said to be fully encrypted throughout, and only visible to users who are involved in them. Telegram also does not provide researchers with any means of collecting and analysing data, such as an API. However, researchers have created their own scraper to access public channels, interactions and messages for research purposes.[47] While scraping is an attractive tool for evaluating social networks for research purposes, it represents, in terms of legality and ethical considerations, a particularly contested way of retrieving data.[48]

General Recommendations

The picture from this overview is at best diffuse: some data is available to researchers, depending on the platform. Generally, platforms reserve the rights to data, and to process or pass it on. However, not all platforms have clearly spelled out the access points and terms of reference for scientific use. A further opening up of many tech companies to science would also be desirable with clear-cut, durable and harmonised APIs and with regard to searches (for instance, for datasets that are created using a search term). On Twitter, for example, tweets linked by replies are not included in search results. Data Grants[49] is a pilot programme to give researchers access to public and historical data, but such access is limited to a few projects selected by Twitter.

The research and investigation of often violent political online extremism is high on the agendas of various political and societal institutions as well as of technology companies. Databases with user data are, as discussed earlier in this report, subject to the respective national data protection regulations. These limit, for good reasons, the sharing of existing data with other scientists domestically and, particularly, internationally. In this context it is worth questioning researchers' potential use of collected data for further analysis and projects. While the GDPR applies to all EU member states, rules for collaboration with outside partners are less clear, even though there is an increasing convergence of standards around the world and tech companies like Facebook implement and push for global rules.

While there still exists a variety of constraints, the tendency is promising. Furthermore, there are certain privileges for researchers in most data protection regulations, including the GDPR. If certain principles are balanced systematically and transparently in data protection strategies for given research projects and in close discussion with data protection officers (and, in some instances, with the platforms), the necessary analyses and access to findings for further researchers are possible in almost every case. Still, there are some limits to reproducing results if data is retrieved from encrypted spaces and under conditions of pseudonymisation or anonymisation.

47 Jason Baumgartner et al., *The Pushshift Telegram Dataset* (2020).
48 Sebastian J. Golla and Max von Schönfeld, „Kratzen und Schürfen im Datenmilieu – Web Scraping in sozialen Netzwerken zu wissenschaftlichen Forschungszwecken," *Kommunikation und Recht* (2019).
49 See "Introducing Twitter Data Grants," 2014, https://blog.twitter.com/engineering/en_us/a/2014/introducing-twitter-data-grants.html.

This is aggravated by the fact that more and more extremist content is quickly deleted. If deleted extremist content were to be safely hosted, researchers with access to such content would likely find themselves able to provide more thorough analysis. In this regard, there is much to discuss with online and print academic publishers, for instance, around ensuring a high degree of external validity for a published study without providing incentives for violating data protection requirements and research ethics. If this balance is not struck, research will yield far too few relevant results.

Close cooperation between tech companies and researchers regarding knowledge-sharing, technical collaboration and shared research is a win-win situation for both sides. Researchers could make much more use of flagging problematic content, for instance, but they should critically engage with the implications of flagging according to the ethical standards outlined above. Tech companies need to be transparent about their mechanisms for dealing with flagged content and aware of the ethical and research-practical challenges researchers face in this regard. One solution could be the provision of an option to deal with content flagged by researchers differently from other content: companies could monitor such content closely without deleting it. An example of successful cooperation between tech companies and researchers is the Global Internet Forum to Counter Terrorism (GIFCT). One of GIFCT's central objectives is to "empower researchers to study terrorism and counterterrorism, including creating and evaluating best practices for multi-stakeholder cooperation and preventing abuse of digital platforms".[50] GNET is funded by GIFCT and the dialogues that this enables – both critical and open – are immensely valuable and need to continued permanently if they are to deepen.

There are several tools or at least initiatives across platforms that are of interest to researchers working with public content from social media. CrowdTangle[51] is one such tool, which allows for analysing public content in social media and compiling it into reports. CrowdTangle makes accessible the timing of a post, the type of contribution (video, image, text) and information about which page, public account or public group it was posted to and how many interactions (e.g. "Like" information, reactions, comments, how often the contribution was shared) or video views it generated, as well as which other public pages or accounts have shared it. While this is a good start, there is room for improvement and expansion. Among other things, criticism has been levelled at CrowdTangle that it is not particularly useful to researchers since it is difficult to scan for patterns not identified in advance.[52] Moreover, many research projects require specifically non-public data. Besides CrowdTangle or a possible revision of its offering, more initiatives are welcome. As users shift from one platform to another, as extremist networks span various platforms and as content is increasingly cross-posted across platforms, cross-cutting tools would be a boost for further research and would bring more disciplines and scholars on board to analyse the various social and political challenges that arise from the online dynamics of extremism: more of such initiatives are needed and welcomed.

50 "Global Internet Forum to Counter Terrorism: Evolving an Institution," 2020, https://www.gifct.org/about/.
51 Comprehensive access to CrowdTangle is only available to selected companies and organisations that meet the requirements. However, the CrowdTangle Link Checker Chrome Extension is available to all interested parties. The extension shows how often a URL has been shared, which public pages or accounts have shared the URL and the interaction data for these posts.
52 Hegelich, "Facebook needs to share more with researchers."

5 Concluding Remarks

Some researchers still avoid working with data from social media or embark upon research projects without giving data protection issues and ethical principles sufficient attention – or any at all. In order to reduce the hesitation felt by researchers, this report has offered insights into the key ethical considerations and data protection requirements that scientists are confronted with when working with personal data from social media, and outlined challenges and limitations such work poses. Despite these hurdles, we cannot and should not avoid the analysis of data from the digital world. Online and offline worlds have long been closely linked. In order to better understand phenomena, a consideration of both worlds is inevitable. Thus, our goal is to encourage other researchers to work with data from social media. To this end, the report also pointed out opportunities.

Whenever possible, researchers must fulfil their duties and responsibilities and mitigate any risk against research subjects. Researchers should also obtain informed consent whenever possible, delete highly identifiable information and reserve the acquisition of informed consent to the dissemination stage of a project. Researchers must consider ethical and data protection requirements at all stages of a research project (from its very beginning until the dissemination of results and the handling of the data after completion of a project).

Data from different platforms is of interest to researchers. The privacy policies applied by individual tech companies are as different as the platforms themselves. While there is some overlap – for example, Facebook and Twitter comply with GDPR requirements for their global users – there are also differences, some of which have been discussed in this article. Although more emphasis has been placed on a user-friendly policy in recent years, not least because of increased requirements and pressure on platform operators, it is often unclear what opportunities are available to researchers. There is an urgent need for further improvements in terms of rights and access for researchers across platforms. Even if there have been positive developments, there is a need for tech companies to make further concessions to researchers. At the same time, researchers should also make more use of existing offers from tech companies – and they should do so in accordance with the basic ethical and legal principles that this report outlined and that are, rightly used in a research designs, less constraints than enablers.

Policy Landscape

This section is authored by Armida van Rij and Lucy Thomas, both Research Associates at the Policy Institute based at King's College London. It provides an overview of the relevant policy landscape for this report.

Introduction

Researching terrorist and/or extremist contents has for decades brought forth challenging questions on the legality, morality and practicality for researchers, governments, activists and law enforcement agencies alike. On the one hand, there is data protection legislation and the constraints by which researchers must operate when handling personal data. On the other, there is the legislation around counterterrorism and the ways in which terrorist and extremist data may be used for research purposes. This creates an increasingly complex field for researchers to navigate, with risks to themselves and others.

In this report, we will take a slightly different approach to previous reports, in that we will address the policy landscape on personal data protection in eight of the nine countries first. Then the report will give an in-depth overview of the counterterrorism landscape in the ninth country, the UK, and address some of the difficult questions researchers interested in researching terrorism may come across.

Data protection on social media platforms: addressing the challenges and assessing new developments

Canada

The Office of the Privacy Commissioner of Canada (OPC) has responsibility for the protection and promotion of individuals' data privacy rights. The OPC's mandate includes enforcing compliance with both the Privacy Act, which governs how federal government agencies handle personal data, and the Personal Information Protection and Electronic Documents Act (PIPEDA), which covers the private sector. PIPEDA is a federal law, but the provinces of Alberta, British Columbia and Quebec have individual data privacy laws that are substantively similar.[53]

Generally speaking, PIPEDA obliges private organisations to "obtain an individual's consent when they collect, use or disclose that individual's personal information," and comply with legislative demands

53 'PIPEDA in brief,' Office of the Privacy Commissioner of Canada. Accessed: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

to safeguard that data. Under PIPEDA, corporations must follow ten 'fair information principles' to ensure individuals' data rights are protected, including accountability, consent, limiting collection, limiting use, disclosure, and retention, accuracy and safeguards.[54]

As well as horizon-scanning research to scope out new technologies and their impact on Canadians' data rights,[55] PIPEDA also gives the OPC enforcement powers for breaches of data protection. These enforcement powers include investigatory powers and financial disincentives – companies who fail to report data breaches to the OPC can be fined up to $100,000. Similarly to New Zealand, this fine falls far below those of other jurisdictions, such as the GDPR's €20,000,000 (or up to 4% of total annual turnover).

In November 2020, Canada's Minister of Innovation, Science and Industry proposed a new piece of legislation to protect personal data. In a press release, the ministry cited the coronavirus pandemic as the context for modernising and updating privacy laws, since many more individuals are making use of technology to communicate with one another.[56]

The proposed legislation, the Digital Charter Implementation Act (DCIA), would establish a new privacy law for the private sector including social media platforms. The DCIA would include far stronger oversight and enforcement powers for breaches – up to 5% of revenue or $25 million – as well as requiring transparency from businesses relating to their use of algorithms and artificial intelligence. The DCIA would mean that "Businesses would have to be transparent about how they use such systems to make significant predictions, recommendations or decisions about individuals. Individuals would also have the right to request that businesses explain how a prediction, recommendation or decision was made by an automated decision-making system and explain how the information was obtained."[57] Ghana's Data Protection Act 2012 has a similar clause (see below).

European Commission

As part of the European Commission's initiative to "get Europe fit for the digital age", the EC has concentrated on regulating the many facets that digital services comprise. This includes personal data protection and privacy. The European Union's data privacy is regulated by the General Data Protection Regulation (GDPR). The GDPR came into force in 2016. It serves to "protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes" and to " will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism".[58] Crucially, it applies to companies who operate within the European market,

54 Ibid.
55 'Research,' Office of the Privacy Commissioner of Canada. Accessed: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/
56 'New proposed law to better protect Canadians' privacy and increase their control over their data and personal information,' Government of Canada, 17 November 2020. Accessed: https://www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html
57 'Fact Sheet: Digital Charter Implementation Act, 2020,' Government of Canada. Accessed: https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html
58 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

regardless of where they are based. This means that companies such as Google also need to abide by GDPR principles or risk being fined and/or sued.

Alongside the GDPR, a European Data Protection Supervisor was also established. This is an independent EU body, tasked with ensuring compliance and handling any complaints under the GDPR.[59]

Aside from protecting the rights of citizens, the GDPR also gave relevant authorities the tools to ensure compliance and aimed to increase accountability for those who handle personal data. Since 2018, when all EU member states needed to have put into action the GDPR, thousands of complaints have been filed, and hundreds of fines have been issued for breaching the regulation. Perhaps one of the most high-profile was France's fining of Google for "lack of transparency, inadequate information and lack of valid consent regarding ads personalisation" and issuing a €50,000,000 fine.[60]

In addition to the GDPR, there is also the Data Protection Law Enforcement Directive. Directive 2016/680 relates to the processing of personal data by law enforcement agencies where one is a suspected perpetrator, a witness or a victim of crime.[61] However, the delineation between the GDPR and Directive 2016/680 in their respective scopes of application is blurred, with a risk that one data processing operation might fall under the GDPR in EU member states, but under the Directive in others.[62]

Finally, there is the EU Directive on the Security of Network and Information Systems (NIS), which provides legal measures to boost cybersecurity.[63] This is in particular related to: enhancing member states' preparedness; increasing cooperation among member states; reinforcing vital infrastructure across the EU.[64]

While data privacy regulation has, to some extent, jurisdictional limits, the EC is also seeking to implement the e-Privacy Regulation (replacing the e-Privacy Directive).[65] This regulation, in turn, seeks to protect the privacy of citizens on online platforms, such as messenger applications. While the European Parliament has adopted the e-Privacy Regulation, discussions have stalled at the European Council level.[66] Some have argued that this emphasis on data protection is in contradiction to the EU's counter-terrorism legislation.[67]

France

France, as an EU member state, implemented the GDPR in May 2018 and the NIS in 2019. If and when the European Council is able to conclude negotiations on the e-Privacy Directive, as discussed above, the Directive will govern citizens' data protection alongside the GDPR and the NIS.

59 See https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
60 See https://www.bbc.co.uk/news/technology-46944696
61 See https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
62 See https://www.tandfonline.com/doi/pdf/10.1080/13600869.2017.1370224?needAccess=true, p.253
63 See https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
64 Ibid.
65 See https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0568:FIN:EN:PDF
66 See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform
67 See https://www.coe.int/en/web/commissioner/-/human-rights-in-europe-should-not-buckle-under-mass-surveillance

A requirement under the NIS is the establishment of a data protection authority. In France this is the Commission Nationale de l'Informatique et des Libertés (CNIL). So far CNIL has issued fines to Google and others for breaching the GDPR.

Ghana

Ghana's flagship data privacy legislation is codified in its Data Protection Act, passed in 2012. Similarly to such other countries as Canada and New Zealand, the Act establishes a Data Protection Commission (DPC), which has oversight and enforcement powers to ensure compliance with the Act's responsibilities.[68]

The Data Protection Act 2012 covers both public and private sector data controllers, obliging them to abide by eight data protection principles, including accountability, specification of purpose and openness.[69] Akin to other countries, the DPC has the power to impose fines on data controllers that breach responsibilities as laid out in the Act.

One of the most innovative aspects of Ghana's Data Protection Act, especially considering that it was passed in 2012, is a clause that gives individuals the right to freedom from automated decision-making. This clause means that "important decisions about you based on your personal details should have a human input and must not be automatically generated, unless you agree to this."[70] This modern and consent-based model for automated and algorithmic data processing could potentially have far-reaching consequences for the ways in which researchers could access and process social media data using software. Although the clause currently relates to information that "significantly affects that individual,"[71] if the Ghanaian government moves to strengthen that clause, it could mean that researchers would have difficulty in using automated data-scraping software.

However, the Data Protection Act 2012 currently undermines its citizens' data rights via a clause stating that "personal data which is processed for research purposes … may be kept indefinitely."[72] Furthermore, if "the data is processed in compliance with the relevant conditions" then "personal data which is processed only for research purposes is exempt from the provisions of this Act."[73] This severely compromises individuals' data rights since researchers can meet the minimum requirements for data protection and otherwise process the data in an unethical manner. The broad and vague definition of 'research' also means that individual data rights can be imperilled with relative ease.

68 See https://www.dataprotection.org.gh/
69 'The Data Protection Principles,' Data Protection Commission. Accessed: https://www.dataprotection.org.gh/data-protection/data-protection-principles
70 'Data Protection for Individuals,' Data Protection Commission. Accessed: https://www.dataprotection.org.gh/data-protection/data-protection-for-individuals
71 Data Protection Act 2012, s.41. Accessed: https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843
72 Ibid., s.65.
73 Ibid.

Japan

Provisions for data protection in Japan are made by the Act on the Protection of Personal Information 2003 (APPI). The responsibility to enforce compliance with the APPI lies with the Personal Information Protection Commission (PPC), established in 2016 in order to centralise previously disparate regulatory authorities.

The PPC has lower-than-average oversight and enforcement powers: data breaches can result in fines and imprisonment. However, the fines for breaches are extremely low – up to ¥300,000 (just above £2,000, or around $2,800).[74] The APPI also does not insist upon any direct obligations on entities that process personal data, but rather imposes light-touch supervisory and guidance measures. This is especially important as regards academic research, since the APPI is extended in terms of its territorial scope beyond Japan, so that anyone handling data about Japanese individuals – even if this handling takes place outside Japan – is obliged only to abide by these light-touch measures.

The APPI was revised and amended in 2020, with significant consequences. Unlike the general global trend towards strengthening citizens' data rights, the 2020 amendments relax a data processor's obligations significantly. For pseudonymously processed information, the purpose of data use may be changed beyond the scope of original use, the obligations to notify the PPC of a data breach no longer apply and individuals no longer have the right to access, correct or request the cessation of use of their data.[75]

In another setback for individual data rights, researchers are also exempted from the APPI, since it "only applies to persons or entities that handle personal information in the course of their business."[76] In reality, this means that Japanese citizens whose personal data is accessed and processed by researchers have very few data rights.

New Zealand

In New Zealand, the Office of the Privacy Commissioner (OPC) has responsibility for the protection of personal information and data. The office was established in 1993 as part of the Privacy Act of the same year, New Zealand's first substantive piece of legislation to govern personal data. This legislation controls how personal information is "collected, used, disclosed, stored, and given access to."[77] The OPC's functions are both reactive and proactive: not only does it investigate complaints about breaches of privacy and enforces compliance with the Privacy Act, but the Commissioner also monitors developments in emerging technologies for their potential impact on individual privacy.[78]

74 Act on the Protection of Personal Information 2003, s.56. Accessed: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
75 'Japan – Data Protection Overview,' Data Guidance. Accessed: https://www.dataguidance.com/notes/japan-data-protection-overview
76 Ibid.
77 'What is personal information and the Privacy Act?,' Data.govt.nz. Accessed: https://www.data.govt.nz/manage-data/privacy-and-security/what-is-personal-identifiable-information-and-the-privacy-act/
78 'What we do,' Office of the Privacy Commissioner. Accessed: https://www.privacy.org.nz/about-us/what-we-do/

In December 2020, new legislation came into force in New Zealand that protects personal information: the Privacy Act 2020. The new act was proposed "in response to the way technology has revolutionized the handling of personal data,"[79] since the nature and volume of personal data has changed almost beyond recognition since 1993. Given this, changes to the 1993 act are remarkably few; the current commissioner stated that this was because "the Privacy Act is a technology-neutral piece of legislation with a principle-based approach that has made it resilient in the face of technological changes."[80]

The main change in the new act is to protect New Zealanders' personal data abroad: information can now not be "disclosed overseas unless there are safeguards comparable to New Zealand law."[81] The 2020 act also explicitly has an "extraterritorial effect" built in to it, so that any business operating in New Zealand will be subject to the data protection obligations, even if there is no physical presence there.[82] These jurisdictional points are interesting, since many major tech and social media companies are based overseas, particularly in the United States – which has weaker data protection laws. With many countries adopting similar legislation, international pressure is increased on the USA to toughen up its own data privacy laws to keep up with overseas obligations.

The Privacy Act 2020 also gives the OPC greater enforcement powers, including increasing the maximum fine for breaches of privacy principles from $2,000 to $10,000. In terms of the international context, this fine falls far below those of other jurisdictions, such as the GDPR's €20,000,000 (or up to 4% of total annual turnover), or Australia's $10,000,000 maximum. Additionally, New Zealand's new act failed to reflect the GDPR's "right to be forgotten," in which individuals can request personal information to be deleted.[83] This right is particularly important considering data ethics as it relates to research, since users posting extremist content on social media platforms – content that may be used for research purposes – have the right to delete it.

UN Counter-Terrorism Committee Executive Directorate

As for within the UN system, data protection there falls under the scope of work of the UN Conference on Trade and Development (UNCTAD). UNCTAD has discussed the need to balance data protection with surveillance and the challenges this brings. It has described how, following a high profile court case referred to the European Court of Justice, there is now "a direction to place conditions and restrictions on surveillance in any data protection regime in Europe, and this may have knock-on effects on all those jurisdictions that follow European law closely."[84]

79 'Input of the New Zealand Human Rights Commission: OHCHR Report on the Right to Privacy in the Digital Age,' United Nations Human Rights Office of the High Commissioner, 10 April 2018. Accessed: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/HRC_NewZealand.pdf

80 'Media Release: Privacy Act turns 25,' Office of the Privacy Commissioner, 19 February 2018. Accessed: https://www.privacy.org.nz/assets/Uploads/2018-02-19.pdf

81 'Privacy Act 2020: One Small Step for New Zealand, but No Giant Leaps in Sight,' Equal Justice Project, 31 August 2020. Accessed: https://www.equaljusticeproject.co.nz/articles/37tbkho3ex74g87sw2n6yz6beyso4a2020

82 'Privacy 2.0: Key changes in the Privacy Act 2020,' Office of the Privacy Commissioner, 16 June 2020. Accessed: https://www.privacy.org.nz/blog/key-changes-in-the-privacy-act-2020/

83 'Privacy Act 2020,' Equal Justice Project, 31 August 2020. Accessed: https://www.equaljusticeproject.co.nz/articles/37tbkho3ex74g87sw2n6yz6beyso4a2020

84 See https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf, p.16

Jurisdiction is another incredibly difficult area, particularly when it comes to online data protection. UNCTAD notes that the GDPR has an extraterritoriality clause, article 3, which in effect tries to ensure "local data protection" that is targeted at local residents, regardless of the location of the business.[85]

United States

Unlike many other nations, the USA has no central federal privacy law. Instead, there are several data privacy laws that focus on separate aspects of data privacy – for instance, health data is protected by the Health Insurance Portability and Accountability Act 1996 and personal data held by the government is subject to the US Privacy Act of 1974.

Crucially, personal data and data privacy on the internet in the United States currently has no federal regulation. In the USA, the internet is somewhat of a regulatory Wild West, in which individuals, groups, organisations and corporations can access and process data without specific data rights regulation.

At present, the only way for individual data rights to be protected on social media platforms is via the Federal Trade Commission (FTC). For instance, in 2019 the FTC was able to levy a huge $5,000,000,000 fine from Facebook for violating privacy as part of the Cambridge Analytica scandal.[86] The FTC investigated and fined Facebook under its powers as laid out in Section 5, which relates to "unfair or deceptive acts or practices." Facebook shared users' personal information with third-party apps downloaded by a users' 'friends', but since many users were unaware of these practices and did not have recourse to opt out of them, it constituted an unfair or deceptive act.[87] This legal point is important, since it means that if a company does not disclose information about their data processing or handling, it cannot be held liable against the "unfair or deceptive acts or practices" clause.

A handful of states have passed legislation to protect consumer data privacy, most importantly California. Since many of the major social media and tech companies are based in California, data protection regulation there is of great importance. The California Online Privacy Protection Act 2004 was the first act to require websites to post their privacy policies and crucially this extends to any website that Californians can access, which therefore obliges virtually all American websites to comply.

On 1 January 2020, the California Consumer Privacy Act (CCPA) came into effect. The CPPA is a landmark for US data protection, since it applies to "for-profit businesses that do business in California" or meet other requirements relating to revenue and Californians' data. In practice, this means that major tech and social media companies fall under the CPPA's scope. The CCPA guarantees individuals the right to know what personal information is collected about them, the

85 Ibid., p.20.
86 Julia Carrie Wong, 'Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports,' *The Guardian*, 12 July 2019. Accessed: https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations
87 'FTC Imposes $5 Billion and Sweeping New Privacy Restrictions on Facebook,' Federal Trade Commission, 24 July 2019. Accessed: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

right to delete this information, the right to opt-out of the sale of their personal information. Businesses are required to give consumers notices to explain their privacy practices.[88]

The passage of the CPPA and the FTC's Facebook fine signal a political appetite in the USA to protect individuals' data rights. In February 2020, Senator Kirsten Gillibrand proposed a sweeping data protection act that would establish an independent federal enforcement agency.[89] Although this falls short of guaranteeing specific privacy rights and obligations for all Americans, it suggests that the USA may be moving in the direction of establishing federal legislation.

Researching Extremist Content in the UK: Prevent, counter-terrorism legislation and policy developments

In the wake of the terror attacks on 11 September 2001 in New York City and the Pentagon in the USA, many Western nations tightened their internal security measures in an attempt to prevent attacks on their own soil. Counter-terrorism policy in the West became increasingly concerned with and centred around the notion of radicalisation – that individuals can increasingly come to identify with terrorist values, eventually coming to espouse them or even carry out violent attacks for terrorist causes. This process of radicalisation has been attributed to a wide range of social and individual factors: exposure to ideology, victimisation, alienation, socialisation, social networks, the internet, deficiencies in family bonds, trauma, relative social and economic deprivation, and "cultures of violence".[90] Given the sheer number of possible 'routes to radicalisation', governments have come to "believe that they can pre-empt future terrorist attacks through a range of interventions in everyday life."[91]

In 2003, the Home Office in the UK launched the Prevent strategy as part of its wider counter-terrorism strategy, CONTEST. Prevent was revised and relaunched in 2011, in order to target individuals who are 'vulnerable' to radicalisation,[92] particularly within civic institutions such as schools, registered childcare providers, universities, colleges, prisons, probation services, healthcare, social services and immigration enforcement. The Prevent strategy occupies the 'pre-criminal space'[93] – it intervenes before any criminal activity has taken place in the hopes of disrupting the radicalisation pathway.[94]

88 'California Consumer Privacy Act,' State of California Department of Justice. Accessed: https://oag.ca.gov/privacy/ccpa

89 'A run-down of US Sen. Gillibrand's proposed Data Protection Act,' International Association of Privacy Professionals, 21 February 2020. Accessed: https://iapp.org/news/a/an-run-down-of-sen-gillibrands-proposed-data-protection-act/

90 Katherine E. Brown & Tania Saeed (2015), 'Radicalization and counter-radicalization at British universities: Muslim encounters and alternatives,' *Ethnic and Racial Studies*, vol. 38 no. 11, pp.1952–68.

91 Ibid.

92 'Prevent Strategy' HM Government, June 2011. Accessed: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

93 David Goldberg, Sushrut Jadhav & Tarek Younis (2017), 'Prevent: What is Pre-Criminal Space?', *British Journal of Psychology* Bulletin, vol. 41 no. 4, pp.208–11.

94 Interestingly, the term 'pre-crime' was coined by Philip K. Dick, author of the science fiction short story *Minority Report*. See: Goldberg, Jadhav & Younis, pp.208–11.

Prevent is focused on "providing support and re-direction to individuals at risk of, or in the process of being groomed/radicalised into terrorist activity before any crime is committed."[95] By framing Prevent as a safeguarding rather than a criminalising action, Prevent is positioned as a protective rather than a repressive programme. The effect of framing it in this way is that responsibility for operationalising Prevent falls to civic institutions. These institutions, such as universities, are obliged to anticipate, monitor and intervene in possible instances of radicalisation as part of their duty of care. It also means that employees and employers are on the lookout for an impossibly vast, complex and vaguely defined number of indicators that a person is vulnerable to radicalisation. In this environment, institutions understandably take an overly cautious approach.

In its early years, the Prevent strategy in universities focused on student communities, particularly British Muslim students. Institutions began to scrutinise lectures, speaker events and student society events in order to comply with the Prevent strategy and avoid any ambiguity as to whether extremist beliefs were being glorified on campus. There have been countless examples of Muslim students being disproportionately targeted and questioned on campus under the auspices of Prevent,[96] including a student who was referred to the University of Staffordshire's security team for reading a textbook for his postgraduate course on terrorism, crime and global security.[97] Nearly 2,500 events in around 300 universities were either cancelled or modified (for example, speakers disinvited) in 2017–18.

The picture is complicated when it comes to academic researchers who study extremism and terrorism. Exposure to extremist and terrorist content and values is far more obvious and direct, since research often includes the access and collection of terrorist and extremist content, such as official statements released by terrorist groups, terrorist propaganda (including visual media), social media posts in support of extremist views, online messageboards and so on. In particular, research with an emphasis on data collection 'from the field', such as interviews with convicted terrorists or radicalised individuals, means that the researcher is in sustained contact with individuals identified as having extremist or terrorist beliefs.

This opens up interesting questions about the nature of risk in research: can and should academic researchers be understood as vulnerable to radicalisation? What are the implications of this from legal and policy standpoints? What are the effects of this on research and researchers?

The UK's foremost pieces of counter-terrorism legislation, as it relates to researching extremism, are the Terrorism Acts of 2000 and 2006. Sections 57 and 58 of the 2000 act established the possession of materials which "give rise to a reasonable suspicion that his

95 Charlotte Heath-Kelly and Erzsébet Strausz, 'Counter-terrorism in the NHS: Evaluating Prevent Duty Safeguarding in the NHS,' University of Warwick. Accessed: https://warwick.ac.uk/fac/soc/pais/research/researchcentres/irs/counterterrorisminthenhs/project_report_60pp.pdf

96 'The Impact of Prevent on Muslim Communities: A Briefing to the Labour Party on how British Muslim Communities are Affected by Counter-Extremism Policies,' The Muslim Council of Britain, February 2016. Accessed: http://archive.mcb.org.uk/wp-content/uploads/2016/12/MCB-CT-Briefing2.pdf; Barbara Cohen and Waqas Tufail, 'Prevent and the normalization of Islamophobia,' *Islamophobia: Still a challenge for us all*, Runnymede Trust. Accessed: https://core.ac.uk/download/pdf/161895664.pdf

97 Randeep Ramesh & Josh Halliday, 'Student accused of being a terrorist for reading book on terrorism,' *The Guardian*, 24 September 2015. Accessed: http://www.theguardian.com/education/2015/sep/24/student-accused-being-terrorist-reading-book-terrorism

[*sic*] possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism,"[98] or that that information is "likely to be useful to a person committing or preparing an act of terrorism."[99] In other words, it is a crime to possess any information or material relating to extremism or terrorism, particularly if that information could aid individuals or groups in recruiting or radicalising others, or carrying out violent attacks.

The Terrorism Act of 2006 builds upon and extends the possession offences laid out in the 2000 Act to now also include the dissemination of these materials (section 1) and creates an offence for glorifying terrorism (including via the possession and dissemination of these materials; section 2). The first section refers to individuals or groups who intend to "directly or indirectly encourage or otherwise induce [others] to commit, prepare, or instigate acts of terrorism,"[100] including statements that "glorify the commission or preparation … of such acts."[101] Furthermore, any UK citizen, including researchers, are subject to these offences even when overseas.[102] In other words, a researcher could be overseas on a fellowship or conducting fieldwork and could still be charged by UK law for encouraging terrorism. The second section covers the dissemination of terrorist publications. More specifically, it criminalises the distribution, circulation, giving, selling, lending, offering, sending electronically of terrorist publications or providing services to others that enable them to obtain, read, listen to, look at, acquire, buy or borrow them.[103]

The problems this creates for academics who teach and research extremism and terrorism are clear. A lecturer who shows a video clip of Islamic State propaganda for their seminar class, for example, could be said to committing several offences: the possession of terrorist material, indirectly encouraging others to commit acts of terrorism and disseminating terrorist publications.

Indeed, the 'Nottingham Two' case exemplifies the point. In May 2008, Rizwaan Sabir, a Master's student at the University of Nottingham, was emailing his academic adviser, Hicham Yezza, to prepare his PhD research proposal on Islamic terrorism. Sabir had browsed the US Department of Justice website and downloaded a government document named 'Military Studies in the Jihad Against the Tyrants: the Al-Qaeda Training Manual' (which had been used in a legal trial to prosecute a group responsible for bombings in East Africa).[104] The document was freely available through the university's library system and can be purchased at UK high street bookshops, such as Waterstones.[105] A colleague noticed the document on Yezza's computer and reported it to the university, which notified the police. Both Sabir and Yezza were arrested without a warrant under the Terrorism Act 2000. Sabir was held for seven days in solitary confinement.[106]

98 *Terrorism Act 2000*, s.57. Accessed: https://www.legislation.gov.uk/ukpga/2000/11/section/57
99 Ibid., s.58.
100 *Terrorism Act 2006*, s.1.2 (b)(i). Accessed: https://www.legislation.gov.uk/ukpga/2006/11/section/1
101 Ibid., s.1.3 (a).
102 Ibid., s.17.
103 Ibid., s.2.
104 Rizwaan Sabir, 'Damages for my unjust "terror" arrest,' *Al Jazeera*, 21 September 2011. Accessed: https://www.aljazeera.com/opinions/2011/9/21/damages-for-my-unjust-terror-arrest/
105 See https://www.waterstones.com/book/military-studies-in-the-jihad-against-the-tyrants/anonymous/9781907521249
106 Rizwaan Sabir and Hicham Yezza were released without charge. In 2011, Sabir brought legal proceedings against Nottinghamshire Police for false imprisonment and racial discrimination, which was settled out of court. See Sabir, 'Damages for my unjust "terror" arrest'.

The 2000 act has been modified over time and in response to various political and social shifts. The first major development came in 2015 with the passage of the Counter-Terrorism and Security Act, which strengthened institutions' obligations to comply with the Prevent strategy. Universities now have a specific legal duty "to have due regard to the need to prevent people from being drawn into terrorism"[107] and requires them to have clear policies and procedures for researchers working in this area. The 2015 act operates using a risk-based approach, meaning that institutions must continually monitor and assess research activities and act to mitigate any risks these pose. In practice, many universities have now absorbed this Prevent risk assessment into their research ethics procedures.[108] Lived experience of these procedures suggests that ethics review boards have expanded a view of risk that places institutional reputation at the forefront of its concerns. The Prevent strategy could be seen to have empowered institutional review boards to mire research ethics applications – for all types of "risky, 'politically sensitive' research"[109] – in complex and slow bureaucracy in the hopes of "frustrating and deterring potential threats to an institution's reputation."[110] This, in turn, has raised serious concerns over academic freedom.

A second major shift came into force in April 2019 with the passage of the Counter-Terrorism and Border Security Act. The act extended the criminal sentences available for all offences outlined above in the Terrorism Acts of 2000 and 2006; for instance, the maximum sentence for the dissemination of terrorist publications more than doubled, from seven to 15 years' imprisonment.[111]

Four new measures in the 2019 Act crucially impact academic research on extremism and terrorism:

1. The act creates an offence of obtaining or viewing terrorist material over the internet;[112]
2. It explicitly excludes individuals carrying out journalistic work or academic research from the collection of information (including over the internet) (Section 58 of the Terrorism Act 2000) offence;[113]
3. It creates an offence for citizens to enter or remain in a "designated area" outside of the UK.[114] The Secretary of State has the authority to designate such an area on a case-by-case basis, for "the purpose of protecting members of the public from a risk of terrorism";[115]
4. It extends a section of the Terrorism Act 2006 to include the dissemination of terrorist publications as an offence outside the UK (whereas previously it covered only glorification of terrorism).

107 'Statutory guidance: Revised Prevent duty guidance for England and Wales,' UK Home Office, updated 10 April 2019. Accessed: https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales#c-a-risk-based-approach-to-the-prevent-duty

108 See, for example, 'Oversight of security-sensitive research material in UK universities,' Universities UK, November 2019. Accessed: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

109 Adam Hedgecoe (2015), 'Reputational Risk, Academic Freedom and Research Ethics Review,' *Sociology*, vol. 50 no. 3, p.495.

110 Ibid.

111 *Counter-Terrorism and Border Security Act 2019*, s.7. Accessed: https://www.legislation.gov.uk/ukpga/2019/3/section/7

112 Ibid., s.3.

113 Ibid., s.7.

114 *Terrorism Act 2000*, s.58(b). Accessed: https://www.legislation.gov.uk/ukpga/2000/11/section/58B

115 'Counter-Terrorism and Border Security Bill: Supplementary Delegated Powers Memorandum,' UK Home Office, 5 September 2018. Accessed: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739267/Supplementary-Delegated-Powers-Memo-designated-area-offence.pdf

Point 2 above – the exclusion of academics from the collection of terrorist material (including on the internet) –at first sight seems like a welcome development that reinstates academic freedom to research terrorism and extremism without fear of legal repercussions. However, a crucial point is that although academic researchers are now explicitly exempt from Section 58 of the Terrorism Act 2000 (possession of terrorist materials), there is no explicit legal protection for academics from Sections 1 (glorification of terrorism) or 2 (dissemination of terrorist materials) of the Terrorism Act 2006.[116]

What this means in practice is that academics accessing and collating extremist materials online for research or teaching would likely have a clear legal defence. However, if they excerpted these materials in journal articles or academic books, or showed them in class as examples of extremist propaganda without explicitly denouncing the groups, the researcher could find themselves in murky legal waters. Furthermore, the Terrorism Act 2000 means that researchers can be arrested without a warrant and held for 28 days while charges may be brought against them, as happened to Rizwaan Sabir and Hicham Yezza.

Similarly, researchers conducting fieldwork or data collection overseas may find themselves subject to this new legislation. If an academic was conducting fieldwork overseas, or plans to do so, in an area in which the Secretary of State declared to be a "designated area", it would be an offence to enter or remain.

Overall, the legal picture for researchers of terrorism and extremism is unclear. Although last year's legislation signals an understanding from the government that researchers will be in possession of compromising material, other legislation remains on the books to which academics very much remain subject. Legislation, policy and academia all reflect and entrench the current political climate; in this era of heightened Islamophobia and broad support for anticipatory surveillance and policing, Prevent and the Terrorism Acts very much speak to both phenomena.

An important factor to consider as we weigh up researchers' likelihood to be impacted by the UK government's counter-terrorism governance (such as the Prevent strategy) and legislation is the disproportionate effect on Muslims. "Islamist extremism" makes of 65% of all referrals to Prevent, meaning that "Muslims have an approximate 1 in 500 chance of having been referred to Prevent last year, approximately 40 times more likely than someone who is not a Muslim." Similarly, over half (54%) of terror-related arrests made in 2017 in the UK were of those deemed to have an "Asian ethnic appearance."[117] The statistical reality is that students and researchers racialised and minoritised as Muslim have been at far greater risk from being exploited – either referred to Prevent, or even criminalised – by the legal grey area.

116 "Sections 2 and 3 of the Terrorism Act 2006 also outlaw the dissemination of terrorist publications, including by electronic means, and give a very wide definition of 'terrorist publication' and 'statements' that could be construed as encouraging or inducing the commission preparation or instigation of acts of terrorism. *Academic research is not a defence under the Terrorism Act 2006* [emphasis mine]." 'Oversight of security-sensitive research material in UK universities,' Universities UK, November 2019. Accessed: https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf

117 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, financial year ending 31 March 2017,' UK Home Office, June 2017. Accessed: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619016/police-powers-terrorism-mar2017-hosb0817.pdf

To date, we have seen that Muslims have been unfairly targeted by counter-terrorism legislation on campus. However, November 2020 saw the greatest ever number of referrals relating to far-right extremism: 43%, compared to 30% for Islamist extremism.[118] This development poses interesting questions about racial profiling and research on extremism and terrorism: will non-Muslim researchers become understood as "vulnerable" and "at risk of radicalisation" for researching white supremacist terrorism? If so, what social and political responses might this trigger? A growing number of critics have come to understand Prevent and counter-terrorism legislation as a mechanism to surveil and control Muslim communities on campus and beyond.[119] If that function has now been established, what function might Prevent now play – if any?

Concluding remarks: a shifting global landscape

The ethical and legal issues facing researchers seeking to access and process individuals' data are complex and varied. In the face of fast-paced legal and political changes on both national and international scales, the global outlook for researchers working in the areas of extremism and terrorism is one of change and uncertainty.

In terms of access of data for research purposes, there is a general global trend towards strengthening data protection legislation in order to better protect individuals' data rights (with some exceptions, such as Japan above). This means that researchers are likely to be more constrained in the future with regard to the data available to them and the ways in which they can process and use this data. As corporations seek to keep abreast of a patchwork of national and supranational legislation, social media platforms need to update and alter their privacy policies consistently. Since the consequences for not doing so – seen, for instance, in the USA's Federal Trade Commission's $5,000,000,000 Facebook fine – become ever more severe, it is possible that platforms will adopt a more conservative approach to their privacy policies to ensure financial and reputational security.

At the same time, the legal and policy outlook for researchers working in the areas of extremism and terrorism is also uncertain. In the UK, a climate of anticipatory policing justified via national security threats produced a policy environment in which researchers are at risk of being criminalised for their proximity to certain material. As the 'War on Terror' progressed through the 2000s, the UK legislative context reflected a law-and-order approach to counter-terrorism, resulting in several legal developments that constrain the material that academics can access, talk about, write about, teach and publish. However, as global attention shifts away from the so-called 'Islamic threat' and towards a consciousness of violent white supremacy, the existing policy and legal frameworks that were designed to target a minority become problematic.

118 Jamie Grierson & Dan Sabbagh, 'Largest number of Prevent referrals related to far-right extremism,' *The Guardian*, 26 November 2020. Accessed: https://www.theguardian.com/uk-news/2020/nov/26/just-one-in-10-prevent-referrals-found-at-risk-of-radicalisation

119 Fahid Qurashi (2018), 'The Prevent strategy and the UK "war on terror": embedding infrastructures of surveillance in Muslim communities,' *Palgrave Communications*, vol. 4 no. 17 (2018); 'Liberty's written evidence to the JCHR's Inquiry on Freedom of Expression in Universities,' Liberty, December 2017. Accessed: https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Libertys-Evidence-to-the-JCHRs-Inquiry-into-Freedom-of-Expression-in-Universities-Dec-2017.pdf

Present mechanisms of denunciation by colleagues and peers in universities relied on racial profiling to a great extent; how will such approaches function when considering Western researchers working on the areas of white supremacy.

The nature and extent of research into extremism and terrorism in the West may change considerably given this shifting global context in the years to come. For instance, it may become harder to carry out large-scale quantitative analysis if data privacy laws and corporate privacy policies are strengthened, or to access individuals involved in terrorist groups or acts. This could mean that methodologies available to extremism researchers change, perhaps becoming more qualitatively focused, smaller scale or emphasising digital ethnography.[120] Although these shifts are alarming, considerable benefits could be gained: more intimate and nuanced encounters with extremism and terrorism that can better reflect the complexities and contradictions of individuals with extremist beliefs online.

120 See, for example: Sarah Pink et al. (eds.), *Digital Ethnography: Principles and Practice* (2015), SAGE Publications Ltd.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.