ISD | Powering solutions to extremism and polarisation

Researching the Evolving Online Ecosystem: Barriers, Methods and Future Challenges

Annex

Jakob Guhl, Oliver Marsh & Henry Tuck

About this publication

This Annex to the ISD report "Researching the Evolving Online Ecosystem: Barriers, Methods and Future Challenges" discusses ethical, legal and security risks to digital research. It outlines how ethical approaches to online research have developed and considers how approaches differ across different sectors that engage in digital research. After describing some of the legal pitfalls surrounding digital research and data collection, it discusses ISD's considerations for a range of data collection approaches and different types of online platforms that are especially relevant when researching "adversarial" online communities (e.g. violent extremists). It lastly presents a series of approaches and tools to mitigate these types of risks, including best practices for cyber-security, "digital hygiene" and Operational Security (OPSEC).

This report outlines the findings from the initial scoping phase of a project supported by a grant from Omidyar Network and launched by the Institute for Strategic Dialogue (ISD) and CASM Technology to identify online spaces used by extremist, hate and disinformation actors and communities as they increasingly move away from mainstream social media platforms. The report outlines the key barriers posed by these platforms to researching and mitigating harmful content and behaviours, and reviews existing research methodologies and tools to address these barriers. Finally, the report presents possible future scenarios for the evolving online ecosystem, and proposes a series of initial recommendations for policy-makers, platforms and the research community.

Acknowledgments:

This report would not have been possible without funding support from Omidyar Network. We would like to express our gratitude to Wafa Ben-Hassine, Anamitra Deb and Emma Leiken for their vision, continuing support and insightful feedback.

The authors would also like thank the wider project team for their contributions that have made this report possible: Francesca Visser, Jacob Davey, Lea Gerster, Daniel Maki, David Leenstra and Francesca Arcostanzo at ISD, and Nestor Prieto Chavana and Carl Miller at CASM.

Finally, we would also like to thank Eduardo Ustaran and Nick Westbrook at Hogan Lovells for their invaluable time and support in understanding the legal challenges addressed in the report.

ISD | Powering solutions to extremism and polarisation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org

Contents

Annex: Ethical Risks

As online spaces have become an integral part of social life over the past two decades, they have provided a new area of study for researchers and analysts. In academia, civil society and beyond, the emergence of online research as a distinct field has raised new discussions around online research ethics. This section outlines how ethical approaches to online research have developed and considers how approaches differ across different sectors that engage in digital research.

The Evolution of Digital Research Ethics Guidelines

The guidelines drafted by the Association of Internet Researchers (AoIR) in 2002, 2012 and 2019 provide a good starting point for tracing the development of online research ethics. In 2002, the AoIR delivered their first ethics guide posing a range of key questions to aid researchers with ethical considerations they would encounter online.[1] While the evolution of the online ecosystem into its current form has naturally resulted in a multitude of new considerations, many of the issues that were identified at the beginning of this century are still at the core of the contemporary debate on digital research ethics, including the right to online privacy, the distinction between online public and private life, and the principle of informed consent. The document included several questions that researchers may ask themselves when conducting research online.

The first of these involved determining where the research takes place and what subsequent ethical expectations have been established by the relevant online platform. In this regard, one of the difficulties is that, while many digital environments have a public character, internet interactions are often shaped by anonymity. This perceived sense of anonymity may potentially lead to individuals sharing more than they would in an offline setting. In other words, the internet has blurred the distinction between public and private life. Analysts are thus expected to consider whether the activity being researched occurs in a public or private online space. As a general rule, the 2002 AoIR guide suggested that the more public the online space, the lesser the obligation to protect individual privacy.

Secondly, inherently related, is the notion of securing informed consent from online research subjects. From 2002 onwards, it has been generally agreed that striving for informed consent is desirable as researchers are expected to respect an individual's rights to privacy and autonomy. As ethical approaches have evolved, however, there has been greater recognition that there are instances in online research where this is neither feasible nor realistic, drawing on approaches to participant observation from the field of anthropology. For example, when researchers study communities that would potentially behave differently if they were aware of the researchers' presence, or when exposing the researchers' identity could threaten their security, it may not be possible to secure informed consent and still conduct the research.

A third, important (and again connected) guiding principle is researchers' responsibility to mitigate potential harm and protect the dignity of online research subjects. The AoIR guide indicated that researchers should generally conduct a reasonable cost-benefit analysis; this should assess whether the benefit of a research project outweighs the potential risks or harms that subjects under study might suffer and mitigate these as far as possible.

To a large extent, the foundational principles of the revised 2012 framework remained the same, as it was designed around the ambition of providing an ethical toolkit that helps to protect 'fundamental rights of human dignity, autonomy, protection, safety, maximisation of benefits and minimization of harms, or, in the most recent accepted phrasing, respect for persons, justice, and beneficence.'[2] But the transformed internet landscape, characterised both by a vastly increased amount of user-generated content and the further dissolution of the private-public boundary, and facilitated by the rise of mass-participation social media networks (e.g. Facebook and Twitter), required an expanded set of considerations to complement those outlined in the first guide. For example, the increased online presence of minors heightened researchers' responsibility to secure informed consent in order to abide by autonomy and equality norms. The guide also acknowledged that the increased availability and accessibility of larger datasets also posed additional ethical questions around data storage and the feasibility of ensuring anonymity. It also touched upon questions relating to the online identities of research subjects, such as whether avatars reflect real people and whether an individual's digital information is an extension of their offline identity.

The latest edition of the guide, published in 2019, has evolved into a more extensive framework that builds on its predecessors by providing a general structure for ethical analysis during different stages of research. At the same time, it draws attention to new ethical considerations around securing informed consent in relation to big data, as well as additional considerations to ensure researchers' online and offline safety, security and well-being.[3]

Similar ethical considerations are at the core of many other academic research guidelines. For example, the Norwegian National Research Ethics Committee's A Guide to Internet Research Ethics takes ensuring the dignity and integrity of research participants as its point of departure, stressing that the accessibility of the public sphere, the sensitivity of the information, the vulnerability of the participants, and the interaction between participants and researchers should be considered.[4] Similarly, UK Research and Innovation (UKRI) lists its key pillars as minimising harm while maximising benefits for individuals, respect for dignity of people, informed consent, integrity, accountability and the independence of research.[5] Almost identical principles guide the British Psychological Society; it asks researchers to respect the autonomy, privacy and dignity of individuals; to uphold scientific integrity; to take social responsibility; and to maximise benefits while minimising harm.[6] A 2016 project entitled 'Social Media, Privacy and Risk: Towards More Ethical Research Methodologies', funded by the Economic Social Research Council and conducted by the University of Aberdeen, raises similar ethical concerns and examines the private-public distinction, informed consent, anonymity and the risk of harm.[7]

A common thread throughout these guidelines is an emphasis on the importance of continuous reflection, mutual critique and dialogue on ethical stances as it is assumed that researchers' judgements on these issues are relational and subjective. Across existing guidance, there is general agreement that it is unrealistic to work towards a universal framework or approach that incorporates all of the potential ethical considerations for online research given the variance of ethical approaches across cultures, research disciplines, and the wide range of social platforms and online spaces under investigation. For this reason, most existing guidelines argue in favour of a principle-based approach, applied on a case-by-case basis, with a focus on protecting the rights of the research subjects.

Online research ethics in practice

A key topic of ongoing discussion is how to approach the range of more public and more private spaces online. Some maintain that the ease of accessing publicly available data online does not imply that the data should not still be considered private. Others defend the notion that users have agreed with platforms' terms of service (ToS) thereby allowing third parties to access their data, including researchers where they also adhere to the relevant terms.[8] Following this line of argument, informed consent is not essential when data is publicly available. In their analysis of ISIS-supporting Twitter accounts, for example, Benigni, Joseph and Carley emphasise that they complied with Twitter's privacy policies, made no attempts to connect online and offline identities and anonymised all users in their research; 'as a result no ethics or IRB [Institutional Review Board] approval was obtained or required.'[9]

There is therefore a "grey area" in digital research ethics around publicly available, textual data like tweets, comment threads or forum discussions in public online spaces. The question is should researchers treat this type of data simply as another form of textual data akin to other published information or as more personal data inherently tied to human research participants.[10] The former approach would imply that disclosing the researchers' identities is not relevant since it is not assumed that the researchers are interacting with research participants by accessing this data. In an explorative analysis of the platform Gettr, Paudel et al argue that only publicly available data was used and the research did not depend on interaction with users in any way, so their research was 'not considered human subjects research by the IRB'.[11]

While most researchers agree that it is good practice to secure informed consent where possible, there may be instances in which exemptions are justifiable. Securing informed consent while guaranteeing anonymity may be impossible in some online settings due to the size of contemporary datasets. To address this challenge, researchers have proposed distinct ethical frameworks that reject a binary public-private approach, for example, through the so-called principle of 'contextual integrity'

of research participants where the particular norms of the relevant online space and its participants are taken into account.[12]

Researching sensitive topics such as online hate, extremism or disinformation also raises important challenges for conducting ethical online research. Lavorgna and Sugiura, who have researched online health misinformation and incel activity respectively, suggest that current guidelines insufficiently deal with challenges that arise from studying such controversial topics. They argue that, in these situations, researchers should be able to conceal their identity, to maintain their safety as well as the quality and integrity of the research by not influencing participants' behaviour.[13] They propose a flexible approach that would allow for research that is in the public interest while also taking steps to minimise any potential harm, for example, by guaranteeing research participants' anonymity and the security of their data.[14]

A similar point was raised by Maura Conway in her reflection on the ethics relating to researching online extremism. Conway states that concerns about researcher welfare have often been missing in discussions about contemporary online research ethics.[15] She argues that minimising the exposure of both researchers and research subjects to risks and harms is critical, especially in contexts when informed consent was not feasible.[16]

In their reflection on research ethics in relation to private messaging platforms like Telegram, WhatsApp and Signal, Barbosa and Milan observe that 'the field is inevitably slow at adjusting research ethics to 'upcoming' digital challenges.' It is therefore crucial to adhere to high ethical standards, consider the benefits of the research, the risks that could potentially arise for the research subjects and the responsibility that researchers have towards research subjects. They argue in favour of approaching digital ethics as a 'recursive, iterative and dialogic process' rather than a static checklist that is "ticked off" at the outset of a project. They further state that researchers should aim for a transparent research agenda and full disclosure of their identity. When 'covert' data collection is the only option, they argue that complete anonymisation and de-identification should take place.[17] This ethical challenge presents itself in cases where awareness of the researchers' presence would (adversely) affect the research subjects' behaviour, for example, when studying secretive or extremist communities.

In her analysis on gendered discourse within pro-ISIS communities online, Marie Criezis relied on data gathered from semi-private and private Telegram channels. In this case, obtaining informed consent would not have been feasible due to the secretive nature of the studied communities. Criezis states she relied on 'deception through the selection of a male name' that enabled her to enter and observe these spaces during the data collection process.[18] At the same time, she used a female account to enter female-only groups. With both accounts, she minimised active engagement. Criezis does not go into her ethical considerations in further detail, but by not disclosing account names, specific dates and other personal information about her research subjects, the anonymity and privacy of the communities under investigation were largely respected.

Semenzin and Bainotti have studied the role of Telegram in the non-consensual diffusion of intimate images using online covert ethnography. While acknowledging the varying positions regarding users' online privacy and the overall importance of informed consent, they state that 'doing covert ethnography is considered ethical when it prevents the risk of loss of the object of study and when the very success of the research depends on it'.[19] To balance the ethical concerns, they anonymised the identities of both perpetrators and victims, do not mention names and channels, and have removed in-text details.[20]

The examples above illustrate the wide range of challenges that online researchers may encounter during their research and several different approaches to research ethics in response. To guide extremism researchers, the Global Network on Extremism & Technology (GNET) outlined a set of ethical considerations in a recent report.[21] The authors of the GNET report state that processing personal data without consent is permissible in cases where the public interest outweighs the subjects' interests and cannot be achieved otherwise. The guide distinguishes between three categories of ethical considerations that researchers should be aware of: the relationship between researcher and subjects, the societal

perspective and a self-reflective dimension. The guide suggests that confidentiality must be ensured and that researchers are required to ensure no harm is done to research subjects. From a societal perspective, it states that research should serve the public interest and respect the law. Finally, researchers should always look out for their own security and make sure they operate in a trustworthy manner.

Digital ethics in journalism and civil society

Many of the ethical considerations listed above are of equal concern to civil society organisations and journalists that rely on social media and digital analysis in their work, for example, journalists providing insights into criminal organisations through undercover reporting or civil society organisations that engage in online research into extremist movements. For example, the editorial guidelines for internet research published by the British Broadcasting Company (BBC) state that, when engaging with online communities or closed social media groups, BBC journalists generally should attempt to work with the consent of administrators; however, the BBC does allow covert research methods that might involve sitting in open spaces or private groups as an acceptable approach when the outcomes serve the public interest and the data cannot be obtained in another way.[22] The scope of ethical reflection on online research for journalists previously remained rather limited, as noted by journalism scholar Heikki Kuuti in 2016. He proposes a range of ethical issues for journalists to consider when gathering online data, including assessing the origin and content of data sets, the possibility of false data, the validity of data and privacy issues.[23] Journalists reflecting on online research ethics should also refer to the traditional rules and ethics of journalistic reporting, such as striving for truth and minimising harm to those being reported on.[24] In this sense, journalists hold a more flexible approach towards digital research ethics than academics, with a greater emphasis on serving the public interest.

Academics, journalists and practitioners have all weighed in on the debate around research ethics online. Multiple civil society organisations have identified a lack of consensus and guidance around research ethics. In a collaborative effort as part of the Wisdom of the crowd project, CASM, Demos and Ipsos proposed a set of recommendations relating to digital research ethics.[25] In this report, the authors raise similar ethical issues to those debated in the academic context, including concerns that anonymity, especially when working with large datasets, cannot be guaranteed. Similarly, ethical concerns can arise where there is a discrepancy between the law and popular perceptions of how users' online data may be used. The report suggests that researchers should aim for transparency by communicating information about a research project to participants and providing the possibility to opt-out where possible. Researchers should also ensure the anonymity of participants as far as possible and carefully handle private data.[26]

Similar gaps in guidelines were pointed out in a 2021 Netgain Partnership report that explores new approaches to social media research.[27] It outlines that IRBs in academic contexts which apply principles of ethical research like risk-benefit assessments and informed consent have also tended to exempt digital research from review because it does not directly involve human subjects.[28] The report criticises this practice, noting that the 'absence of a coherent institutional approach to overseeing ethical research on social platforms has left researchers to create a patchwork of approaches, including their own appetites for legal risk.'[29] Another ethical challenge that the report highlights is the tension between social media research and rights to privacy as privacy activists attempt to protect user data from exploitation. Researchers should therefore carefully assess the privacy implications before gathering data. The authors also call for the establishment of a cross-institutional body that would bring together social media researchers from different sectors to formulate answers on questions relating to ethical research standards and practices.

Defining Areas of Ethical Risk

Based on the literature review outlined above, we have identified five key areas of ethical risk researchers may face when analysing online data. These risk areas cover the unexpected, negative consequences of unethical activity during the delivery of research. They include:

- **Respect for persons**: This means recognising the intrinsic value of human beings and researchers' obligations towards them. Specifically, this encapsulates recognising the autonomy of research

subjects, the necessity of gaining consent in research and the need to protect those with limited consent. Due to the complexity of gaining consent in online research, we have chosen to split consent out into its own discrete category (outlined below).

- **Concern for welfare**: This means researchers must be aware of the impact their presence has on any individuals and communities they are researching. It also covers concerns about the wellbeing of researchers analysing potentially traumatic content online. Specifically, this encapsulates privacy and the protection of private information, concern for the welfare of a group (e.g. looking beyond the welfare of individuals and considering the impact of analysis on a whole community), and risks to the physical, mental and spiritual health of researchers.
- **Pursuing justice**: This refers to the obligation of researchers to treat people fairly and equitably. Equity does not mean treating people the same; it means being mindful and respectful of differences and how these differences may determine the impacts of research upon them. Specifically, this encapsulates considering the inclusion criteria of communities within analysis and considering power imbalances between researchers and participants.
- **Online consent**: When conducting online research, in some circumstances, there is a practical impossibility of gaining informed consent from all individuals studied. Here the use of data should be balanced against the public benefit and importance of the research conducted. In particular, research without explicit consent must be considered, justified and documented. Efforts must be made to protect the anonymity of subjects and ensure that individual users are not identifiable in published reports. Furthermore, perceptions of privacy must be considered. In some cases, individuals may give consent to being analysed, for example, through consenting to a platform's ToS, but they may reasonably expect that their content is private, for example, through posting on certain forums.

  Analysts manually reviewing online conversation may be able to view data which is not accessible through platform API's (e.g. through monitoring comments made on groups and pages); in such cases, consideration should be given to whether researchers could be considered to have used deceptive practices to view online content (e.g. through an avatar account).

  In cases where research is of significant public interest (e.g. through analysing terrorist material), researchers may be able to justify activity which would otherwise bring with it unacceptable ethical risk. In these cases, researchers should consider the ethics of inaction (i.e. the potential risk of not conducting research into a particular online harm). Should any activity take place which is a variation from standard ethical protocol, this should be justified by the researchers.
- **Considering exploitation**: Digital research into harmful online activity like hate, extremism, terrorism or disinformation is often sensitive, subject to great interest by the general public, media and governments, and may have intelligence or security applications. In order to promote certain positions, political groups, individuals or states can exploit research findings, such as scapegoating certain groups, or the exaggeration or minimisation of a particular social problem. Authoritarian governments may use the threat of harm areas like terrorism to change laws, erode civil liberties or infringe on human rights. Accordingly, when conducting analysis into harmful online activity, consideration must be given to the way research findings or new methodologies or tools could be exploited by nefarious actors.

Considering the areas of ethical risk outlined above, we have identified specific ethical risks that could be associated with each of the research barriers outlined in this report in the table below.

Research Method	Fragmentation barriers	Ethical barriers	Technological barriers
Respect to persons	**Challenges in obtaining consent**: Outlined below in more detail under online consent. **Risks of misrepresenting research subjects**: It may be the case that, through gathering large unstructured datasets from fragmented platforms, specific users are misrepresented as being affiliated with a particular community. **Data storage and recombination**: By gathering unstructured data from fragmented platforms, there is the risk that the data could be recombined or cross-referenced with other data in ways that increase the risks, for example, if combining user data from across platforms to identify linked accounts or user identities in a way which limits their autonomy.	**Expectations of privacy**: Platforms posing ethical barriers include spaces where individuals might have a higher expectation of privacy than those operating on more public platforms. Accordingly, these higher expectations of privacy bring with them greater risks to the autonomy of individuals if they are subject to analysis.	**Imbalances in expertise/understanding of platforms**: Due to the novel nature of platforms driven by emerging technologies, individuals may not understand what data is accessible from these platforms to researchers.
Concerns for welfare	**Uncertainty in data collection**: Uncertainty around what data might be gathered from platforms posing fragmentation barriers brings with it the risk that researchers might unexpectedly gather material which negatively impacts on their wellbeing. Additionally, through gathering unstructured data from fragmented platforms, there is the risk that whole communities operating on a platform might be misrepresented. **Risks around crowdsourcing**: One option for analysing platforms posing fragmentation barriers is the use of crowdsourcing to gather data from a larger group of users and/or researchers. Such an approach, however, brings with it potential risks to the wellbeing of individuals conducting this research, for example, unexpected exposure to traumatic content which cannot be mitigated by the research institution overseeing the analysis.	**Impact on researchers**: Monitoring of platforms posing ethical barriers will likely bring with it the need for long-term, qualitative analysis of content. Should researchers be monitoring a harms area like terrorist content, this approach will intrinsically bring with it a greater risk of exposure to potentially traumatic content. Additionally, analysis in encrypted spaces where research subjects expect privacy may bring with it the increased risk of inadvertent exposure to unexpected content (e.g. sexual material). **Welfare of research subjects**: Analysis of platforms where there is a greater expectation of privacy brings with it the risk that a research subject may be exposed engaging in particularly egregious or unusual activity, which could be detrimental to their wellbeing if made public.	**Risks of immersive technology**: Exposure to harmful content in AR/VR formats has the potential to be more visceral. Consequently, it may come with greater risk of impacting on the researchers' wellbeing.
Pursuing justice		**Inadvertent analysis of minors**: In spaces that pose ethical barriers due to the existence of pseudonymous, encrypted channels, there is greater risk that researchers may inadvertently collect data on minors, heightening the risk of power imbalance. **Use of deceptive tactics to facilitate analysis**: In some instances (e.g. the analysis of potential terrorist communications) researchers may use deceptive practices, such as the use of proxy accounts, to gain access to a spaces posing ethical barriers, such as encrypted chats. In this instance, there could be a heightened risk of power imbalance between researchers and research subjects.	**Inadvertent analysis of minors**: In pseudonymous, AR/VR channels there is greater risk that researchers may inadvertently collect data on minors, heightening the risk of power imbalance.

Research Method	Fragmentation	Ethical	Technological
Online consent	**Uncertainty in data collection**: Through gathering large amounts of data from platforms posing fragmentation barriers, there is the risk that researchers may inadvertently gather personal data which is unnecessary for research purposes. Additionally, due to the fragmented nature of the data in question, it might be difficult to assess the risk of any data access before gathering said data.	**Expectations of privacy and use of deception**: Users of encrypted applications will likely have much greater expectations of privacy than those on more open platforms. Accordingly, when gaining access to an encrypted channel, it can more reasonably be assumed that researchers will be accessing data without the research subject's consent. This risk is heightened if researchers use deceptive tactics to facilitate analysis (e.g. through the use of avatar accounts). **Difficulty to assess the nature of encrypted spaces**: Gaining access to encrypted spaces for research purposes may be ethically justifiable if analysis is considered to be of significant public interest; however, making a justification for this analysis becomes more challenging if the nature of the community in question is unknown until analysis is initiated.	**Audio-visual content**: Analysing audio-visual content potentially requires more contextual data to fully understand a message, bringing with it the necessity of storing more personal data. **Analysing AR/VR content**: Exploring and analysing augmented and virtual reality brings with it the potential need for deception when accessing spaces. **Considerations around AR/VR avatars**: AR/VR avatars raise several considerations around consent, including questions around whether AR/VR personas/avatars should be considered as persons and afforded the same protections as human subjects. **Clarity and consistency of expectations of privacy in new types of online space**: Analysis of AR/VR spaces is currently in its infancy. Consequently, it is necessary to develop norms for this research and establish realistic expectations of privacy for research subjects.
Considering exploitation	**Data storage**: Gathering and sorting data from fragmented spaces brings with it the risk that the recombination of data is such that it is open to greater exploitation than in its original uncombined format.	**Exploitation of methods**: Analysis of platforms posing ethical barriers would likely require the use of avatar accounts to gain access to certain channels. There is the risk that research using these methods may be utilised to justify similar activity by more nefarious actors. **Justification of breaking ethical barriers**: Public research about harmful activity in spaces posing ethical barriers may be used by governments as a justification for breaking encryption and/or compelling companies to provide them access to these spaces.	**Issues of early access to tech under developmen**t: Analysts accessing emerging technology might have difficulty assigning ownership to data. **Lack of tried and tested safeguards for new technology**: Analysts seeking to explore new technologies may be uncertain about what types of personal data could be exposed when accessing data.

Annex: Legal Risks

Introduction

Beyond technical, ethical and security considerations, collecting data from online platforms also raises a series of legal questions, varying by jurisdictions, that researchers and their organisations should address to ensure they operate within the law and do not expose themselves to unnecessary legal or reputational risks. These legal risks apply to all online platforms that include personal user data, whether public or private, and to any research methodologies or tools that allow researchers to collect, process, transfer and/or analyse this data. As such, legal risks will need to be considered in the context of all three different types of research barriers identified in this report where access to personal data is possible.

Key questions addressed in this section include:

- What are the risks that accessing platform or user data could cause researchers to breach data protection regulations or privacy laws?
- How can researchers effectively balance privacy concerns with public interest research exemptions?
- Are political opinions or affiliations considered personal data, including for anonymous accounts, and do existing research exemptions cover this?
- What are the legal risks to scraping data from a platform and/or using their API if this breaches the platform's terms of service (ToS)?
- Which jurisdictions are relevant to consider when accessing data from online sources, and for what reasons (e.g. location of organisations, researchers, research partners and their respective servers; location of the platform and their servers; location of relevant users of the platform; etc.)?

The purpose of this annex is to provide **practical assistance** on conducting ethnographic and big data research into hate, extremism and dis/misinformation on emerging platforms in compliance with privacy and data protection laws. It also considers the effect of platforms' ToS. It outlines **the relevant legal principles**, explains **how they apply to online research activities** and provides **practical steps** to help researchers ensure that they comply with them; however, this annex should not be considered as formal legal advice, and researchers should ensure they are familiar with the specific legal requirements in the context in which they operate.

We have chosen to focus on the GDPR (General Data Protection Regulation)[30], as it is considered to be among the most comprehensive data protection laws worldwide.[i] It therefore serves as a set of best practices that, if followed, should ensure that research is conducted in a privacy-respecting manner. Researchers must, however, be aware of and follow all relevant data protection laws in the jurisdiction(s) in which they operate. It should also be noted that individual EU Member States may also have specific national provisions associated with their application and enforcement of the GDPR, and the UK has transposed the GDPR into UK law following its exit from the EU. Additionally, researchers must also be aware of and comply with other relevant organisational policies and procedures, such as research ethics guidelines, principles or processes.

Given the significant variations across different legal jurisdictions, this section does not cover legal issues relating to illegal content, defamation law or "SLAPPs" (or Strategic Lawsuits Against Public Participation). When researching smaller platforms, especially those with little or no content moderation, those that are known to host illegal content, or where it is not possible to assess beforehand whether illegal content may be encountered, researchers should be aware of the relevant laws on accessing or "possessing"[ii] illegal content in their specific contexts, and whether these include exemptions for public interest or journalistic research. Researchers should also be aware of legal risks associated with *publishing* their research, but again these laws can vary significantly across jurisdictions and are not necessarily a risk to consider when *conducting* research.

Privacy and Data Protection Laws

Relevance: Collecting and analysing information about individuals, including publicly available data from online sources, engages privacy and data protection

i Please note, all content marked with single quotation marks in this section are direct quotes from the GDPR.

ii Which can include deleted content if it is retained on a computer or server in some form, and could be restored.

laws. Breaching these laws can lead to high fines; negatively impact the reputation of researchers, or their institution or organisation; and could risk civil action by affected users.

Jurisdictions: The number of privacy and data protection laws worldwide has increased significantly in recent years. Many of these laws apply to:

- Personal data processed by organisations within the jurisdiction
- Personal data relating to individuals located within the jurisdiction

The European Union General Data Protection Regulation 2016/679 (EU GDPR) is typically seen as the "gold standard" in relation to privacy laws. Compliance with the GDPR will often, although not always, result in material compliance with privacy and data protection laws in other jurisdictions. It should also be noted that there are certain areas of the GDPR where EU Member States are able to create supplementary rules, and national regulators are the primary enforcers of the GDPR in each country. Therefore researchers working in the EU should be aware of any national variations in the relevant national contexts. The GDPR has also been incorporated into domestic UK law by virtue of the European Union (Withdrawal) Act 2018 (UK GDPR).

Because of the open nature of many online platforms, individuals who are the subject of research can be located anywhere in the world, and it is often not practical to determine their precise location. Even where it is, there will often be privacy concerns with obtaining additional information purely in order to do so. This section therefore focuses on the steps which, at a minimum, researchers must take in order to ensure compliance with GDPR requirements when carrying out their research.

Applicability: The GDPR applies to the 'processing' of 'personal data'.

- *Processing* means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'. This includes collecting personal data, storing it, sharing it and using it in any way.
- *Personal data* means 'any information relating to an identified or identifiable natural person'. This includes any expressions of opinions and even any information inferred about individuals.

The GDPR further clarifies that:

- An 'identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. social media handle or account pseudonym) or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.
- To determine whether a natural person is identifiable, consideration should be taken of 'all the means reasonably likely to be used, such as singling out, either by the controller or another person to identify the natural person either directly or indirectly'.
- To determine whether means are 'reasonably likely to be used', account should be taken of all objective factors, such as the cost and amount of time required for identification, and the available technology.

These definitions have been interpreted broadly. For example, European courts have held that dynamic IP addresses can constitute personal data in certain circumstances. In practice, much of the data collected will qualify as personal data and therefore researchers would be subject to GDPR requirements.

GDPR research exemptions: In recognition of the value of research to society, the GDPR contains limited exemptions to various requirements where personal data is being processed for the purposes of 'scientific research'. Although this term is not explicitly defined, the GDPR recognises that it should be 'interpreted in a broad manner' and that it includes 'studies conducted in the public interest in the area of public health'. Social science research carried out into online hate, extremism or dis/misinformation in line with appropriate research standards and methodologies can generally be considered scientific research for the purposes of the GDPR.

In order to ensure that these exemptions do not cause undue risks to the privacy of individuals, the GDPR

requires that processing for research purposes is subject to 'appropriate safeguards'. These are discussed further below.

Lawfulness: The GDPR requires that all processing of personal data is based on one of six 'legal bases'. In research similar to the types of research outlined in this report, the two 'legal bases' likely to be most relevant are:

- *Public interest*: This applies where processing is necessary for the performance of a task carried out in the public interest which is laid down by law. In order to rely on public interest as a legal basis under the GDPR, researchers must be able to point to a specific law which authorises particular research.
- *Legitimate interest*: This applies where there is a legitimate interest in the processing which is not outweighed by any detriment to the data subject. In order to rely on this legal basis, researchers must therefore identify the interest in carrying out the research and balance this against any risks to the research subjects.

The GDPR specifically notes that the benefits associated with research can include new knowledge about the 'long-term correlation of a number of social conditions', and that the results of research can 'provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services'. These benefits can be taken into account when researchers are performing a legitimate interest balancing exercise.

When assessing the risks to individuals, it is relevant to consider:

- Whether the personal data has been placed in the public domain by the data subject, for example, on a public message board
- Whether the user would otherwise expect that their personal data could be used for research purposes
- Whether individual data subjects will be identifiable from any published research results
- Whether the research will be used to take any particular decisions about an individual
- Whether the research is otherwise likely to cause research subjects significant distress

Considering these questions and conducting a full Data Protection Impact Assessment (DPIA) can help to determine the most appropriate legal basis and, where necessary, help to ensure that research can be carried out on the basis of 'legitimate interest' by identifying and mitigating any risks to data subjects.

The GDPR places further restrictions on the use of certain 'special category' data which is deemed more sensitive. Special category data includes data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs or trade union membership; genetic and biometric data; health data; data about sex life or sexual orientation; and criminal data. Social research into hate, extremism or dis/misinformation online often means that researchers will need to process this type of personal data, particularly data revealing political opinions, for research purposes. The GDPR allows researchers to do this as long as appropriate safeguards are applied (see below). Researchers should only collect and use special category data where doing so is necessary for their research purposes and they have applied appropriate safeguards, or otherwise as permitted by law.

Transparency: The GDPR requires that the processing of personal data is conducted in a 'transparent manner'. In particular, it requires that various information is provided to data subjects, depending on whether personal data is collected directly from them or indirectly through other means. This must include, among other things, the purposes of the research project, and the legal basis for processing (see above). Where researchers collect information other than directly from the data subject, they must also describe the types of personal data they collect and their sources.

Where researchers collect personal data indirectly, for example, through data scraping or non-participatory ethnographic methods where researchers do not interact directly with data subjects, the GDPR provides an exemption to the transparency obligations to the extent that providing the information would be impossible, involve disproportionate effort, or would undermine the objectives of the research. Factors such

as the number of affected data subjects, the age of the data and any protections used to minimise the impact on individuals can form part of researchers' rationale for not notifying. It is also relevant to consider whether the data collected is used to profile or target individuals, or merely for aggregate-level insight. Where researchers do not have the individuals' contact details, they do not need to acquire them simply in order to provide active notice.

Where this exemption applies, researchers still need to take appropriate measures to protect the individual's privacy interests, including making the transparency information publicly available, for example, by means of a website privacy notice.[iii] In order to comply with these requirements before starting a new project, researchers should check whether their existing privacy notice will cover the intended research activities and, if not, whether they must inform individuals in some other way before proceeding. Researchers should also consider whether to bring the activity to research subjects' attention. If they do not do this, they must be able to justify why doing so would be impossible, disproportionate or would undermine their research objectives.

Purpose limitation: The GDPR requires that personal data is:

> *'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'*

Processing for research purposes, however, is not considered incompatible with the initial purpose as long as appropriate safeguards are applied (see below). It is key to ensure that research activities are carried out for 'specified, explicit and legitimate purposes', and researchers must therefore clearly define their objectives at the outset of each research project.

The nature of some online research may mean that it is not always possible to fully specify research objectives in advance, for example, when researching a new online platform, space or community. This does not mean that the research cannot be carried out, but researchers should at least be able to articulate the broad goals of the research and why it is necessary to conduct initial exploratory research in order to refine those goals. Where research is exploratory in nature, researchers must articulate what unknowns they are seeking to explore in order to enable a more systematic analysis of a particular issue. Finally, where research goals evolve, researchers should update their defined research objectives.

Data minimisation: The GDPR requires that personal data is:

> *'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*

This requirement relates to:

- *The amount of personal data researchers process*: Researchers should seek to achieve their research goals with as little personal data as necessary. For example, if the objective is to investigate trends in one particular country, can researchers take steps to minimise the amount of personal data they collect about individuals in other jurisdictions?
- *The granularity of the data*: Researchers should seek to use less detailed personal data where possible. For example, do they need to know the day a particular individual was born or would the year suffice?
- *The degree of identification*: Researchers should work with pseudonymised or aggregate data where possible. For example, if the output of the research is statistical in nature, can researchers work with aggregate rather than individual level data? If individual-level data is needed, can researchers store it in pseudonymous form (i.e. by storing direct identifiers separately) as early in the research process as possible?

Complying with this requirement is particularly important in allowing research to be conducted on the basis of the research exemptions in the GDPR (see further below). Data minimisation does not prevent researchers from using systematic or "big data" methodologies in order to conduct research; however, they must be able to justify why large-scale processing of personal data is necessary in order to achieve their defined objectives.

In summary, researchers should consider at the outset

iii The required information is set out in Article 13 of 'General Data Protection Regulation GDPR', Intersoft Consulting, 2018, https://gdpr-info.eu.

of a project what personal data they will need in order to achieve their defined research objectives. Research should be structured in a manner that enables the objectives to be achieved with as little personal data as possible. Where researchers do need personal data, they should use less detailed or aggregate-level data where possible, and they must take steps to ensure they only collect and process the personal data they have identified as necessary.

Accuracy: The GDPR requires that personal data is accurate and, where necessary, kept up to date. This is generally less of an issue when researchers collect information that has been directly posted on platforms by the data subject; however, if a research project involves collecting other types of personal data from third-party sources, researchers should consider the reliability of the source, or whether the data may be out of date. As a result, researchers should only collect personal data which is up to date and from sources which they are confident (to the best of their knowledge) are reliable. While it will not always be feasible to assess the accuracy of data collected directly from platforms, researchers should take appropriate steps to ensure any data obtained from third parties is reliable.

Storage limitation: The GDPR requires that personal data is kept in a form that permits individuals to be identified for no longer than is needed for the purposes for which it is processed; however, where personal data is processed solely for research purposes, it may be held for longer periods as long as appropriate safeguards are applied (see below).

Security: The GDPR requires that organisations take appropriate technical and organisational security measures to protect personal data. Organisations should set out the security measures they implement to protect personal data in a data protection policy (or similar), as well as in any other relevant policies and procedures, such as an IT policy or staff induction process. This also applies to the security measures adopted by suppliers acting on researchers' behalf.

Researchers should comply with relevant organisational security requirements when collecting or processing personal data and consider whether the specifics of a research project mean that additional security measures are appropriate. Where researchers use suppliers to collect or process personal data on their behalf, they should ensure third parties are contractually obliged to implement appropriate security measures to protect personal data.[iv]

Data subject rights: Under the GDPR, individuals have various rights in relation to their personal data. These include rights to access the personal data held about them, to require that inaccurate data is updated, to require deletion of personal data in certain circumstances and to object to the way in which organisations process their personal data. Some of these rights are restricted in the context of processing for research purposes. In particular:

- The right to require deletion of personal data does not apply where deleting the data 'is likely to render impossible or seriously impair the achievement of research objectives'.
- The right to object to processing does not apply where the processing is necessary for the performance of a task carried out for reasons of public interest.

These exemptions may help researchers where, for example, they receive an objection from a specific individual into whom they are conducting an investigation; however, each request must be considered on a case-by-case basis, and researchers must comply with legitimate requests from individuals to exercise their rights in accordance with the GDPR and other privacy laws. Despite this, researchers are not required to obtain additional information in order to respond to a request, and therefore a user of an anonymous platform would need to reveal their identity to make such a request.

Appropriate safeguards: GDPR requires that 'appropriate safeguards' are applied to protect the interests of data subjects when processing for research purposes. These safeguards must in particular ensure that the principle of data minimisation is complied with (see above). What is appropriate will depend on each research project, and so should be considered on a case-by-case basis; however, safeguards which will often be appropriate include:

iv See the section below on "Outsourcing and data suppliers" and the subsequent annex on security risks for more information.

- Pseudonymising and anonymising personal data where possible.
- Ensuring that research is not likely to cause substantial damage or distress to data subjects (this is a required safeguard under UK law). For example, ensuring that individuals are not identifiable in published research findings may help to achieve this.
- Ensuring that research does not involve taking measures or decisions about a particular data subject (this is a required safeguard under UK law). This means that researchers should not use their findings or results in order to make specific decisions about research subjects.

In order to identify and apply the appropriate safeguards:

- Researchers must consider the potential risks to data subjects at the outset of a new project.
- Researchers must identify and implement appropriate safeguards in light of the risks they have identified.

Supplier Onboarding

When engaging suppliers, carry out appropriate due diligence.

General Questions

- How does the supplier ensure compliance with privacy laws generally?
- What steps does the supplier take to ensure the accuracy and relevance of the information it collects?

Sources

- Which sources does the supplier collect information from? Are these reputable?
- Can the supplier confirm it does not circumvent any technical restrictions (e.g. password barriers) on access to content?
- How does the supplier ensure that it does not breach the platform's ToS?

Information Collection

- Will the supplier collect "fresh" information for the research project, or will it provide researchers with access to a pre-existing database (or both)?
  - If collecting fresh information, is the supplier able to collect only specified categories of information from specified sources? Can it ensure that information about specified individuals is not collected?
  - If providing access to a pre-existing database, when was the information collected?
- Can the information collected be searched, filtered, amended, extracted and deleted at an individual level if required?

Ensure an appropriate contract is in place from the outset.

Elements that all contracts should include:

- Specify the type(s) of information to be collected, the sources of the information and the purposes for which researchers will use it.
- Assurance that the supplier has complied and will comply with all applicable laws and third-party website terms, and that it has not and will not circumnavigate any technical controls which restrict access to information.
- All legally required data processing terms, including with respect to international data transfers.

Include the following if the supplier will be collecting "fresh" information:

- State that the supplier will be a processor for the researchers' organisation.
- State that the supplier may only process and retain the personal data for the purpose of providing the contracted service.
- State that the supplier will provide all necessary assistance to enable the researchers' organisation to comply with applicable law.

Include the following if the supplier will be providing access to a pre-existing database:

- State that the parties are independent controllers of the data they process.
- State that the supplier has provided all necessary notices and obtained any necessary consents to enable researchers to lawfully use the data for the stated purposes.
- State that the supplier will provide all necessary assistance to enable the researchers' organisation to comply with applicable law.

Accountability: The GDPR requires that researchers are able to demonstrate their compliance with the GDPR. In order to achieve this, researchers need to keep appropriate documentation which enables them to demonstrate that they are meeting the necessary requirements. In addition, the GDPR requires that a DPIA is carried out for all 'high risk' processing. European regulators have stated that 'the gathering of public social media data for generating profiles' is likely to require a DPIA. The process of conducting a DPIA early on in a research project can help to spot and resolve issues ahead of time. Once completed, researchers should comply with any steps agreed to in the relevant DPIA.

Outsourcing and data suppliers: In some circumstances, researchers may use external suppliers to help carry out elements of research projects. For example, suppliers can help to collect data, or help with data cleansing or tagging. This is permitted under the GDPR, but using inappropriate suppliers can put research organisations at risk. In addition, where there is a supplier processing personal data solely on the researchers' behalf, the GDPR requires a contract to be in place which imposes specific obligations on them. When researchers plan to use suppliers, they should ensure appropriate due diligence is carried out and appropriate contractual terms are agreed with them (see below). A similar process may also be required internally within an organisation if members of the research team are based in different jurisdictions, and data would be transferred between them; however, this can often be addressed via an overarching internal agreement rather than needing a new agreement for each research project.

Platform Terms of Service (ToS)

Separate from the privacy and data protection requirements set out in laws and regulations, when researchers collect data from platforms, they should also consider any ToS imposed by the platform in respect of its use by any participants or third parties. Platform ToS set out the terms under which third parties may access and use the platform, whether by means of an API, a web browser or otherwise. Some platforms may require that third parties click to accept their ToS before they are permitted to access the platform. Other platforms may simply provide a notice informing visitors that, by accessing the platform, they are deemed to have accepted the platform ToS.

Where researchers actively agree to (e.g. click to accept) platform ToS, they will generally be entering into a legally binding contract with the platform operator. Where ToS are merely displayed as a notice, their status as a legally binding contract is less clear and may depend, among other things, on the extent to which they have been brought to researchers' attention and the applicable governing law.

Commonly encountered terms: Platform ToS will often include provisions which:

- Prohibit or limit scraping and other methods of collecting information from the platform
- Prohibit users from misrepresenting their identity
- Prohibit the circumnavigation of technical controls (e.g. password barriers) used to restrict access to information

ToS may also include third-party rights provisions and/or indemnities as discussed further below.

Potential consequences of breaching platform ToS: Where platform ToS form a binding contract between the platform operator and researchers or their organisation, any breach of the ToS by them or anyone acting on their behalf could allow the platform to claim remedies for breach of contract under the applicable law governing the contract. For example, under UK contract law this can include:

- A claim for compensation for any damages caused to the platform by a breach, subject to the duty to mitigate
- An application to court for injunctive relief, such as an order to delete the data researchers have obtained

In addition:

- If the ToS contain a third-party rights provision, it may be possible for third parties, such as platform users, to claim directly against researchers or their organisation for any damages they suffer due to a breach of the ToS.

- If the ToS contains an indemnity, researchers may be required to compensate the indemnified party or parties for any losses they incur as a debt rather than a damages claim. This means the indemnified party will have no duty to mitigate its losses.

Before collecting data from a platform, researchers should review their ToS and consider whether their intended methodology could potentially breach the terms. Where it is possible to achieve the research goals in compliance with platform ToS, researchers should endeavour to do so.

Situations where the ToS does not mention a particular use-case or activity: Where the ToS are silent about a particular activity, there will generally be no contractual bar on researchers carrying out that activity; however, researchers should ensure that they still comply with relevant data protection and any other obligations.

Summary

- Much of the data researchers collect will qualify as personal data, and the research they conduct will therefore be subject to privacy and data protection requirements.
- Researchers must determine the most appropriate legal basis for their processing. Where necessary, researchers must ensure that their work can be carried out on the basis of 'legitimate interest' by identifying and mitigating any risks to data subjects.
- Researchers must only collect and use special category data, such as data about political opinions, where doing so is necessary for their research purposes and researchers have applied appropriate safeguards, or otherwise as permitted by law.
- Before starting a new project, researchers should check whether their existing privacy notice will cover the intended research activities. They must also consider whether to bring the activity to research subjects' attention. If they do not do this, they must be able to justify why doing so would be impossible, disproportionate or would undermine their research objectives.
- Researchers should define their objectives at the outset of each research project. Where research is exploratory in nature, they must articulate what unknowns they are seeking to explore in order to enable a more systematic analysis of a particular issue. Where research goals evolve, researchers must update their defined research objectives.
- Researchers should consider at the outset of a project what personal data they will need in order to achieve their defined research objectives. They must structure their research in a manner which enables them to achieve their objectives with as little personal data as possible. Where researchers do need personal data, they should use less detailed or aggregate level data where possible. They must take steps to ensure they only collect and process the personal data identified as necessary.
- Researchers should only collect personal data which is up to date and from sources which they are confident to the best of their knowledge are reliable.
- Researchers should comply with any organisational security requirements when collecting or processing personal data. They must consider whether the specifics of a research project mean that additional security measures are appropriate. Where researchers use suppliers to collect or process personal data on their behalf, they must ensure any third parties are contractually obliged to implement appropriate security measures to protect personal data.
- Researchers must comply with any requests from individuals to exercise their rights in accordance with the GDPR and other privacy laws.
- Researchers must consider the potential risks to data subjects at the outset of a new project, and they must identify and implement appropriate safeguards in light of the risks they have identified.
- Determine if a Data Protection Impact Assessment (DPIA) is required and/or has already been conducted. Once completed, researchers must comply with any steps agreed to in the relevant DPIA.
- When researchers plan to use external suppliers, they should ensure they carry out appropriate due diligence and agree clear and appropriate contractual terms with them.
- Before collecting data from a platform, researchers should review the platform's ToS and consider whether the intended methodology could potentially

breach its terms. Where it is possible to achieve the research goal in compliance with the platform's ToS, they should do so. Where this is not possible and researchers decide to go ahead with their proposed methodology, they could potentially face legal action from the platform in question.

Annex: Security Risks

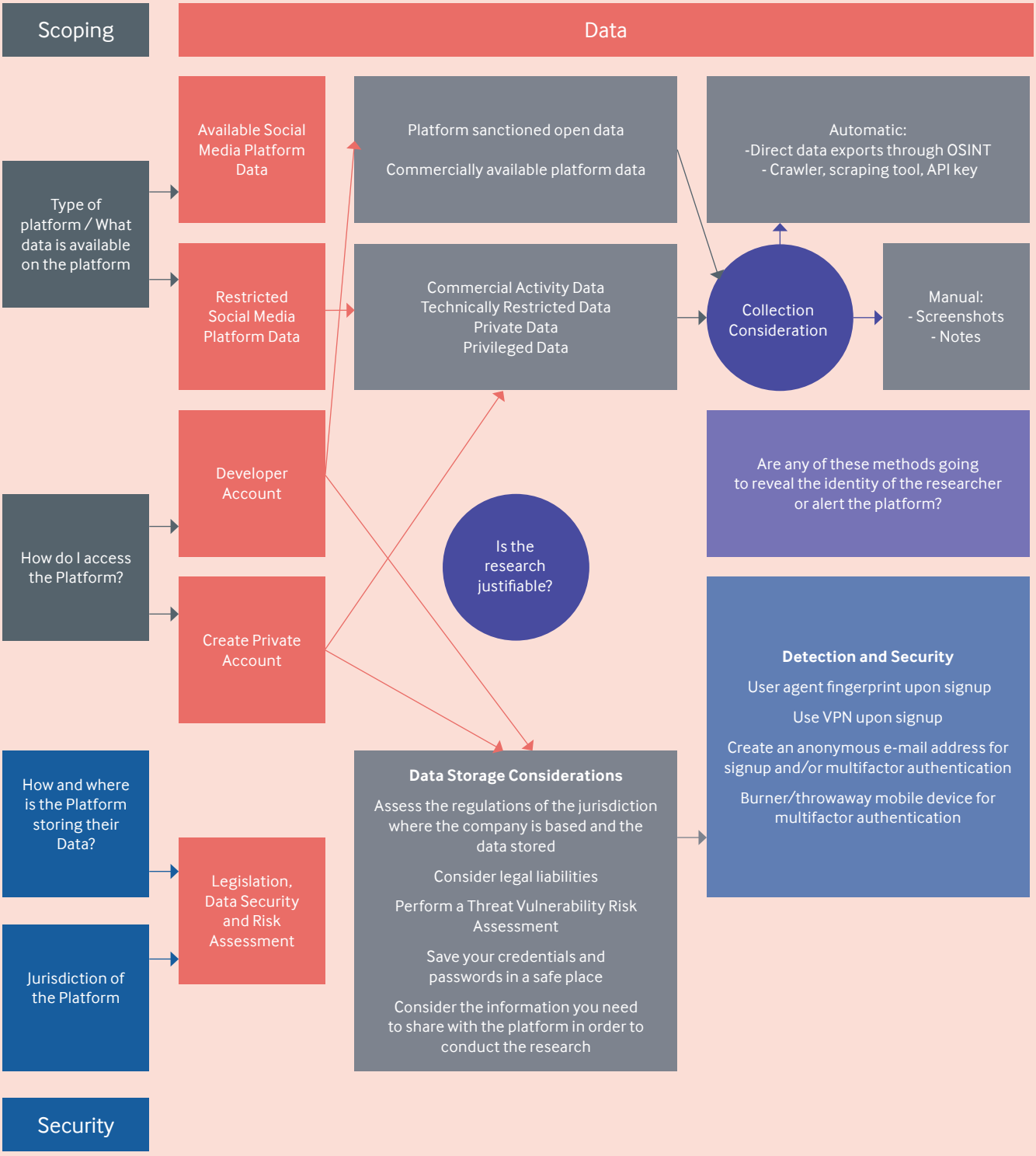
Conducting research on new social media platforms should always be preceded by an assessment of security risks alongside ethical and legal risks. This section outlines key security considerations for a range of data collection approaches and different types of online platforms that are especially relevant when researching "adversarial" online communities (e.g. violent extremists). It includes a series of approaches and tools to mitigate these types of risks, including best practices for cyber-security, "digital hygiene" and Operational Security (OPSEC). While this section focuses primarily on online risks, in a worse-case scenario, these online risks could lead to offline risks that might impact the physical safety and security of researchers and organisations; consequently, these are also included in brief.

The decision tree below is meant to guide researchers and organisations who are considering starting social media research and intelligence collection through a series of steps to guarantee the integrity, security and safety of the research and those conducting it, especially when researching a new platform or implementing new methodologies. The decision tree represents the various stages that should be taken into consideration. During the scoping phase of a research project, it is recommended that researchers consider the questions outlined below. Depending on the platform, its level of data access, its jurisdiction, and the storage of its data, researchers may be exposed to different risks. The top half of the decision tree showcases the different data access and data collection considerations (further discussed below). The bottom half of the decision tree displays the legal and security implementations that should be considered when conducting the data collection.

The overall security risks and consequences for researchers and their organisations are:

- **Detection of IP address**: If an IP address is detected, researchers can risk being banned from a platform. Moreover, if research was conducted on platforms catering to extremist groups, or tied to authoritarian or adversarial states, this could lead to a counter hack which would pose a security risk for the organisation and/or individual researchers.
- **Breaches of personal data**: Researchers' personalised information can be disclosed during the research. This can lead to information of researchers and their organisations being doxxed, putting them at risk of physical and mental harm (e.g. via online and/or offline abuse or harassment). Additionally, there is also the risk of collected platform user data being breached. This would present similar risks to the subjects of the research, especially when researching sensitive topics like hate, extremism or dis/misinformation.
- **Breaching laws and regulations**: While legal risks are covered in more detail in the previous section, if digital research is conducted without sufficient consideration for security risks, then researchers may also risk contravening relevant laws and regulations in the jurisdiction in which they operate. This could result in legal exposure to researchers, organisations and, potentially, subjects of the research (for example, if collected data were to be breached and shared publicly) from users, platforms, regulators or even law enforcement. Researchers should also be aware of the potential security implications in jurisdictions where laws may be in place that could force the seizure of data or even the detention of researchers or research subjects.

Figure 1: Security Risks Decision Tree



Data access

Different considerations need to be made based on the kind of data researchers want to access. Based on a definition by Shapiro et al,[31] we can divide data into two main groups:

- **Available social media platform data** (e.g. content posted in public groups on Facebook or public posts on Twitter)
- **Restricted social media platform data** (e.g. content posted in private groups on Facebook or messages posted in group chats on WhatsApp)

Available social media platform data is openly accessible and can be of two types: platform sanctioned open data, including public data; and commercially available platform data. The first kind of data is generally accessible through APIs that allow retrieval from a given social media platform's servers. APIs can be provided directly from the platforms and accessed through a developer account (and researchers may might be required to provide a detailed explanation of the project in order to gain access). In other cases, an API can be designed by external developers and then downloaded and applied in scripts.[v] Commercially available platform data can also be easily accessed through permission-based tools like CrowdTangle, which allows users to retrieve public data from Facebook in a structured way. Such commercially available tools are often created for marketers and advisers in order to provide certain types of social media data to subscribed users.

Access to restricted data implies ethical, legal and technical considerations based on the kind of restrictions in place. Restricted data can be divided into four main categories:

- **Commercial activity data**, which is generally only accessible to researchers employed by the platforms or for marketers in order to guide ad targeting
- **Technically restricted data**, such as data protected by encryption
- **Private data**, such as private messages or posts published in private groups
- **Privileged data** (i.e. sensitive data which is shared with the company and protected by contract)

Commercial activity data is currently not available to external researchers for scrutiny; however, technically restricted and private data can theoretically be accessed by researchers who join the closed groups or chats of interest (i.e. using ethnographic research methodologies). This step might require using deception and should be preceded by careful considerations of ethical risks, for example whether it is justifiable, proportionate and necessary. Only if these two considerations are answered affirmatively should researchers proceed to safety and security considerations in conducting covert research. Privileged data can be made public to legislative, regulatory and oversight committees as part of their mandates; produced during the discovery process in litigation; or made available to researchers in special circumstances and with limitations on its use (e.g. under non-disclosure agreements and with publishing restrictions).

Creating an account

Conducting social media research might require the use of an account to access a platform. The nature of this account would depend on the type of data to be gathered. When obtaining data from a specific platform can be done openly and no covert intelligence collection is necessary, researchers might want to use their own account or the organisation's account; however, it is more often the case that, primarily due to safety considerations, researchers may want to conduct their research without leaving "footprints". In that case, the creation of a new account is recommended.

Accounts to conduct research can be of three types: an already existing account; a developer or bot account; or a "sock puppet" account. When the research can be conducted in an automated way through an API or through the creation of a bot account, researchers may be required to share information about the nature of the research and about their organisation. Based on the platform, its jurisdiction and its ownership, researchers should be aware of the risks of sharing this information.

If it is the case that a given research project or exercise needs to remain covert, researchers would need to create

v Although third-party APIs may break a platforms' terms of service – see Annex: Legal Risks

a new account. In order to maintain the anonymity of such an account, the following OPSEC measures should be considered:

Risk Avoidance	Solution
Ensure a user-agent switcher or other browser anonymisation tools is used when signing up for an account on a given site/network in order to reduce the risks of researchers' computers being compromised through browser detection.	User Agent Switcher
Ensure that the personal IP Address is not recognised by providers by using a VPN upon sign-up.	VPN
Ensure the researcher's private information (e.g. private and work email addresses) is not connected to the sites being explored.	Create an anonymous email address for multi-factor authentication (when required).
Ensure that researchers are not directly linked with covert operations or automatic data collection.	Use a "burner" mobile device for multi-factor authentication (when required). With cash, buy a mobile device and a sim-card that do not need to be registered with identification.
Avoid uploading a real picture of the researcher when required for authentication. AI-generated images can be used for face identification. Alternatively, a stock image if fake image recognition is not needed.	Generated Media's AI face-generator
Reduce the risk of malware from accessing unknown content by analysing URLs, IPs and domains before accessing them in order to detect malware and other breaches.	VirusTotal

Data collection considerations

Once researchers are ready to collect the data, a new set of considerations need to be addressed. A risk assessment should always precede data collection and the following questions need to be assessed:

- Is the collection of data ethical and legal? And if not, can this be justified?
- Where is the data going to be stored?

Regardless of whether the data will be collected manually or automatically, the risks of collecting and storing data should always be assessed beforehand. Data that is collected manually should be stored safely, and researchers should be aware of the risks that could result from the disclosure of that data. Data that is collected automatically raises additional concerns, the first being whether the method used could automatically reveal the identity of researchers or alert the platform; this risk can be mitigated by limiting the volume of crawls or calls (i.e. requests for data) that the tool makes at any one time. A second concern is whether the platform requires further information about the research to authorise collection. In some circumstances, a limited number of crawls can be made without needing to share information about the research, but when informing the platform is inevitable, researchers should be aware of the threats that can result from sharing sensitive information about their organisation or about the subject of study.

An additional consideration, as with manual data collection, is where the data should be stored. When the storage of the data is outsourced to a third party, it is crucial to know in what country and where the company is storing the data as well as the regulations for that specific jurisdiction; who has access to the database and who can request access; and what the company's security posture is? To mitigate the risks connected to data storage, a Threat Vulnerability Risk Assessment (TRVA) is recommended. This assessment needs to take into consideration threats derived from sharing data with a particular company as well as dangers of the exposure to researchers and/or organisations should others be alerted to the research. Finally, researchers should be aware of the risks associated with accessing unknown files and opening unknown links. This risk can be mitigated by scanning all content before access with antivirus software or tools designed to detect malware.

Annex: Platform-Scoping Data – Link Counts

	English		French		German	
Rank	Platform	Links	Platform	Links	Platform	Links
1	Facebook	75,210	Facebook	133,774	Telegram	69,256
2	Twitter	47,564	YouTube	16,623	YouTube	47,369
3	YouTube	47,559	Twitter	1,904	Telegra.ph	12,727
4	Reddit	24,200	WhatsApp	1,421	Twitter	10,791
5	Telegram	23,407	Odysee	1,187	DLive	2,999
6	Rumble	5,008	Google Sheets	982	Odysee	2,816
7	BitChute	4,151	Telegram	909	Facebook	2,407
8	Odysee	1,423	BitChute	356	Querdenken-711	1,900
9	Gab	797	LinkedIn	354	BitChute	1,629
10	Parler	401	MediaFire	283	Rumble	1,623
11	Bitly	293	Dailymotion	241	veezee.tube	1,240
12	DLive	262	SoundCloud	228	Instagram	1,137
13	BrandNewTube	236	Discord	181	Wtube	765
14	VK	207	osini.co	180	Kla.tv	697
15	Discord	201	Tipeee	174	Trovo	428
16	Minds	175	VK	171	Twitch	350
17	Telegra.ph	158	Eventbrite	165	Vimeo	345
18	Gettr	137	Change.org	161	BitTube	331
19	Twitch	131	MesOpinions	155	VK	307
20	Trovo	120	Linktree	137	Youmaker	295
21	MeWe	119	Bitly	113	Gettr	237
22			Spotify	103	Gab	202
23			Google Play Store	99	Frei3	157
24			Vimeo	95	Parler	139
25			Show2babi	86	Brighteon	114
26			Mixcloud	86	Spotify	112
27			Patreon	83	TikTok	100
28			smaack.me	80	OKiTUBE	70
29			LBRY.tv	79	WirTube	61
30			Apple Music	74	telesco.pe	57
31			stickytickets.com	64	Gegenstimme.tv	55
32			Twitch	59		
33			Rutube.ru	58		
34			helloasso.com	56		
35			Streamable	50		

Methodological Notes

ISD compiled the above list of platforms and apps referred to by different harmful communities in 2021 in order to identify new and emerging platforms.

To conduct this analysis, ISD used a "seed list" with actors and communities on Facebook, Instagram, Twitter, YouTube, Reddit, 4chan, Telegram and Gab. This list was gathered from previous research projects on disinformation, hate and extremist groups in French, English and German. These datasets, compiled in 2021, included lists of actors and groups that were found to have spread disinformation and conspiracy theories about COVID-19 and vaccines, and/or to have participated in far-right extremist or antisemitic activities.

As the datasets were drawn from recent but distinct projects, the date range and sizes were varied. The English data included 2.5 million posts between 1 January 2021 and 30 November 2021. The German data included 659,000 posts between 1 January 2021 and 12 September 2021. The French data included 2 million posts between 31 July 2020 and 31 January 2021.

As detailed in the table above, ISD was able to use these datasets to identify any links to other platforms shared in these groups.

Endnotes

1 'Ethical decision-making and Internet research', Association of Internet Researchers, November 2002, https://aoir.org/reports/ethics.pdf.

2 'Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)', Association of Internet Researchers, 2012, https://aoir.org/reports/ethics2.pdf.

3 'Internet Research: Ethical Guidelines 3.0', Association of Internet Researchers, 2019, https://aoir.org/reports/ethics3.pdf.

4 'A Guide to Internet Research Ethics', The Norwegian National Research Ethics Committees, May 2019, https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.

5 'Framework for Research Ethics', UK Research and Innovation, August 2021, https://www.ukri.org/councils/esrc/guidance-for-applicants/research-ethics-guidance/framework-for-research-ethics/relevant-ethics-terms-and-conditions/#contents-list.

6 'Ethics guidelines for internet-mediated research', The British Psychological Society, 7 June 2021, https://www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research.

7 Townsend, Leanne and Wallace, Claire, Social Media Research: A guide to Ethics, The University of Aberdeen, 2016, https://www.gla.ac.uk/media/Media_487729_smxx.pdf.

8 Ibid.

9 Benigni, Matthew C., Joseph, Kenneth and Carley, Kathleen M., 'Online extremism and the communities that sustain it: Detecting the ISIS supporting community on Twitter', PLoS ONE, 12(12), December 2017, https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0181405&type=printable.

10 Rambukkana, Nathan, 'The Politics of Gray Data: Digital Methods, Intimate Proximity, and Research Ethics for Work on the "Alt-Right"', Qualitative Inquiry, 25(3), January 2019, p. 313, https://journals.sagepub.com/doi/abs/10.1177/1077800418806601.

11 Paudel, Pujan et al, 'An Early Look at the Gettr Social Network', arXiv:2108.05876, August 2021, https://arxiv.org/abs/2108.05876.

12 Zimmer, Michael, 'Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity', Social Media + Society, 4(2), May 2018, p. 7, https://journals.sagepub.com/doi/full/10.1177/2056305118768300.

13 Lavorgna, Anita and Sugiura, Lisa, 'Direct contacts with potential interviewees when carrying out online ethnography on controversial and polarized topics: a loophole in ethics', International Journal of Social Research Methodology, 25(2), 2020, p. 2, https://www.tandfonline.com/doi/full/10.1080/13645579.2020.1855719.

14 Ibid., p. 6.

15 Conway, Maura, 'Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines', Terrorism and Political Violence, 33(2), March 2021, https://www.tandfonline.com/doi/full/10.1080/09546553.2021.1880235.

16 Ibid., p. 372.

17 Barbosa, Sérgio and Milan, Stefania, 'Do Not Harm in Private Chat Apps: Ethical Issues for Research on and with WhatsApp', Westminster Papers in Communication and Culture, 14(1), 2019, https://www.westminsterpapers.org/article/id/274/#B80.

18 Criezis, Meili, 'Many Sisters Wish They Were Men': Gendered Discourse and Themes in pro-ISIS Online Communities', Journal for Deradicalization, 25, Winter 2020/21, https://journals.sfu.ca/jd/index.php/jd/article/view/409/251.

19 Semenzin, Silvia and Bainotti, Lucia, 'The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities', Social Media + Society, 6(4), December 2020, p. 5, https://journals.sagepub.com/doi/pdf/10.1177/2056305120984453.

20 Ibid.

21 Sold, Manjana and Junk, Julian, 'Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities', Global Network on Extremism & Technology, 2021, https://gnet-research.org/wp-content/uploads/2021/01/GNET-Report-Researching-Extremist-Content-Social-Media-Ethics.pdf.

22 'Guidance: Internet Research', BBC, 2019, https://www.bbc.com/editorialguidelines/guidance/internet-research/.

23 Kuutti, Heikki, 'Ethics of data journalism: Four ethical phases in the working process', University of Jyväskylä, 2016, https://jyx.jyu.fi/handle/123456789/58616.

24 McBride, Rebekah, 'Giving data soul: best practices for ethical data journalism', DataJournalism.com, 31 August 2017, https://datajournalism.com/read/longreads/giving-data-soul-best-practices-for-ethical-data-journalism.

25 Evans, Harry, Ginnis, Steve, Bartlett, Jamie, '#SocialEthics: a guide to embedding ethics in social media research', Wisdom of the crowd, 12 November 2015, https://www.ipsos.com/sites/default/files/publication/1970-01/im-demos-social-ethics-in-social-media-research.pdf.

26 Ibid.

27 Shapiro, Elizabeth Hansen et al, 'New Approaches to Platform Data Research', Netgain Partnership, February 2021, https://drive.google.com/file/d/1bPsMbaBXAROUYVesaN3dCtfaZpXZgl0x/view.

28 Ibid., p. 44.

29 Ibid., p. 45.

30 'General Data Protection Regulation GDPR', Intersoft Consulting, 2018, https://gdpr-info.eu.

31 Shapiro et al, op. cit.

ISD | Powering solutions to extremism and polarisation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org