"*Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*".

Chapter title: ***Ethical Approaches to Studying Cybercrime: Considerations, Practice and Experience in the UK.***

Authors

Brian Pickering is a Senior Research Fellow in the School of Electronics and Computer Science, University of Southampton, carrying out research into online behaviours and the acceptance of technology. Using mainly qualitative research methods, he investigates trust relationships and online group formation. Further, as part of application and technology evaluation, he focuses on how potential adopters and users create narratives with technology embedded as a predictor of technology acceptance rather than more traditional models in domains from healthcare to cybersecurity. https://orcid.org/0000-0002-6815-2938

Silke Roth Dr Silke Roth is Associate Professor of Sociology in the Department of Sociology, Social Policy and Criminology at the University of Southampton (UK) and Chair of the Faculty Research Ethics Committee of the Faculty of Social Sciences. She is the author of Paradoxes of Aid Work and is particularly interested in questions of solidarity, inclusion and exclusion. This includes a critical assessment of the impact of information and communication technologies (ICT) on aid relationships (ICT for development/ICT4D, digital humanitarianism). Her article 'Deconstructing the Data Life-Cycle in Digital Humanitarianism' challenges an optimistic view on digital humanitarianism and ICT for development and highlights how Big Data and ICT reproduce Global inequalities. She recently co-edited the e-special Digitizing Sociology. Continuity and Change in the Internet Era" for Sociology https://orcid.org/0000-0002-8760-0505

Craig Webber is Associate Professor in Criminology within Sociology at the University of Southampton, carrying out research into the intersection of criminological, sociological and psychological insights on cybercrime, youth crime and criminological theory. Dr Webber has been a key member of the Web Science Institute at the University of Southampton since its inception. Dr Webber has written on various aspects of cybercrime including online fraud called carding and hacktivism. https://orcid.org/0000-0003-3900-7579

Abstract Traditional normative ethics focuses on doing what is right as agreed by the community at large. For society as a whole, this is likely the protection of property and the safety of individuals, making the criminal a justifiable target of law enforcement and research. For criminals themselves, loyalty to fellow criminals may take precedence instead. Similarly, as research ethics introduce imperatives such as ensuring the rights and expectations of research participants are respected, informed consent, and anonymity,

it is unclear where these rights apply. A criminal in a research study is unlikely to give consent but expect anonymity. Yet have they intentionally waived such rights by committing crimes? In this chapter, we explore the ethical challenges related to research into cybercrime and how this relates to normative approaches, including a critical evaluation of guidance from social science professional associations. We conclude with a set of recommendations to researchers of cybercrime. [150 words]

Words for indexing purposes Research Ethics; Normative expectations; Online context; Informed consent; Privacy

Chapter title: ***Ethical Approaches to Studying Cybercrime: Considerations, Practice and Experience in the UK.***

[4,977 Words]

Introduction

Over the last few decades, more and more life-spheres have been digitalised, from commercial interactions such as retail and banking, to civic life, leisure and social behaviours. These developments offer opportunities for criminal activities in cyberspace. Some commentators see the emergence of cybercrime as nothing more than the Internet-enabled equivalent of what we already know (Grabosky, 2001). Others have identified not only an online version of offline criminal activity, but developing new types (Wall, 2001, 2007). Furthermore, some have argued that cybercrime can only be understood as an activity that 'drifts' on and off-line, making ethical considerations complicated by the shifting locus of action (Webber & Yip, 2012). Understanding if and how this cyber landscape differs from what is already known is essential if law makers and law enforcers are to be able to provide effective measures to protect society. It falls to the research community through its work to inform this process.

Researchers based at UK universities and research institutions who conduct research involving human participants, animals, and sensitive research in general are required to seek ethics approval when they have drafted their research protocol. The ethics review process encompasses

all stages of the research lifecycle, from the recruitment of participants and collection of data, to data analysis, data storage, and the dissemination of research findings. Research Ethics Committees (RECs) or Institutional Review Boards (IRBs) are responsible for providing training and guidance and for reviewing submissions. Principles of ethical research concern preventing harm to research participants and researchers as well as the reputation of research institutes and disciplines. Potential harm must be carefully assessed, avoided, mitigated and – if deemed unavoidable – justified. The Belmont Report (Belmont, 1979) sets out common principles such as autonomy, respect, benevolence, non-maleficence, and equanimity. In many ways, though, these are ideals. What is more, although broadly in line with these ideals, different committees may well vary in their practical interpretation and application. Reviewing how these ideals relate to cybercrime research and how different institutions apply theme is one goal of this chapter.

Important aspects of ethical research include informed consent and confidentiality, therefore. For most studies, this means that research participants are informed about the aims of the study and on this basis consider the risks of taking part. Hence the concept of *informed consent*. These general principles for ethical research are a good starting point, but changes in society's views, in the affordances of technology, and what constitutes ethical research in different domains require a more nuanced approach. The focus of this chapter is to review how these principles are applied and develop recommendations for what needs to be considered when dealing specifically with cybercrime research.

Ess (2002),Markham and Buchanan (2012) and most recently franzke, Bechmann, Zimmer, Ess, and the Association of Internet Researchers (2020) (AoIR) stress that ethical guidance must be contextualised to the different online environments. RECs/IRBs and Professional Associations may need new guidance on how to evaluate research protocols submitted for review. For the

cybercrime environment, though, it is unclear who the human participants should be. On the one hand, collaborative networks of criminals (Yip, Webber, & Shadbolt, 2013) involve multiple actors. On the other, risk-taking researchers become part of the cybercrime network they study (Decary-Hetu & Aldridge, 2015; see also Latour, 2005). Further considerations concern deception and informed consent, which could be justified under specific circumstances.

In this chapter, we begin with a brief overview of the typology of cybercrimes to provide a context within which to gauge impact on the various actors. This is important for research ethics since this enables ethics reviewers to judge the potential research benefit versus the burden on researchers and participants. These ethical principles are then applied to assess the effects on the main actors involved with cybercrime in connection with the cybercrime components we have identified. This offers an opportunity to critically evaluate existing guidance and to identify additional recommendations for researchers in this area.

Researching Cybercrime

Advances in technology, especially the pervasive reach of the Internet, has many benefits (Chopik, 2016; Hoser & Nitschke, 2010; Norman, 2010). However, this comes at a cost (O'Neil, 2016; Turkle, 2017), not least in terms of individual privacy rights (Michael, McNamee, & Michael, 2006). This duality surrounding the impact of technology has motivated an extension in research ethics thinking Floridi (2002). Ethical behaviour is regarded as contributing to the overall wellbeing (or 'entropy') of a complex network of agents and objects (the 'infosphere'). Applying this to cybercrime, the contention between individual rights and public benefit has been understood for some time (Barratt, Ferris, & Winstock, 2013; Decary-Hetu & Aldridge,

2015; Holt & Bossler, 2014; Holt & Lampke, 2010). In this section, we provide an overview of cybercrime in the context of the ethical challenges it poses.

Typology of cybercrimes

There have been several attempts to classify the types of online crimes in recent years (Holt, 2016; Koops, 2010; Sabillon, Cano, Cavaller Reyes, & Serra Ruiz, 2016; Wall, 2001), suggesting cyberspace has provided new opportunities for criminal activity to be sanctioned appropriately (Upadhyaya & Jain, 2016). Grabosky (2001); (2014) sees cybercrime as little more than an online version of existing types crime, whereas Holt and Bossler (2014) and Crown Prosecution Service (n.d.) include both traditional crime moving online and exclusively online activities. By contrast, Wall (2004) and subsequently (Bossler & Berenblum, 2019) identify traditional crime with cyber elements as distinct from cybercrime that solely exists online. For the current discussion, Wall's original typology (2001) summarised in Table 1 provides a useful starting point for this discussion.

Table 1: Typology of Cybercrime after Wall (2001)

Type	Brief Summary	Perpetrator(s)	Victim(s)	Impact
Cyber-trespass	Gaining access to property or assets without the owner's permission	Individual hackers; Organised groups (scammers)	• Individual targets • Institutions	Loss of privacy and integrity; potential breaches
Cyber deception and theft	Related to the above, taking possession of information or assets	Hackers / Scammers	• Individual targets • Institutions	Individual financial loss; loss of trust; economic loss to institutions; possible fines for institutions
Cyber-porn and obscenity	Access and sharing of indecent content	Organised groups; individuals	• Those depicted • Those in receipt	Individual distress (for anyone shown in content); socially unacceptable
Cyber-violence	Computer-mediated violence (bullying) or incitement	Organised groups; individuals; 3rd party states	• Individual targets • Political integrity • Society	Individual distress; Social disruption; Political extremism

Koops (2010) offers a slightly different classification, based on the Council of Europe's Cybercrime Convention which may easily be mapped to Wall's. The importance of such classification in terms of ethics is the implications for the researcher. Firstly, with multiple victims and/or perpetrators, which of research participant rights take precedence? But in addition, where there is no direct, individual victim such as attacks against infrastructure (Martin, Ghafur, Kinross, Hankin, & Darzi, 2018), should the assessment of impact be scaled up since more people are affected, or differentiated along the lines of personal *versus* economic effects? Similarly, if there is no single perpetrator but rather a group or network, do we need to consider the dynamics of that network and how individuals respond to group membership (Vilanova, Beria, Costa, & Koller, 2017)? What is more, whether individual or networked, is it appropriate for researchers to engage directly with cyber criminals? The answers to these sorts of questions will affect how we assess and review ethical research. One final observation: the pervasive nature of the Internet allows cybercriminals to transcend jurisdictional boundaries. This alone introduces additional complexity for research in this area.

Network of actors

Collaboration between criminal actors is well-established in the offline world, including youth gangs, organised crime groups and cross-border organisation (Aas, 2013). Cyberspace, however, is a unique system for facilitating collaboration and provides the means for various different forms of task-delegation, for example it offers opportunities such as "crime-as-a-service" (Decary-Hetu & Aldridge, 2015: 123), where *ad hoc* relationships can be formed for specific activities or transactions (Grabosky, 2014; Lusthaus, 2012, 2018a, 2018b; Lusthaus & Varese,

2017; Yip et al., 2013). Carding fora, for example, display the kinds of relationship mechanisms, such as trust and reputation, found in offline collaborative networks (Holt & Lampke, 2010; Hoser & Nitschke, 2010; Webber & Yip, 2020). Not all actors within the network may be committed criminals, but also private individuals looking to make difficult or illegal purchases (Barratt et al., 2013; Sugiura, 2018). For the researcher dealing with networked activity has implications not least in seeking consent from research participants (Beaulieu & Estalella, 2012; Lusthaus, 2018b; Sugiura, Wiles, & Pope, 2017), but also in their relationship with the network under study (Sugiura et al., 2017; Yip et al., 2013).

Where does the researcher fit?

Awareness of potential interlopers amongst online criminals (Holt & Lampke, 2010; Yip et al., 2013) leaves the cybercrime researcher in an equivocal position. It has been well attested in various domains that making yourself known may not always be welcome (Beaulieu & Estalella, 2012; Holt & Lampke, 2010; Lusthaus, 2018b; Sugiura et al., 2017). Specifically for cybercrime, it may well be inadvisable to identify themselves and risk retribution (Decary-Hetu & Aldridge, 2015; Lavorgna, Middleton, Pickering, & Neumann, 2020). Some researchers as well as cybersecurity experts will deliberately target the practices of cybercriminals exploiting the very vulnerabilities that the criminals use themselves (Spitzner, 2003a, 2003b). How ethical such practices are is not easy to determine. On the one hand, there is the societal effort to prevent and protect against crime; on the other, controlling it online may prevent the offline consequences (Pastrana, Thomas, Hutchings, & Clayton, 2018). Ultimately, the researcher has to understand and obey the rules of the networked group they observe (Flick, 2016; Hoser & Nitschke, 2010; Markham & Buchanan, 2012; Yip et al., 2013), including differences between the clear and dark web. Finally, there is evidence of trauma for those exposed to various offences (Burruss, Holt, &

Wall-Parker, 2018), including a displaced feeling of obligation to help remote victims (Lee, 2017). Researchers need to consider their own emotional well-being, therefore, depending on the research they undertake.

Ethics Landscape

Despite individual differences in definition, normative approaches to ethics stress duty or morally acceptable action (Kagan, 1992). This may be in terms of an actor doing the right thing (deontological), of the desirability of the outcome (utilitarianism), or more specifically, the equitability of outcomes (Rawls' theory of justice) (franzke et al., 2020; Parsons, 2019). When associated with cybercrime, however, many issues arise. Can Australian law enforcement taking over a paedophile site and not shutting it down immediately be justified on utilitarian grounds (Safi, 2016)? Similarly, can online drug markets be justified based on keeping drug-related violence off the streets (Pastrana et al., 2018)? In one of the few references to regional differences, Ess (2002) observes that ethics in the US tends to be utilitarian by nature seeking the best for the common good. By contrast, he claims, Europe is broadly deontological, stressing the rights of the individual. In general, research ethics calls for respect for research participants, equanimity in outcomes, and optimising benevolence and non-malevolence (Belmont, 1979). Where there are multiple actors, including multiple private individual and institutional victims (see Table 1), it is not always clear how impact (benevolent or otherwise) should be balanced across actors. The ALL European Academies, of course, take Belmont's principles further and require context sensitivity and risk awareness (ALLEA, 2017: 6), respect extended to all actors involved (ALLEA, 2017: 4), and independence from the interests (in this case law enforcement) of funders (ALLEA, 2017: 8). There is clearly a need to examine how normative as well as

research ethical principles inform the study of cybercrime. Such evaluation will doubtless lead to more specific recommendations for researchers and reviewers.

Research in cyberspace poses different challenges, of course. Floridi (2002), for instance, suggests ethical judgement be based on the contribution of an action to the general ecosystem. Accordingly, the online environment may need a different approach to ethical evaluation. Interestingly, others have highlighted that online distinctions between, for instance, individuals and their data are blurred (Markham & Buchanan, 2012). Many researchers, however, call for a fine-grained approach highlighting a need to contextualise ethical assessment (Ess, 2002; Flick, 2016; Markham & Buchanan, 2012). The researcher must identify and respect the normative expectations of a specific forum or space online (Hoser & Nitschke, 2010), and continually assess what is appropriate across the different stages of the research process (Pastrana et al., 2018). Private and public cyberspaces are no longer distinct (Ess, 2002; Markham & Buchanan, 2012; Sugiura et al., 2017). Individual attitudes to privacy change depending on context (Acquisti, 2012; Acquisti, Brandimarte, & Loewenstein, 2015), with concern mainly about information being directed and used appropriately than necessarily being kept confidential (Nissenbaum, 2011). So, judgements about a research participant's expectations of privacy become all the more problematic. Even where it's possible to request, informed consent under such conditions no longer makes sense. Pastrana et al. (2018) suggest instead focusing on research on collective rather than individual behaviours and encourage additional pseudonymisation of data prior to publication.

The general research ethics landscape poses many and varied problems for the researcher and the reviewer, therefore. No one size fits all, of course, as many have pointed out (Ess, 2002; Flick, 2016; franzke et al., 2020; Markham & Buchanan, 2012). What is clear, though, and particularly

relevant for cybercrime is that the researcher must consider firstly that the more vulnerable any of the participants or the stakeholders in their research may be, the higher their responsibility to be sensitive to context and the rights of the individual (Markham & Buchanan, 2012). In the next section, we turn from the general principles as they relate to cyberspace and specifically cybercrime to guidance offered currently in the UK.

UK Guidelines for Researchers

Having reviewed the general research ethics landscape, in this section we turn specifically to the UK. At UK universities, research ethics committees or institutional review boards are responsible for providing training, guidance and the review of ethics submissions. Ethics applications are usually screened and categorised as low(er) or high(er) risk. High risk applications – such as cybercrime research – require extra-careful scrutiny by reviewers, chairs of research ethics committees, and data protection officers. What guidance is available for researchers carrying out cybercrime research at UK Universities and research institutes? We reviewed websites of UK funders, professional organisations and UK universities and spoke with colleagues based in criminology departments, ethics boards and involved with data protection. In our review, we included universities with criminology departments known for research of cybercrime (Cambridge, Leeds, Portsmouth, Southampton, and Surrey) as well as other leading criminology departments (for example at Essex, Manchester and Oxford). We also conducted a web-search (using the search terms 'security sensitive research') which led us to guidance provided by a range of other universities (for example City, University of London, and Huddersfield). In addition, we reviewed ethics guidance from the professional organisations representing our disciplines (the British Psychological Society (BPS), the British Society of

Criminology (BSC), and the British Sociological Association (BSA)) and the Association of Internet Researchers. Our review found that while there is little explicit guidance concerning ethical aspects of cybercrime research available, the following four frameworks provide useful resources:

- General research ethics
- Guidelines concerning Internet research
- Data protection regulation (GDPR) which regulates the management of personal data
- Guidance on research on terrorism and extremism and the Prevent Strategy

In each of the following subsections, we provide a brief introduction to each of these four areas and then identify any specific guidance available.

General research ethics

All UK universities and research institutions have adopted ethics policies which are usually displayed on publicly accessible websites facing while some universities (for example, Leicester and Kings College London) make this information available only to members of the university. UK universities have research ethics committees (REC) or institutional review boards (IRB) which ensure that all research which requires ethics approval is reviewed and documented.

Cybercrime research – as well as research on crime in general – requires ethics review and approval. It might be hampered by the usual practice of gaining informed consent. Therefore, deception and data collection without gaining consent can – but must -- be justified.
Furthermore, like other criminologists, those conducting cybercrime research must avoid getting involved in criminal activities while collecting data and interacting with (cyber) criminals.

Available guidance: Researchers based in the UK have access to guidance concerning research ethics from professional organisations (for example, the BPS, the BSC, and the BSA), and

funders (for example, the Economic and Social Research Council (ESRC)). Research ethics are taught at undergraduate and post-graduate levels. Individual universities and research institutes provide information about the ethics application process on public and/or internal webpages. Ethics applications are reviewed by ethics committees within the institution.

Ethics guidelines for Internet research

General ethics principles also apply to Internet research. However, over the last decades Internet research has raised important questions concerning the conceptualisation of "the public sphere" and to what extent it is justified to collect data in the public sphere of the Internet without informing data subjects and obtaining their consent. Even if it might be legal to analyse data that has been shared on social media platforms, social media users have the legitimate expectation that their data is not used without obtaining consent or that every effort is undertaken to prevent the identification of data subjects.

In the previous sections, we have outlined different types of cybercrime which might be an extension of traditional forms of crime which utilise information and communication technologies (ICT) or Internet-based crimes which do not have an offline equivalent. This includes researching the dark web. Accessing any online sites might endanger the researcher and the institution at which she is based and requires careful data management.

Available guidance: for Internet research is available from the Association for Internet Researchers. The BSA has provided Internet specific guidance, including case studies (for example "Researching Online Forums", "Researching Social Machines"). Of particular interest for researchers of cybercrime is the BSA case study "Using Twitter for Criminological Research". UK universities provide limited guidance on Internet-based guidance and ethical

considerations concerning cybercrime. Oxford University is an exception and provides "Best Practice Guidance" for "Internet based research" which addresses deception, dark web studies and deep fakes. Some universities (City, Huddersfield, Aberystwyth, De Montfort) mention criminal activities under security sensitive research and, for example, human trafficking or child pornography.

GDPR, protection of sensitive personal data

The General Data Protection Regulation (GDPR) (European Commission, 2016) concerns the collection, handling and storage of identifiable personal data. Some personal data is regarded as particularly sensitive ("special category", Art. 9) which includes information about race, sexual orientation, political attitudes and activities, as well as criminal behaviour (Art. 10). Collection of such data must be minimal and well justified. Data collection might be online or offline.

Cybercrime research will fall under the GDPR regulations if the data on criminal behaviour includes identifiable personal data. Any such research may require additional approval from the appropriate authority. If published results are completely anonymous after data collection and analysis, then it falls beyond the scope of the GDPR. It therefore requires careful data management at different stages of the research process.

Available guidance: GDPR guidance is widely available from the ESRC, the UK Data service and on the websites of individual universities. The guidance includes detailed information about the legal aspects and what it means for data management and processing.

Prevent, research on terrorism and extremism

The recruitment to and planning of terrorist and extremist acts represents one specific category of cybercrime and in the UK is regulated through the "Prevent duty guidance: For higher education

institutions in England and Wales" (HM Government, 2019) which requires that institutions, including schools and universities, monitor the online and offline activities of staff and students.

Researchers, who are studying the recruitment and planning of terrorist and extremist acts, are carrying out security-sensitive research which requires not only the highest level of scrutiny during the ethics review process, but also secure data storage and registration of the research project in order to prevent harm to the university and its community and the accusation levelled at researchers that they are involved in terrorist and extremist activities.

Available guidance: Universities UK (UUK) has provided guidance for the "Oversight of Security Sensitive Research Material at UK Universities" which responds to the Prevent strategy and provides support for researchers who are carrying out research on security and terrorism. It details the obligations of researchers to register their research projects and use dedicated computers to access and store data related to terrorism. Many universities refer to the UUK guidance on their websites, in some cases citing the UUK document verbatim. Some examples of universities referring to Prevent and the UUK guidance include Cambridge, Sheffield, UWE, Glasgow, Cardiff, and Keele.

Recommendations: Towards ethics guidelines for cybercrime research

Our review indicates that the ethics approval process at UK universities and research institutions is rigorous and provides extensive guidance on research ethics, Internet research, GDPR regulations, and security-sensitive research. The guidance seeks to balance the risk to researchers and the institutions with which they are affiliated and their ability to carry out cutting edge research. This balancing act requires case by case decision making in order to avoid being

neither too risk-averse or overly risk-taking. We found that with the exception of terrorism and extremism specific guidance on cybercrime is limited.

The existing guidance provides an excellent basis for the development of cybercrime specific research ethics. Such research ethics guidance must draw on and combine guidance on Internet research, GDPR regulations, and security-sensitive research. Core issues of cybercrime specific ethics include:

- Lack of informed consent
- Deception
- Secure access and storage of data
- Registering cybercrime with data protection officers or REC boards
- Specific training for researchers and reviewers of cybercrime ethics applications.

In the following section, we provide recommendations for each of these areas as they apply to the overview of cybercrime research in the preceding sections.

Recommendations

Based on the discussion in the previous three sections on the cybercrime landscape, general and UK-specific research ethics considerations, we summarise here recommendations for researchers and reviewers in RECs/IRBs, when considering research protocols for the study of cybercrime. As others have said, this is not intended as a cookbook, but rather to encourage ongoing reflection. The pointers below include specific factors concerning research around cybercrime. The researcher must be sensitive, for instance, to how different cyberspace is in terms of risks to the researcher, the vulnerability of individual actors, and the fine line between research and the requirements of law enforcement. At the same time, both research and reviewer should consider each case on its individual merits, and in consideration of the different stages of the research lifecycle.

Our first two considerations are not specifically covered in the guidance we have reviewed in the previous section. The first, whether it is research or not, is intended to make researchers and reviewers examine whether what is proposed is crime agency monitoring rather than independent research. The second relates to the care and support that the researcher may need in regard to the types of information and behaviours they observe.

Is it research?

The complexity and sensitivity surrounding any cybercrime (see Table 1) suggests that it is important to consider from the start whether a proposed engagement with online activity should be unequivocally research. This may be defined, for instance, with reference to Frascati. There are clear social imperatives to reduce the suffering and protect victims of crime; in addition, there are socio-economic motivators to prevent crimes against institutions, both enterprise and broader structures such as democracy. Although research into such activities could doubtless inform policy and support law enforcement, it is clear that research into cybercrime should be motivated primarily for the search for knowledge. Researchers have a responsibility to the research community; social and legal obligations are beyond the scope of ethical research. Although REC/IRB reviewers should point out any non-research obligations, their primary responsibility is to review the ethical appropriateness of research.

Does the researcher need support?

Security-sensitive research may well need to register with an external agency to protect both the researcher and the reputation of the institution (see below). A more pertinent issue for the researcher themselves and therefore which needs to be evaluated during ethics review is the potential effect that exposure to crime may cause long-term distress to the researcher. This would be particularly relevant where the moral code of the researcher and their peers finds

the criminal activity unacceptable. This would often be the case for crimes against children, but also other forms of human trafficking and hate crime. Reviewers should look for the measures that are in place to provide emotional and psychological support to the researcher.

Consent

There needs to be a careful consideration about whether consent is possible, feasible or desirable and whether it can be truly *informed*. Reviewers therefore need to consider the researcher's position vis-à-vis the rights of research participants, and the relevance of consent. Notwithstanding confusions between consent as a legal basis for processing personal data, consent is not specifically about privacy. The researcher must clearly assess the expectation of privacy for the specific context under investigation. Certainly, in terms of privacy, research subjects may knowingly share information for reasons of their own and very much dependent on the context. Researchers should therefore consider the normative expectations around information sharing on a context-by-context basis. Reviewers should in turn, we suggest, consider not in absolute terms whether research consent can be waived, but rather whether the proposed research shows that it has taken account of the specific online context.

Deception

Well-motivated deception can be an acceptable research method, if appropriately managed (see BPS above). However, the rationale there is typically to observe spontaneous responses. Similarly, lurking can be justified to avoid intrusion or influencing normal behaviours. Deception or lurking should be justified in terms of the expectations of research participants in the particular context and virtual environment in relation to the potential benefit of the

research. It is important to ensure that researcher safety is appropriately handled. In the case of deception in particular, researchers and reviewers should be clear that the researcher's actions are not construed as entrapment.

Secure access and storage of data

GDPR and Prevent regulations require the secure storage of data in order to prevent harm to research participants, researchers, and the institutions in which they work. This means that researchers are only allowed to access the dark web or contact terrorist networks using computers which are separate from the university IT infrastructure in order to avoid making it vulnerable to hacking and other cyber-attacks. Reviewers should consider an appropriate data management plan across the lifecycle of the research study, including publication of results. This should clearly describe how data are secured, how access is managed and how the data will be disposed of.

Registering cybercrime with data protection officers, RECs/IRBs and / or external agencies

Researchers need to register projects that involve criminal and terrorist activities with data protection officers or chairs of ethics committees. They should also check whether their research activities need to be registered or made known to any relevant agency. This is so to minimise the risk of being accused in illegal activities in the case of criminal investigations. However, registering does not necessarily provide legal protection for researchers. Reviewers should check that researchers demonstrate awareness of the legal requirements they should consider.

Specific training for researchers and reviewers of cybercrime ethics applications

We are only aware that Portsmouth University carries out training for PGT students in the context of their MSc on Cybercrime. Further research is needed to assess the extent of cybercrime ethics guidance that is available to researchers and reviewers in the UK. As a minimum, we would recommend that ethics reviewers should be supported in understanding the specifics of the context (i.e., the normative expectations of cybercriminals), relevant regulatory requirements (including Prevent and the GDPR if personal data are involved), and the role of the researcher in relation to the individual or group they study.

Limitations and future research

In the preceding sections we have considered general research ethics and how these relate to research in the virtual world in regard to cybercrime. On that basis, we have summarised the available guidance and practices of ethics reviews for cybercrime research in the UK. It is essential, we believe, that research ethics keeps pace with the changes afforded by the virtual world and not only in regard to cybercrime. If academia is to retain a significant role within research when faced with competition from technology giants, then it must demonstrate that it can manage transparent and accountable research even within security sensitive environments.

There is a final consideration, however, which is relevant especially to the study of cybercrime. The nature of the Internet and ease with which individuals can ostensibly achieve some level of anonymity even on the clear web may have promoted this type of crime. But the reach of the Internet also provides an opportunity for criminal activities to span jurisdictional boundaries. In consequence, law enforcement as well as research activities must take into account this international aspect, not least in encouraging cross-border collaboration and data sharing.

Similarly, cybercrime ethics also concern the approach to contemporary counter-movements on the left and the right, and to what extent they are classified as extremist, and how foreign influence can affect civic life. The current political landscape, in particular Brexit and the reshuffling of international research relations raises important questions about data management and international collaboration (Rotenberg, 2020).

Our chapter is only a starting point, though. Our contribution is intended to highlight the need to contextualise ethics review in regard to all stages of the research lifecycle. We welcome ongoing surveys of these practices to assess the needs of cybercrime researchers and university research ethics committees in order to balance the need to carry out cutting edge and high-risk research and the security of universities.

Useful Links

The British Psychological Society

https://www.bps.org.uk/news-and-policy/ethical-guidelines-applied-psychological-practice-field-extremism-violent-extremism

https://www.bps.org.uk/news-and-policy/ethics-guidelines-Internet-mediated-research-2017

The British Society of Criminology

https://www.britsoccrim.org/ethics/

The British Sociological Association

https://www.britsoc.co.uk/ethics

https://www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf

https://www.britsoc.co.uk/media/24309/bsa_statement_of_ethical_practice_annexe.pdf

Association of Internet Researchers

https://aoir.org/ethics/

Universities UK

https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/security-sensitive-research-material-UK-universities-guidance.aspx

UK Data Service

https://www.ukdataservice.ac.uk/manage-data/legal-ethical/gdpr-in-research.aspx

Economic and Social Research Council

https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/

https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/frequently-raised-topics/data-requirements/data-protection/

Selected Universities:

City, University of London

https://www.city.ac.uk/research/ethics/help-and-guidance/policy-on-security-sensitive-research

Huddersfield

https://staff.hud.ac.uk/portal/informationforresearchers/securitysensitiveresearch/

Oxford University

https://researchsupport.admin.ox.ac.uk/files/bpg06Internet-basedresearchpdf

References

Aas, K. F. (2013). Globalization & Crime. *Sage Publications, London, 156*, 18-20.
Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. *Digital Enlightenment Yearbook 2012*, 193-197. doi:10.1109/MSP.2009.163
Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi:10.1126/science.aaa1465
ALLEA. (2017). The European Code of Conduct for Research Integrity. In (Revised Edition ed.). Berlin, Germany: Allea.org.
Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2013). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction, 109*(5), 774-783. doi:10.1111/add.12470
Beaulieu, A., & Estalella, A. (2012). Rethinking research ethics for mediated settings. *Information, Communication & Society, 15*(1), 23-42. doi:10.1080/1369118X.2010.535838
Belmont. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research.* Retrieved from https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html
Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice, 42*(5), 495-499. doi:10.1080/0735648X.2019.1692426
Burruss, G. W., Holt, T. J., & Wall-Parker, A. (2018). The Hazards of Investigating Internet Crimes Against Children: Digital Evidence Handlers' Experiences with Vicarious Trauma and Coping Behaviors. *American Journal of Criminal Justice, 43*(3), 433-447. doi:10.1007/s12103-017-9417-3
Chopik, W. J. (2016). The Benefits of Social Technology Use Among Older Adults Are Mediated by Reduced Loneliness. *Cyberpsychology, behavior and social networking, 19*(9), 551-556. doi:10.1089/cyber.2016.0151
Crown Prosecution Service. (n.d.). Cyber / online crime. Retrieved from https://www.cps.gov.uk/cyber-online-crime
Decary-Hetu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime, 2*(2), 122-141.
Ess, C. (2002). *Ethical decision-making and Internet research: Recommendations from the AoIR ethics working committee*. Retrieved from https://aoir.org/reports/ethics.pdf
European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics, 12*(1), 14-28. doi:10.1177/1747016115599568
Floridi, L. (2002). On the intrinsic value of information objects and the infosphere. *Ethics and Information Technology, 4*(4), 287-304.
franzke, a. s., Bechmann, A., Zimmer, M., Ess, C., & the Association of Internet Researchers. (2020). Internet Research: Ethical Guidelines 3.0. Retrieved from https://aoir.org/reports/ethics3.pdf
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243-249.
Grabosky, P. N. (2014). The Evolution of Cybercrime, 2004-2014. *RegNet Working Papers, 58*. doi:10.2139/ssrn.2535605
HM Government. (2019). Prevent duty guidance. Retrieved from https://www.gov.uk/government/publications/prevent-duty-guidance
Holt, T. J. (2016). *Cybercrime through an interdisciplinary lens*.
Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant behavior, 35*(1), 20-40.
Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies, 23*(1), 33-50. doi:10.1080/14786011003634415
Hoser, B., & Nitschke, T. (2010). Questions on ethics for research in the virtually connected world. *Social networks, 32*(3), 180-186. doi:10.1016/j.socnet.2009.11.003

Kagan, S. (1992). The structure of normative ethics. *Philosophical perspectives, 6*, 223-242. doi:10.2307/2214246
Koops, B.-J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational criminology manual* (Vol. 1, pp. 735-754). Nijmegen: WLP.
Latour, B. (2005). *Reassembling the social-an introduction to actor-network-theory*. Oxford UK: Oxford University Press.
Lavorgna, A., Middleton, S. E., Pickering, B., & Neumann, G. (2020). FloraGuard: tackling the online illegal trade in endangered plants through a cross-disciplinary ICT-enabled methodology. *Journal of contemporary criminal justice*. Retrieved from https://eprints.soton.ac.uk/437583/
Submission of evidence to the all party Parliamentary Group Drones: How are RAF Reaper (drone) operators affected by the conduct of recent and ongoing operations, (2017).
Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime, 13*(2), 71-94. doi:10.1080/17440572.2012.674183
Lusthaus, J. (2018a). Honour among (cyber) thieves? *European Journal of Sociology/Archives Européennes de Sociologie, 59*(2), 191-223. doi:10.1017/S0003975618000115
Lusthaus, J. (2018b). *Industry of anonymity: Inside the business of cybercrime*. Cambridge, MA: Harvard University Press.
Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. *Policing: A journal of policy and practice*. doi:10.1093/police/pax042
Markham, A., & Buchanan, E. (2012). *Ethical decision-making and internet research: Recommendations from the aoir ethics working committee (version 2.0)*. Retrieved from https://aoir.org/reports/ethics2.pdf
Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry—a year on. In: British Medical Journal Publishing Group.
Michael, K., McNamee, A., & Michael, M. G. (2006). *The emerging ethics of humancentric GPS tracking and monitoring*. Paper presented at the 2006 International Conference on Mobile Business.
Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32-48. doi:10.1162/DAED_a_00113
Norman, D. A. (2010). *Living with Complexity*. Cambridge, MA: MIT Press.
O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data increases inequality and threatens democracy*. New York, NY: Crown.
Parsons, T. D. (2019). *Ethical Challenges in Digital Psychology and Cyberpsychology*. Cambridge, UK: Cambridge University Press.
Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). *CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale*. Paper presented at the Proceedings of the 2018 World Wide Web Conference, Lyon, France.
Rotenberg, M. (2020). Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection. *European Law Journal*. doi:10.1111/eulj.12370
Sabillon, R., Cano, J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6).
Safi, M. (2016, 13th July 2016). The takeover: how police ended up running a paedophile site. *The Guardian*. Retrieved from https://www.theguardian.com/society/2016/jul/13/shining-a-light-on-the-dark-web-how-the-police-ended-up-running-a-paedophile-site
Spitzner, L. (2003a). The honeynet project: Trapping the hackers. *IEEE Security & Privacy, 1*(2), 15-23.
Spitzner, L. (2003b, 8-12 Dec. 2003). *Honeypots: catching the insider threat*. Paper presented at the 19th Annual Computer Security Applications Conference, 2003. Proceedings.
Sugiura, L. (2018). *Respectable deviance and purchasing medicine online: Opportunities and risks for consumers*. London, UK: Palgrave.
Sugiura, L., Wiles, R., & Pope, C. (2017). Ethical challenges in online research: Public/private perceptions. *Research Ethics, 13*(3-4), 184-199. doi:10.1177/1747016116650720

Turkle, S. (2017). *Alone Together: Why We Expect More From Technology and Less From Each Other*(3rd ed.). Retrieved from https://www.ted.com/talks/sherry_turkle_alone_together

Upadhyaya, R., & Jain, A. (2016). *Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet.* Paper presented at the 2016 International Conference on Computing, Communication and Automation (ICCCA).

Vilanova, F., Beria, F. M., Costa, Â. B., & Koller, S. H. (2017). Deindividuation: from Le Bon to the social identity model of deindividuation effects. *Cogent Psychology, 4*(1), 1308104. doi:https://doi.org/10.1080/23311908.2017.1308104

Wall, D. S. (2001). Cybercrimes and the Internet. *Crime and the Internet*, 1-17.

Wall, D. S. (2004). What are cybercrimes? *Criminal Justice Matters, 58*(1), 20-21.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Malden: Polity Press.

Webber, C., & Yip, M. (2012). Drifting on and off-line Humanising the cyber criminal. In S. Winlow & R. Atkinson (Eds.), *New directions in crime and deviancy* (pp. 191-205). London: Routledge.

Webber, C., & Yip, M. (2020). Humanising the Cybercriminal. In R. Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (pp. 258-285). London: Routledge.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society, 23*(4), 516-539. doi:10.1080/10439463.2013.780227