Ethical issues in research using datasets of illicit origin

Daniel R. Thomas
Sergio Pastrana
Alice Hutchings
Richard Clayton
Alastair R. Beresford
Cambridge Cybercrime Centre, Computer Laboratory
University of Cambridge
United Kingdom
Firstname.Lastname@cl.cam.ac.uk

ABSTRACT

We evaluate the use of data obtained by illicit means against a broad set of ethical and legal issues. Our analysis covers both the direct collection, and secondary uses of, data obtained via illicit means such as exploiting a vulnerability, or unauthorized disclosure. We extract ethical principles from existing advice and guidance and analyse how they have been applied within more than 20 recent peer reviewed papers that deal with illicitly obtained datasets. We find that existing advice and guidance does not address all of the problems that researchers have faced and explain how the papers tackle ethical issues inconsistently, and sometimes not at all. Our analysis reveals not only a lack of application of safeguards but also that legitimate ethical justifications for research are being overlooked. In many cases positive benefits, as well as potential harms, remain entirely unidentified. Few papers record explicit Research Ethics Board (REB) approval for the activity that is described and the justifications given for exemption suggest deficiencies in the REB process.

CCS CONCEPTS

• **Social and professional topics** → **Computing profession; Codes of ethics; Computing / technology policy;** • **General and reference** → *Surveys and overviews;* • **Applied computing** → *Law;* • **Networks** → Network privacy and anonymity;

KEYWORDS

Ethics, law, leaked data, found data, unintentionally public data, data of illicit origin, cybercrime, Menlo Report

ACM Reference format:
Daniel R. Thomas, Sergio Pastrana, Alice Hutchings, Richard Clayton, and Alastair R. Beresford. 2017. Ethical issues in research using datasets of illicit origin. In *Proceedings of IMC '17, London, UK, November 1–3, 2017,* 18 pages.
DOI: 10.1145/3131365.3131389

IMC '17, London, UK

1 INTRODUCTION

The scientific method requires empirical evidence to test hypotheses. Consequently, both the gathering, and the use of, data is an essential component of science and supports evidence-based decision making. Computer scientists make significant use of data to support research and inform policy, and this includes data which was obtained through illegal or unethical behaviour.

In this paper we consider the ethical and legal issues surrounding the use of datasets of illicit origin, which we define as data collected as a result of (i) the exploitation of a vulnerability in a computer system; (ii) an unintended disclosure by the data owner; or (iii) an unauthorized leak by someone with access to the data.

The collection, or use, of a dataset of illicit origin to support research can be advantageous. For example, legitimate access to data may not be possible, or the reuse of data of illicit origin is likely to require fewer resources than collecting data again from scratch. In addition, the sharing and reuse of existing datasets aids reproducibility, an important scientific goal. The disadvantage is that ethical and legal questions may arise as a result of the use of such data.

There is evidence that some researchers who use datasets of illicit origin consider ethical and legal issues, particularly through the introduction of ethical consideration sections into papers [83] and the development and use of institutional resources such as Research Ethics Boards (REBs) [26]. Unfortunately, our work shows that neither is common practice, and even where they are tackled, ethical and legal considerations often appear incomplete. It therefore follows that potential harms may have taken place which might otherwise have been mitigated or avoided. Research that lacks sufficient ethical consideration may still be ethical, but it is difficult to assess this.

General guidance, such as that provided by the Menlo Report [28], provides useful advice, but does not address all the issues that arise in using data of illicit origin. Academic discussions have taken place [32], and there are blog posts and other informal articles by academics on the topic [119, 124], but to date there is little in the way of detailed analysis, or a systematisation of knowledge, which explores this problem in depth.

The goal of this paper is to address this gap and provide a detailed evaluation of the use of data of illicit origin in peer-reviewed research, and to support the development of a more nuanced understanding of the issues and problems in this space. We do this by first reviewing previous work to identify the ethical (§2) and legal (§3) issues that can arise. We then analyse over 20 recent peer-reviewed papers which make use of data of illicit origin (§4), and systematize (Table 1) the ethical and legal decisions made against a common set of justifications, safeguards, potential harms and potential benefits (§5).

2 ETHICS

Ethical norms are constantly changing with research ethics developing over the course of the 20th century and becoming more prominent in our field in the 21st century. Previous work related to the ethical use of data of illicit origin spans a number of topics, including informed consent, human rights, releasing and using shared data, hacking, analysis techniques, ethical review, and Research Ethics Boards (REBs). We consider each of these in turn.

Informed consent: The earliest work on the ethics of computer-monitored data explored informed consent and emphasised the right of withdrawal as well as the importance of data anonymisation [89]. The first difficulty with data of illicit origin is that it is not always possible to meet these requirements. Acquiring consent from users involved in leaked data is challenging, particularly if they are involved in illegal activities [72]. In the case of data obtained from underground marketplaces, covert research without consent is necessary to understand what is traded due to the illegality of the goods bought or sold – consent could affect the results [101]. This is one of the exceptions for informed consent in the ethics statement of the British Society of Criminology, which states that "covert research may be allowed where the ends might be thought to justify the means" [23].

In cases where consent is possible, previous work has concluded that if informed consent has been given on the basis of a promise of confidentiality by the researcher, then researchers should take particular care to ensure that they are willing to keep the promises they make, particularly if doing so might require them to break the law [52].

Where informed consent is impossible to obtain, the Menlo Report recommends that the REB must protect the interests of the individuals [26]. Thus, the REB has a particularly important role to play in research which makes use of data of illicit origin where informed consent is not possible [23].

Human rights: Human rights also provide an important ethical baseline. These include, the right to life, the right to be free of arbitrary arrest, the right to a fair trial, a presumption of innocence until proven guilty, a right to not have arbitrary invasions of privacy, and a right not to be arbitrarily deprived of property [112]. Research using data of illicit origin may indirectly deprive people of such rights and so this needs to be considered. For example, in Philippines in 2016, suspected illegal drug users or dealers were subject to extra-judicial assassination [6] and hence care would need to be taken with data collected from online drug markets to ensure this did not result in such abuse.

Releasing and using shared data: The WECSR workshop in 2012 convened a panel of experts from different domains who agreed that research involving data of illicit origin would need to have a clear benefit to society [32]. They also argued that simply because data is public does not exempt research using such data from obtaining REB approval since it might contain personally identifiable information. This echoes the Menlo Report's suggestion that the REB must protect the interests of individuals where informed consent is impossible.

Sharing of datasets is beneficial for data science, but the purpose and scope for using such data must be stated [19]. Allman and Paxson discussed the ethical issues of releasing data, using data released by others, and the interactions between providers and users of data [4]. A key ethical consideration in this context is privacy protection. It is likely that data of illicit origin was not intended for research purposes or public exposure, and thus it may not be anonymised. In such cases, the raw dataset should not be shared publicly, and research conducted with such data should aim to preserve privacy. Researchers who hold data of illicit origin should only provide details of their source or (as Allman and Paxson suggest) share data with verified researchers under a written acceptable usage policy. None of the papers we discuss later took this approach. Partridge argues that papers in network measurement research should have an ethics section, partly to increase the availability of examples of ethical reasoning [83]. We show in §5 that few papers using data of illicit origin have an ethics section.

Both Allman & Paxson, and Partridge warn against relying on the anonymisation of data since deanonymisation techniques are often surprisingly powerful. Robust anonymisation of data is difficult, particularly when it has high dimensionality, as the anonymisation is likely to lead to an unacceptable level of data loss [3].

Hacking and intervening: Hacking into computers to extract information is usually unethical [102] and illegal. Moore and Clayton considered ethical dilemmas in take-down research resulting from nine dilemmas they faced during their research. They considered the balance between reducing harm uncovered during measurements and the accuracy of such measurements, the dangers of telling criminals the flaws in their systems and the importance of ensuring that proposed interventions are likely to work [75]. Dittrich et al. provide two case studies on ethical decision making for remote mitigation of botnets [29]. They discuss the ethical issues involved including the reasons for and against intervening.

Analysis techniques: The ethics committee of the Association of Internet Researchers' (AoIR) has produced guidance for ethical decision making in Internet research in 2002 [33] and 2012 [71]. This cross-disciplinary work provides useful questions to aid researchers in considering the ethics of their research and defines a process for ethical decision making. AoIR aimed to publish case studies of the application of their

guidelines but this has not yet happened. This paper considers over 20 papers which might have used the AoIR ethics guidelines but only one of them (§4.3.2) did so. Keegan and Matias developed a multi-party risk benefit framework for use in analysing ethical considerations for online community research [56]. While this was implicitly intended for research surrounding particular online community platforms, the same principles apply to research that considers the online community of the Internet, and so it may be a helpful technique.

Ethical review: The Menlo Report [28] and its companion [26] are the primary reference on ethical practice in Information Communication Technology Research (ICTR), particularly for USA-based researchers. It includes numerous questions to help researchers consider ethical issues and case studies to illustrate their application. It identifies that ICTR has a greater scale, speed, coupling, decentralisation, distribution, and opacity than traditional human subject research and hence it re-examines the particular ethical principles required to evaluate ICTR. It identifies four ethical principles [26, §B]: **Respect for persons**: individuals should be treated as autonomous agents and persons with diminished autonomy should be given additional protection. **Beneficence**: minimise possible harms, and maximise possible benefits. The researcher should also use safeguards against potential harms. **Justice**: risks and benefits should be distributed fairly and not on the basis of protected characteristics such as race, or other characteristics that correlated with protected ones. **Respect for law and public interest**: in general ethical research conforms to applicable laws in relevant jurisdictions. Research should always be in the public interest. Additionally, research should be open, transparent, reproducible and peer-reviewed.

Research Ethics Boards (REBs): Program committees or journal editors are able to review the ethics of work after it has been conducted but before it is published. REBs, known as Institutional Review Boards (IRBs) in many US institutions or Ethics Committees in some UK institutions, review the ethics of proposed research before it is conducted. Many REBs were originally formed in response to a review of the ethics of medical research following revelations of unethical medical research conducted prior to the 1970s [26, §A.1]. In this context there were clearly human subjects who had rights that needed to be protected. The term "human subject" is now deprecated in ethical review in favour of considering the wide variety of people who might be "participants" in the research, even if they are not aware the research is being conducted. However, some REBs are still structured around serving this original purpose, and thus they lack the expertise to understand ICTR or the process to evaluate research whose risks and challenges differ from a medical trial. Such structures discourage researchers from using REBs as they do not add value and may introduce many months of delay. By contrast other REBs (such as ours in Cambridge) have ICTR specialists and aim to provide a response in five working days for simple cases. In general REBs are required because researchers are biased when assessing the ethics of their own research [26]. REBs can help researchers identify additional safeguards or improvements in experimental design that make the work ethical, and can help protect researchers from liability.

2.1 Ethical issues

In order to support analysis of case studies in §4, we now list the set of ethical issues that require consideration when conducting research with data of illicit origin:

Identification of stakeholders: The primary, secondary, and key stakeholders should be identified to support the analysis of the potential harms and benefits of the research. Primary stakeholders are those directly connected with data, such as those identified in it; secondary stakeholders are intermediaries in the delivery of benefits or harms, such as service providers; and key stakeholders are those such as the leaker or the researcher who are critical to the conduct of the research.

Informed consent: In most of the research we consider it was impossible or impractical to obtain informed consent from the primary, and in some cases secondary, stakeholders. However, research may be designed such that informed consent is not required. Since none of the case studies we have considered obtained informed consent for their use of data of illicit origin, we do not consider it in later analysis.

Identify harms: The potential harms arising from the use of the data of illicit origin should be identified.

Safeguards: Researchers should apply mechanisms to mitigate or reduce the potential for harm.

Justice: The research does not unfairly advantage or disadvantage any particular social or cultural group.

Public interest: The research has been published, is reproducible, and there is a "social acceptability" exceeding the harms [35].

3 LEGAL ISSUES

Legal issues surrounding research with data collected illegally can be complex, particularly as the laws of multiple jurisdictions are likely to be applicable. We are not lawyers and researchers should seek their own legal advice. Countries whose laws that may apply to research being conducted include those where individuals or systems that these data refer to reside, the countries where data was stored, the countries where the researchers conducted the research, and possibly also any countries that data transited during any part of this process. Researchers often travel and so they should consider the impact of committing offences, both in their home jurisdiction and in countries that they visit or that they might be extradited to.

The key legal issues applicable to research with data of illicit origin are as follows:

Computer Misuse: Most jurisdictions now have laws against the misuse or abuse of computers such as the UK [21], the US [1], and Germany [38, 39, 40, 41]. These can cover generic actions such as the unauthorised use of a computer system

(even if there was no technical measure in place to prevent it), and the use of malware, or 'dual use' tools that may be used for malicious purposes.

Copyright: The right to produce copies, including, in some jurisdictions, database rights, and trade secrets may apply to data obtained by researchers. In particular, it may affect the further sharing of data with other researchers as that might constitute the creation of copies. There are exemptions to copyright such as "fair use", which vary with jurisdiction.

Data Privacy: Data may contain personally identifiable information which may mean it needs to be protected and processed in accordance with relevant Data Privacy and Data Protection rules. In several jurisdictions IP addresses may be considered personal data, which complicates their use, particularly where consent has not been obtained. This is the case in Germany [115, p29], though a European Court of Justice ruling has found that personally identifiable data can still be processed without consent for security purposes (e.g. IP addresses in web server logs) [48]. There is an exemption for the use of the personal data in Germany "if it is necessary for a research entity in order to conduct a scientific research, the scientific interest to conduct the research project substantially predominates over the interest of the data subject in exclusion of the change of purpose the data was collected for, and if the research cannot be conducted otherwise or can otherwise be conducted under disproportional effort." (German Federal Data Protection Code §28.2.3 [115]).

The General Data Protection Regulation (GDPR) [22] applies from May 2018 to the collection and processing of personal data in the EU and to organisations that offer goods or services to individuals in the EU [50]. It provides specific measures to allow processing of personal data for scientific research in the public interest, subject to appropriate safeguards such as encryption, pseudonymisation, and data minimisation. It mentions that scientific research should increase knowledge and that personal data should not be included in publications. It specifically allows the processing of data collected for other purposes for scientific or historical research (Article 5). It requires (Article 14.5.b) that the interests of data subjects be protected and that information about the data collected, how it is being processed and safeguarded, and who is responsible be made publicly available. It encourages the use of approved codes of conduct surrounding data processing and it may be helpful for research communities to develop such codes of conduct. Penalties for violating the GDPR include fines of up to EUR 20 million, or 4% of worldwide turnover, whichever is higher.

Terrorism: In some jurisdictions (e.g. UK) it may be an offence to fail to report terrorist activity [108], including any discovered during a research project. Additionally, possession of terrorist materials may be an offence unless specific exceptions for research are met. REB approval and institutional oversight are likely to be necessary if the research involves terrorist materials, such as discussion of planned attacks or techniques, to ensure the researcher is protected [113].

Indecent images: Possession of indecent images of children is an offence in many jurisdictions including the UK [88], USA [2], and Germany [37]. In general there are no exemptions for research. Hence, care may need to be taken when scraping or receiving some types of data dump in case they contain such material.

National Security: Data obtained may be protected by national security legislation. Therefore unauthorised use or publication of these data may expose the researchers to legal risks. Even if data is publicly available it may still be classified [36]. This is discussed further in §4.5.2.

Contracts: Researchers may be exposed to civil liability resulting from breach of contract by using certain data if doing so violates terms of service or other contracts that researchers have agreed to.

Occasionally research may be illegal but still ethical. In such cases researchers should be transparent about what they are doing and both they and their institutions should be willing to accept the consequences. REB approval is essential in such cases. In such circumstances researchers should actively engage with lawmakers to improve the law so that the ethical work that they want to do is made legal in future [52].

There are generic defences against legal liability that may apply. *Mens rea*: In some cases if the researcher can demonstrate lack of criminal intent then a criminal prosecution cannot succeed; REB approval may be a useful way to demonstrate this. *Not in the public interest to prosecute*: This is an especially generic defence, but it is uncertain.

The use of an REB may transfer legal risks to the researcher's institution or ensure that the institution provides legal assistance to the researcher. This alone is a strong incentive for individual researchers to use an REB.

3.1 Related work on law and ICTR

Others have discussed legal issues in ICTR for particular kinds of research in particular jurisdictions.

Soghoian discusses legal risk arising from conducting phishing experiments, with four case studies and a discussion of the copyright, trespass to chattel, trademark, terms of service violation, computer fraud, and anti-phishing issues in the USA [100]. He recommends all such research should be subject to ethical review as well as legal advice, and that the institution IT staff and anyone else likely to receive a cease and desist letter related to the project should be consulted. He also notes the importance of not gaining any financial benefit from the work, for example, adverts should not be shown on pages associated with the work.

Ohm et al. examine the legal issues for network measurement research arising from USA Federal Law [81]. They suggest capturing only the required data, scrubbing IP addresses, encrypting data when not analysing it, restricting monitoring to the smallest possible network, and ensuring that measuring tools do not store the full packets to disk.

Burstein discusses the legal issues surrounding cybersecurity research, and in particular research using network traces, running malware honeypots, or mitigating attacks by interfering with malicious systems [15].

4 CASE STUDIES

The ethical and legal considerations of conducting and publishing academic research with data of illicit origin depends on the context [124]. Many factors may come into play, such as the type of data involved, the measurement techniques used or the results of the research. Thus, ethical and legal consideration must be conducted separately for each research activity. This section presents a series of concrete case studies where different kinds of data of illicit origin was used. We do not attempt to provide a complete survey on each topic. Instead, for each topic we consider recent and relevant work, focussing on those that mention or expose interesting ethical issues. We selected from papers we were already aware of, those we found from searches, and from following references forwards and backwards. Decisions on which papers to include were necessarily subjective. We consider work by people who self-identify as researchers even if they do not publish in academic venues, although we have focussed on publications which have undergone peer review. We highlight the ethical (e.g. *Identification of stakeholders*) and legal (e.g. *Computer misuse*) issues defined in §2.1 and §3 in each case, and the overall results are summarised in §5. We do not cover research using active measurements such as the controversial Encore work discussed by others [78].

4.1 Malware and exploitation

Research conducted using hacking tools such as botnets or exploit kits is necessary to understand how malicious actors use them and to provide countermeasures. However, the use of such tools can be harmful, and sometimes researchers have used them without considering legal or ethical issues. In this section we cover three particular cases: the use of a botnet to scan the IPv4 address space, the exploitation of a discovered vulnerability to gather email addresses, and research using source code of malware specimens.

4.1.1 Carna scan. In 2012 an anonymous individual claimed to have carried out a complete scan of all IPv4 addresses on all ports and made the dataset publicly available. However, the means they used to do this was a botnet of 420 000 devices with default passwords [18]. Creating a botnet of compromised computers to carry out research is illegal since it is *Computer misuse*. Is research that uses these data ethical?

CMU CERT wrote a blog post explaining how these data could be used and, while they pointed out there were some ethical issues, they noted that: "As far as we can tell, this data set does not contain legally restricted information, like classified information, personally identifiable information, or trade secrets." [99]. CAIDA found that there were some problems with this data since some bot-devices were behind HTTP proxies which meant that the results for port 80 scans were incorrect [18]. They noted ethical concerns without giving details, and referred the reader to the Menlo report [26]. To prevent harm, CAIDA only looked at data targeting their own darknet. Malécot and Inoue took a similar approach, analysing their network telescope [70]. However, they then realised that they knew the IP addresses of the botnet devices as they were the sources of the probes of their network telescope. These IP addresses thus once belonged to devices that could be easily brute forced as they had weak Telnet passwords, in doing so the authors *Identify harms*. The *Safeguards* they used were that they kept these IP addresses confidential pending finding an ethically acceptable and practical way of dealing with the situation.[1]

Krenc, Hohlfeld and Feldmann published a non-peer reviewed editorial note where they analysed the scan results [62]. They found numerous technical problems with the data, and the authors concluded that given that Carna scan made no technical contributions, it had been unethical to conduct. While they did not provide an opinion on whether it is ethical to use these data for research, they did use it for these purposes.

When these scan data were first released, it was not necessary to use them to answer research questions as researchers could conduct their own scans legally, ethically, and with better technical validity. For new research that requires comparison with the Internet of 2012, these Carna scan data might be of use. However, due to substantial technical problems with these Carna scan data [62] in many cases there will be no good argument for using them.

Dittrich, Carpenter and Karir use the Menlo report to present a thorough analysis of the ethics of the Carna botnet [27], from which they conclude that there is a "lack of a common understanding of ethics in the computer security field".

4.1.2 AT&T iPad users database brute force. In 2010 researchers from Goatse Security discovered a web service run by AT&T that, when provided with the ICC-ID of a 3G iPad, would return the associated email address. They used this to obtain the email addresses for 114 000 iPad users and passed this information to Gawker [106] as well as making the vulnerability known to third parties. They did not contact AT&T to report the vulnerability. The subsequent FBI investigation [107] resulted in the authors being found guilty of *Computer misuse* and one of them was sentenced to 41 months imprisonment [30]. While it was argued that this imprisonment was an overreaction [98] the research was clearly both unethical and illegal.

Finding vulnerabilities in third party systems without permission can be ethical, since this helps that party to *Identify harms* and to avoid future attacks. However, in this case it was unethical, because: i) The authors collected far more personal data than they needed to prove it to be a real vulnerability, ii) The authors shared this data and the existence of the vulnerability (including the exploit script) with third parties before reporting the problem to AT&T. Hence, the authors identified risks for iPad users, but exploited the vulnerability and, given that they did not contact AT&T, they failed to implement *Safeguards*. Indeed,

[1] In 2016 the Mirai botnet was also built by brute forcing Telnet passwords. As a security research community we did not successfully mitigate the risks that the Carna botnet demonstrated [91]. We were not able to contact Malécot and Inoue to discover if they found a solution to ethically using the IP addresses.

the research work is not in the *Public interest*, since they did not minimise harm or maximise benefit, except to their own notoriety (a lack of *Justice*).

4.1.3 Malware source code. Malware source code has been publicly released on multiple occasions. This code has then been used by malicious actors to attack computer systems or networks. Additionally, malware source code can be obtained from public databases such as vxHeaven or Contagio Dump. For example, the source code for Zeus was leaked in 2011 [45]. Since then, many variants of Zeus have been reported by anti-virus vendors. Similarly the source code for Mirai botnet was released in 2016 [60]. The release of malware source code often lowers the barrier to entry for using the malware: after Mirai's source code was released, myriad Mirai based botnets began operation. Release of source code is sometimes correlated with prosecution of its author, as in the example of Agobot in 2004 [43]. Additionally, the release of source code might result in changed business models for malware authors such as the Zeus botnet as-a-service [45]. The source code of malware can also be obtained from its operational settings. Stone-Gross et al. [103] identified and obtained access to some of the C&C servers for the Pushdo/Cutwail botnet (used mainly for spam delivery) by contacting the hosting providers (i.e. the authors first performed *Identification of stakeholders*). They obtained sensitive data such as the statistics of infection, target email addresses and the source code of the malware.

Kotov and Masacci collected source code of exploit kits from a public repository as well as underground forums where code was leaked or released [58]. Their analysis showed how exploit kits evade anti-crawling techniques and how malware authors protect against code analysis. However, as the authors state, the fact that the code was leaked biased their analysis, for example due to removal of obfuscation from the source code. Calleja et al. analysed 151 malware samples dating from 1975 to 2015. They show how the malware landscape has evolved using traditional software metrics on a dataset of malware code from various repositories, including vxHeaven, GitHub, hacker-related magazines, and P2P networks. The authors do not share the collected source code, but only provide a dataset containing the metrics obtained from the malware pieces [17].

Research using malware source code has substantial benefits as better understanding of how malware works, so as to facilitate developing new detection and mitigation techniques. Publishing the results and explaining the tools and techniques used to analyse the malware makes this research of *Public interest*. Both possession and accidental disclosure of malware could be illegal. Researchers could use secure storage, enforce retention policies, and not publicly distribute the malware source code as *Safeguards*. However, none of the research works using source code mentioned ethical or legal issues, nor whether they have obtained permission from their corresponding REB. Calleja et al. shared a dataset with metrics from the source code, but not the sources themselves, as *Safeguards* that allow for reproducibility without releasing the malware [17]. Additionally, stylometry analysis allows code writers to be identified [16]. By identifying who has written some piece of code, it is possible to group malware families, detect plagiarism, and attribute attacks. Thus, the release of source code (not just malware code) should be done with care, since it can be used to identify the authors.

4.2 Password dumps

Password dumps are the archetypal leaked dataset – a list of passwords that has been been made public, normally by illegal action; criminals regularly compromise databases (e.g. by SQL injection) and then publish the contents online [120]. Since people include personal data in passwords, the password alone can be sensitive [104] and the lists may also include other personal data such as email addresses or names.

Research into password dumps is controversial but widely practised [104], not least because they provide researchers with ground truth data, that otherwise would be difficult to obtain [32]. A variety of dumps have been investigated. One of the largest dumps, is the RockYou dump, others include MySpace leaked in 2006, or Facebook leaked in 2010. These dumps and many others can be found online by using common search engines.

Weir et al. use lists of compromised and publicly disclosed passwords [121]. They say that "while publicly available, these lists contain private data; therefore we treat all password lists as confidential" and that "due to the moral and legal issues with distributing real user information, we will only provide the lists to legitimate researchers who agree to abide by accepted ethical standards". In a later paper by the same authors they note that it is a "mixed blessing" that research into passwords used for high value targets, such as bank accounts, will not be possible until relevant breaches occur and the data is made public [120].

Das et al. study trends in password reuse across different sites by analysing passwords obtained through an internal survey and several hundred thousand leaked passwords [24]. They state that the ethics of conducting research with data acquired illegally is under debate, but they justify their work saying that: 1) these datasets were used in several previous studies, 2) they protected users privacy by only working with hashed email addresses, 3) they obtained approval from their REB to conduct the survey. Finally, the authors state that their results help system administrators and researchers understand how cross-site password attacks work.

Kelley et al. used two datasets of leaked passwords as well as passwords collected through an online survey [57]. The authors received approval from their REB for this survey, and they discuss the ethics of using leaked databases of passwords. They argue that, given these data were already public, using it for research does not increase harm to users, since no further connection with real identities is sought. Moreover, given that attackers can use these datasets to construct their dictionaries or cracking tools, system administrators can benefit from research and can prepare defences such as improved password policies. This view is also shared by Ur et al., who use three different password dumps to compare

real-world cracking techniques with those proposed in the research literature [114].

Durmuth et al. proposed OMEN, a cracking algorithm that outperforms state of the art crackers [31]. The authors tested their algorithm on leaked databases from MySpace, Facebook and the website RockYou. The authors justify this by claiming that these datasets have been used in several previous studies, and they have been made public. Moreover, they claimed that these data have been treated carefully and they do not reveal actual information about the passwords.

Bonneau used leaked password databases to investigate the statistical properties of passwords and developed the α-guesswork metric for password strength [13]. He notes that "care was taken to ensure that no activities undertaken for research made any user data public which wasn't previously" and rejects "the appropriateness of ever collecting cleartext user passwords, with or without additional identifying information". By this argument, leaking a password database and making a leaked password database more available than it would otherwise be are both unethical.

Researchers mostly use two arguments to justify the ethics of conducting research on password dumps. First, since the passwords are public, studying them might not increase harm and could help advance science. Moreover, since attackers may have access to these lists as well, the defences derived from analysis of these passwords may protect people, making these works of *Public interest*. Second, most authors state that they do not reveal personal information derived from the passwords, and some of them claim that they "treat these lists with the necessary precautions" [31] or that they "treat them as confidential" [121], which should include secure storage of the lists. All the works covered *Identify harms* and provide *Safeguards*. Some authors justify the ethics of their research on the basis that previous research was conducted with these dumps.

Some uses of leaked password databases are clearly not ethical. `leakedsource.com` was shut down and its operators arrested as a result of its use of leaked passwords [61]. It made password hashes (or even cracked passwords) available to anyone who was willing to pay for the access. This is in marked contrast to the ethical service `haveibeenpwned.com` which never makes passwords available and doesn't expose any personal information without verification of control of the email address for that leaked information [44]. `haveibeenpwned.com` maximises benefit by enabling users to find out if their data has been leaked and notifying them if their data is leaked in the future while minimising harm as it does not share private data with anyone or use it for any other purpose.

4.3 Leaked databases

While password dumps are a specific restricted form of data, in this section we consider more general leaking of entire databases that contain more detailed information such as messages or logs of activity. These databases are available in underground forums or from public repositories, sometimes for free. In this section, we cover three cases: Databases of distributed denial of service (DDoS) providers (booters), the Patreon database (a web site aimed at crowd-founding projects), and the databases of several underground forums.

4.3.1 Booter databases leak. Booters (sometimes called stressers) provide DDoS-as-a-Service. While their operators might sometimes claim that this is legal [46], this activity is almost always illegal[2] (*Computer misuse*), and it is also unethical. Several approaches have been used to understand this criminal ecosystem: interviewing operators after contacting them through their websites [46], measuring the attacks they produce [110], and using their leaked databases and source code. Karami et al. analysed a database dump of the TwBooter service. Their *Safeguards* to make this research ethical were to not publish personally identifiable data, except when this was already publicly known [54]. Later they analysed database dumps from Asylum and LizardStresser and scraped data from VDOS [55]. For the latter they obtained an REB exemption on the basis these data did not contain any personally identifiable information and used publicly leaked data. In some jurisdictions (e.g. Germany [115]) IP addresses may be personally identifiable data and the dumps likely contained email addresses which can be similarly identifiable. Santanna et al. analysed database dumps from 15 distinct booters and used Karami's procedures to justify it ethically [93]. Thomas et al. used database dumps and scraped data from booters to evaluate the coverage of their honeypot based measurement of DDoS attacks, they argued that using this data was necessary as there was no other ground truth on attacks initiated by booters [110].

All these papers had some *Identification of stakeholders*, *Identify harms* and used *Safeguards*. These dumps can contain details of user accounts including names, email addresses, password hashes and security questions; details of the backend and frontend servers used for attacks (including compromised hosts); logs of connections to the site including IP addresses and user agent strings; logs of attacks including target IP addresses, ports, domain names and the method used; tickets and messages sent between users and site owners; records of payments; details of pricing plans; and chat logs of site operators. Concretely, Thomas et al. used the attack logs [110]; Santanna et al. [93] and Karami et al. [55] used attack logs, payment records, pricing plans and counts of users. The password hashes could be used for password research and the ticket databases for qualitative research into the attitudes of booter users and operators [46].

4.3.2 Patreon crowd-funding. In October 2015 the Patreon crowd-funding website was hacked and the entire site made available. This included data on projects, private messages, source code, email addresses, and passwords. Poor and Davidson, who were conducting research based on incomplete data obtained by scraping the Patreon website would have

[2]The aim is usually illegal: attempting to stop someone's Internet connection from working; and the mechanism is often also illegal: using UDP amplification attacks that make unauthorised use of misconfigured UDP servers or using botnets of compromised machines.

liked to use this data but concluded it would be unethical to do so [85]. These data were publicly available and the researchers hoped to serve the public through their research. However, it would be hard for them to distinguish between public and private data within the dump, and they might see private data unintentionally. Furthermore using the dump might legitimize criminal activity, violate user's expectations of privacy, and the use of this data would be without their consent. Importantly they also did not need to use this data to do their research, as scraping the Patreon website would also provide the data they needed, without the risk of accidentally including private data. This is an example where the authors *Identify harms* and chose not to use data of illicit origin as a result since they could not ensure that there would be no additional harm.

4.3.3 Underground forums. Underground forums focus on trading, learning and discussing illegal or criminal topics, such as hacking material, credit cards and drugs. These forums often also cover other non-illegal topics, such as video-games, financial help, politics, and sport.

Several forum databases have been leaked in the past. The `worm.ws` forum database was hacked by an anonymous group of hackers under the pseudonym "Peace of Mind", allegedly in response to some prior attack on the forum "Hell" [116]. All the forum content, personal data, as well as exploits and hacking material was made public. The database of `carders.cc`, a German forum focused on financial information trading (such as credit cards or bank accounts) was hacked and leaked [59]. In 2016, the database of the forum `nulled.io` was leaked, containing "536 064 user accounts with 800 593 user personal messages, 5 582 purchase records and 12 600 invoices which seem to include donation records" [90]. Motoyama et al. presented one of the first works analysing underground forums using leaked databases, however, they did not discuss ethics [76]. Yip et al. perform social network analysis using a database of three carding forums (Cardersmarket, Darkmarket and Shadowcrew) which included private messages of the participants [123]. This research showed that forums are a preferred way for criminals to communicate. They do not provide any discussion about the ethics of their research, however they indicate that the marketplace actors are anonymous, so it is not possible to obtain *Informed consent*.

Analysing data from underground forums can provide valuable insights into how markets for stolen data work [47], how malware configurations are shared [45], new forms of criminal networks that arise in cyberspace [76], common goods and assets being traded [86], economy of spam campaigns [103] or even to provide Indicators of Compromise (IoC) and other useful information for threat intelligence [69, 92]. This makes it of *Public interest*. Indeed, the conclusions drawn from these works are undoubtedly valuable to law enforcement agencies and crime prevention strategies that arise as a result can provide social benefits (e.g. preventing terrorist attacks, cyberattacks, or child sexual exploitation). However, there are other ethical considerations: the research should consider potential harms to the users of the forums, including prosecution or physical threat, and compare them with the benefits. None of the works mentioned use *Safeguards* to protect the data, which was originally illegally obtained [116]. Some authors have publicly re-released leaked datasets, even including private information [14, 86]. While the goal is to provide other researchers with datasets to conduct their experiments and for reproducibility, public release means that these datasets are potentially being shared with malicious actors.

4.4 Financial data leaks

Leaks of commercially sensitive data such as data on contracts and client relationships can reveal the hidden behaviour of companies and individuals in ways that would be difficult to achieve through external measurement. In this section we describe the leak of data from a law firm that revealed the financial behaviour of companies and individuals. Leaks of peering arrangements between ISPs together with traffic statistics likely present similar ethical issues, particularly if the data demonstrate illegal behaviour such as contravening network neutrality rules or the imposition of censorship.

Panama / Mossack Fonseca papers leak. In 2015 the internal database of the Panamanian law firm Mossack Fonseca was leaked to the German newspaper Süddeutsche Zeitung, which shared it with the International Consortium of Investigative Journalists (ICIJ) [109]. In 2016 the consortium and its partners released numerous reports based on analysis of the leaked data [42]. World leaders, celebrities, and companies were found to be using Mossack Fonseca's services for tax evasion and other criminal purposes. Some of these data were made publicly available and Europol identified 3 500 criminals among the clients of the firm using this data [84]. There was a substantial *Public interest* to this release as it identified criminal and unethical activity by numerous individuals and companies. This revelation may result in money laundering and tax evasion becoming more difficult in future due to greater transparency, international cooperation, and fear of disclosure. However, not all the clients of Mossack Fonseca were engaged in illegal or unethical behaviour. Trautman surveys the consequences of the leak describing many of the media reports and investigations that resulted from it [111].

Murphy states that money laundering and tax evasion are illegal, while tax avoidance is unethical [77]. He says tax is the rightful property of the government, tax evasion is the theft of the government's rightful property, and tax avoidance is a "con trick". Promoting tax competition between countries is seeking to undermine national sovereignty and subvert the democratic (or other political) process and hence unethical. The Guardian reports that 95% of Mossack Fonseca's work involves selling financial products to avoid taxes [42] and hence almost all of the work they do would be described by Murphy as unethical.

The Panama papers have been of interest to researchers, as well as journalists, and law enforcement. Sharife uses the Panama papers in a historical analysis to understand the downfall of Banco Espírito Santo [97]. Walkowski uses the

Panama papers to argue for reform in legislation to increase transparency and avoid tax competition [117]. O'Donovan et al. evaluated the impact of the Panama papers on firm values and found it reduced market capitalisation of 397 firms implicated in the leak by US$135 billion or 0.7% [79]. Omartian used the Panama papers to investigate investor response to changes in tax legislation in terms of offshore entity usage [82]. He uses the introduction of legislation: European Union Savings Directive (EUSD), Tax Information Exchange Agreements (TIEAs), the Foreign Account Tax Compliance Act (FATCA), and the Common Reporting Standard for information exchange (CRS) as natural experiments, evaluating the impact on offshore activity as revealed by the Panama papers. He finds that they do have a significant impact.

None of these papers explicitly discuss the ethics of using this data; they implicitly argue that they are in the public interest. O'Donovan et al. [79], and Oei and Ring [80] *Identify harms* resulting from the data being released while Omartian provides evidence for tax laws that provide more *Justice* [82].

McGregor et al. use the successful collaborative investigation into the Panama Papers that the ICIJ conducted as a case study of secure collaboration [74]. They used a survey of the journalists who used ICIJ's systems and IRB approved interviews of ICIJ's staff but did not analyse the content of the Panama Papers. They detail many of the safeguards used to protect the data and the investigation.

4.5 Classified materials

In this section we cover two well-known leaks of classified information: Manning's Wikileaks dump and Snowden's NSA data leak. In both cases, classified documents from the USA government detailing war decisions, espionage or diplomatic activities were publicly leaked.

4.5.1 Manning's WikiLeaks dump. In 2010 Chelsea (then Bradley) Manning leaked 700 000 documents and diplomatic cables from the USA's government systems to WikiLeaks [73]. This information was available to more than three million USA government employees [65] and so it is likely that other parties such as Russia and China that have large intelligence agencies would already have had access to at least some of this information. Originally WikiLeaks shared the unredacted documents with carefully selected journalists. However, later journalists published what they believed to be a temporary encryption password only to discover that a copy of the archive encrypted under that password had been shared on BitTorrent [7]. Hence, the full and unredacted cables were publicly released.

The use of WikiLeaks diplomatic cables and documents in the academy is controversial. For example, professors do not agree on the morality of using this information for teaching foreign policy studies, despite the cables being a valuable teaching tool [25]. Barnard "borrowed" classified documents from the "controversial WikiLeaks" to analyse covert relationships between USA and South Africa during the Cold War [9]. The author claims that there were no ethical dilemmas since all the classified data used was open source and declassified. However, there is no evidence that any of Manning's WikiLeaks dump has been declassified. Talarico and Zamparini analysed the smuggling of tobacco in Italy between 2004 and 2014 [105]. They used a confidential document from the American Embassy in Italy, obtained through WikiLeaks that said that the USA government had blacklisted an Italian harbour because of collusion by harbour staff. Berger references several Manning cables to study the international restrictions on the trade of weapons with North Korea [12]. For example, Berger mentioned that the United Arab Emirates bought missiles from North Korea, and a diplomatic cable where USA thanked Iran for its cooperation in blocking one cargo from North Korea.

Researchers have used this data to better understand the diplomatic position of the USA government in several international conflicts. As Barnard points out, these documents are controversial [9]. However, none of the studied works discussed the ethics of their research. Some consider Manning as a traitor while others consider her as a freedom fighter. In the research community, there is no consensus as to whether publishing results based on these documents is ethical, and in general, authors prefer not to confront the question.

4.5.2 Snowden's NSA data leak. In 2013 Edward Snowden, a contractor for the USA's National Security Agency (NSA), leaked large amounts of NSA and GCHQ data to journalists [8]. He was the latest in a long line of NSA leakers who have revealed various aspects of NSA programmes [122]. Landau provides an overview of the data that was revealed by Snowden, covering early leaks [64] and later leaks [63]. She criticises the ethics of some of the leaks since "the specifics on China had little to do with privacy and security of individuals", but is mostly critical of the NSA/GCHQ and the USA and UK governments, and she is mostly positive about Snowden's actions.

Several uses of the Snowden leaks make no mention of the ethical considerations of doing so, but are implicitly critical of the ethics of the activities exposed. In a newspaper article, Schneier uses documents leaked by Snowden to explain how the NSA unconditionally exploits Tor users' browsers to install implants that exfiltrate data [95]. In a magazine article he argues that the metadata collection that was exposed represents ubiquitous surveillance of everyone [96]. RFC 7624 uses the Snowden leaks to inform a threat model for pervasive surveillance, in order to inform protocol design, such that the activities detailed in the Snowden leaks would be more difficult in future [10]. Lustgarten argued in 2015 that the American Psychological Association had not taken account of the Snowden leaks in its 'Ethics Code' and 'Record Keeping Guidelines' as the leaks showed that the NSA would have access to client data stored on cloud servers. Clinicians were responsible for protecting this client data, and had legal protections against enforced disclosure. This then raises ethical concerns for psychologists, as their clients would not have given informed consent for access to their data by the NSA [67].

Others used the fact that the leaks had happened and their impact rather than the actual content of the leaks for their research. Preibusch used Snowden's revelations to conduct an experiment on the privacy behaviour of people after a major privacy incident; he found little change in user behaviour [87].

There has been substantial discussion of whether Snowden's actions were legal and ethical and whether the NSA's activities were legal or ethical. Scheuerman argues that Snowden's actions were ethical civil disobedience and serve as an example of correct behaviour [94]. Kadidal describes the impact on civil liberties of mass surveillance based on what Snowden (and others) revealed [53]. Walsh and Miller provide an ethical and policy analysis of intelligence agency activity on the basis of Snowden's revealing what current practice was [118]. Lucas discusses the application of the principle of informed consent to mass surveillance as revealed by Snowden, suggesting that revealing the outline of what kind of activity is being conducted to the public is necessary for the public to consent to it [66]. Barnett argues that the NSA's activities revealed in the Snowden leaks were unconstitutional under the fourth amendment [11]. Inkster, a former British Secret Intelligence Service Director, provides a counter-narrative, claiming that the exposed activities were not illegal, but rather entirely proper, in particular he states that collecting data on everyone is not mass surveillance if this data is only processed by computer programs and not read by humans [51]. He implicitly argues that the newspapers that published the leaked data acted unethically in doing so and Snowden's actions are clearly depicted as unethical and illegal.

Since the leaked data was classified, and much of it remains classified despite being publicly available, the use of it for research or in court cases may have unexpected difficulties. For example, in 2015 Barton Gellman gave a talk at Purdue University that included some classified NSA slides. Purdue University had a facility security clearance to perform classified USA government research and this incident was treated as a classified information spillage. As a result, the video recording of the talk was destroyed [36]. There is thus an additional risk for researchers at institutions with facility security clearances as if they work with leaked classified data then they may find that all their resulting work is destroyed by facility authorities. In 2017 the UK government was considering making it an offence to obtain sensitive information, and if that became law then any researcher using leaked classified data could be imprisoned, possibly for up to 14 years [34]. In the USA court cases have been thrown out because the evidence that the government had the supplicants under surveillance was classified (even though the supplicants had that evidence) [53]. In contrast, the Vault 7 leak of CIA data [68] contained data that might be expected to be highly compartmentalised Top Secret (source code for weaponised zero day exploits), but, due to the fact that if it were classified it could not be deployed on enemy systems, it was unclassified. Additionally, as the USA government cannot own copyrights, the source code for this state level malware was not even protected by copyright [5]. The lack of legal protections might make it easier for researchers to work with this data.

5 ANALYSIS

In this section we analyse the case studies with respect to the ethical and legal considerations described in Sections 2.1 and 3. We first discuss common justifications made by authors to justify the use (or not) of these data. The main goal is to understand how the authors approached the legal and ethical issues as well as the justifications, safeguards, harms, and benefits. A summary of this analysis is shown in Table 1. The acronyms used for safeguards, harms and benefits in the table are given in brackets below.

5.1 Justifications

We have observed common justifications made by the researchers regarding ethical issues in the case studies, which are summarized in Table 1. Here, we describe them and provide *comments in italics*.

Not the first Previous research using these data was published and peer-reviewed, and so our work must be ethical. *This is a poor argument: not all published work is ethical under current norms, and while the work that was published may have been ethical, if your work does something different with these data then that requires its own justification.* **Public data** Since these data are publicly available, anything we do with these data is ethical. *The ethics of the work must still be considered and in some cases REB review may still be required [32]. Researchers may develop or apply new techniques to public data that, for example, deanonymise these data, and this may cause harm [4].* **No additional harm** Any harms that might arise have already occurred and therefore our work produces benefits and no (or negligible) additional harm it is ethical. *For there to be no additional harms the research should not identify any natural persons and data may need to be stored and managed securely. In some cases any use of the data of illicit origin is considered additional harm, for example with images of child abuse, every viewing is considered additional abuse of the victim.* **Fight malicious use** These data are already used by malicious actors, and so we also need to use these data to defend against them. *If researchers can use the same data to prevent or reduce harm caused by malicious actors, without creating greater harm by doing so, then it may be ethical to do so.* **Necessary data** This research cannot be conducted without using this data. *This might be a good justification if there is sufficient benefit to the work (Public interest) and there is no additional harm.*

5.2 Safeguards

When dealing with leaked data, holders must take care as to how it is processed and stored so as to avoid further disclosure of sensitive information. Here we analyse the actions taken by the researchers to maintain the confidentiality, integrity and privacy of these data and the stakeholders. **Secure storage (SS)** to protect the integrity and confidentiality of these data maintained, e.g. by means of encryption and

access control to avoid accidental leakage. **Privacy (P)** No deanonymisation is attempted and no identities are revealed. **Controlled Sharing (CS)** Researchers publish only partial / anonymised data, provide it under legal agreements that prevent harms or do not make these data publicly available. This includes approaches such as letting researchers visit the institution holding the data to analyse it, or the holding institution performing analysis on behalf of other researchers, such as by running their code.

5.3 Harms

Conducting research using data containing sensitive information entails risks dependant on the consequences of the data gathering, the research itself, or any further leakage of these data maintained by the researchers. In general only harms to natural persons (rather than corporate persons), or to the environment, are considered during ethical review. **Illicit measurement (I)** Research obtained these data by means of illicit activities such as hacking or paying the offenders, which can lead to researchers being prosecuted. **Potential Abuse (PA)** Research results from these data can be used by malicious actors to cause additional harm, for example by means of designing evasive malware or updating password cracking policies. **De-Anonymization (DA)** Research on these data can be used to de-anonymise or re-identify people or networks. Also, identification of group of individuals may raise ethical concerns such as discrimination or violence towards identified groups [35]. **Sensitive Information (SI)** These data contains sensitive and private information, which can be used to harm natural persons. For example, if the user password from one service is leaked, their credentials to other services can be compromised due to password reuse [24]. **Researcher Harm (RH)** The research can lead to the researchers being prosecuted by law enforcement, since these data may include illegal material. Researchers could be threatened by criminals, e.g. in underground forums [72], or by state or industry actors that dislike the work. There may also be a risk of emotional trauma to researchers if they come across distressing content, such as pornography or violence, during the work. **Behavioural Change (BC)** The research can change the behaviour of the stakeholders of these data, which may have negative consequences. For example, a market vendor can provide fake information if she knows that she is being measured [101]. Alternatively the research may encourage future collection or use of data of illicit origin.

5.4 Benefits

In this section, we enumerate academic and social benefits particular to research using data of illicit origin. **Reproducibility (R)** The data allows the comparison of different algorithms or tools. This is the great benefit of data sharing, but **Controlled Sharing** is required when these data contains sensitive information. **Uniqueness (U)** Data is either unique (cannot be obtained through other means) or historical (can no longer be obtained by other means), so similar measurements on the same topic are hard or even impossible to attain. This only becomes a benefit if the data is also useful. **Defence Mechanisms (DM)** Data can be used to study the underground economy, new forms of cybercrime or new attack techniques. This allows new defences to be designed, such as anti-malware tools or efficient password policies. **Anthropology and Transparency (AT)** Data contains ground truth on the behaviour of human beings, which other methods could only obtain in a filtered or biased way. For example, data can reveal real human behaviour when creating passwords without the reporting bias of surveys or experiments with human participants. Additionally, data can provide transparency through information that aids understanding of government surveillance activities, external relationships, or of company behaviour. The additional transparency into state or corporate actors may have greater benefits than if the data concerned individuals, as it may have additional public benefit by providing checks and balances on power.

5.5 Discussion

We observe a wide variation in the ethical issues mentioned by the authors and their justifications for using these data, even when they are using the same data. This is clear from studying Table 1. Two works stated that they were exempt from REB approval, two received REB approval and 24 did not mention REBs. The reasons given for exemption were: no human subjects or ethical concerns [110]; no personally identifiable information (despite email addresses and IPs) and public data [55]. Both of these works used *Safeguards* to mitigate potential *Harms* and have clear ethical justifications. These exemptions are all based on the absence of direct human subjects. However, in each case they were measuring human behaviour and if they had tried to identify individuals they might have been successful. The absence of human subjects appears an artificial distinction in these cases, as there were human participants. Both of the papers that received REB approval [57, 24] obtained it not because of their usage of data of illicit origin, but because they also conducted surveys or other human subject research. Not having REB approval solely on the basis that data is public is contrary to the opinions of experts [32], since this data may contain private information.

Explicit ethics sections were included in 12 of the 28 papers. However, since we specifically selected papers for this table because they talked about ethics, this is unlikely to be representative. Nonetheless, it does show that a high proportion of papers using data of illicit origin do already have ethics sections. We do not have enough information to show any trend in this behaviour, and because we would expect this behaviour to be field dependent, we would need a large representative sample from each field to be able to show any trend.

Discussion of safeguards, harms and benefits in the papers is highly variable. We included those that were implicitly or explicitly discussed in the papers. However, we are aware

Category	Sources	Reference	Year 20XX	Legal issues: *Computer misuse*	*Copyright*	*Data privacy*	*Terrorism*	*Indecent images*	*National security*	Ethical issues: *Identification of stakeholders*	*Identify harms*	*Safeguards*	*Justice*	*Public interest*	Justifications: Not the first	Public data	No additional harm	Fight malicious use	Necessary data	Ethics section	REB approval	Safeguards	Harms	Benefits
Malware & exploitation	AT&T database	[106][a]	10	•		•				✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗		I,PA,SI,RH	
	Pushdo/Cutwail botnet	[103]	11	•	•	•				✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗			R,U,DM
	30 exploit kits	[58]	13	•	•					✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗			DM,AT
	Carna Scan	[18][a]	13	•						✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗			
		[70]	13	•						✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✗	P,CS	PA	
		[62][a]	14	•						✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗			
		[27][b]	14	•						✓	✓	✓	✓	✓						✓	∅		RH,BC	
	151 malware pieces	[17]	16	•	•					✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	CS		R,U,AT
Password dumps[e]	MS + 2 others	[121]	09	•		•				✗	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	SS,P,CS	SI,BC	R,DM
	MS,RY + 4 others	[57]	12	•		•				✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	P	SI	DM
	MS,YV,FB + 7 others	[24]	14	•		•				✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	P	SI	DM,AT
	MS,RY,YV	[114]	15	•		•				✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	P	SI	DM
	MS,RY,FB	[31]	15	•		•				✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	SS,P	SI	DM
Leaked databases	6 underground forums	[76]	11	•	•	•	•	•		✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗			U,DM,AT
	3 carding forums	[123]	13	•	•	•	•			✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗			DM,AT
	TwBooter	[54]	13	•	•	•				✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓	✗	P	SI	
	TwBooter, 14 others	[93]	13	•	•	•				✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	P	SI	
	Asylum, Lizard, Vdos	[55]	15	•	•	•				✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	E	P	SI	
	Patreon	[85][c]	16	•	•	•				✓	✓	✓	✓	✓	✗	✓	●	✗	✓	✓	∅		SI,RH	U,AT
	Vdos, CMDBooter	[110]	17	•		•				✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	E	P,CS	SI,BC	U,AT
	4 underground forums	[86]	17	•	•	•	•	•		✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗			R,DM,AT
Classified materials	Manning Wikileaks	[12]	15	•		•	•		•	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗			
		[9][a]	16	•		•	•		•	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗			
		[105]	17	•		•	•		•	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗			
	Snowden NSA leaks	[64]	13	•	•	•	•		•	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗			
		[95][a]	13	•	•	•	•		•	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗			
		[10]	15	•	•	•	•		•	✗	✗	✗	✓	✓	✗	✗	✗	✓[d]	✗	✗	✗			
		[118]	16	•	•	•	•		•	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗			
Financial data	Mossack Fonseca database	[82]	16	•	•	•	•			✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗			DM
		[79]	16	•	•	•	•			✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗		BC	

[a] These works were not peer reviewed. [b] This paper analysed the ethics of the Carna scan and its use, but did not use it. [c] The authors did not use the leaked database. [d] Here the argument is that the NSA is the malicious actor. [e] MS: MySpace, RY: RockYou, FB: Facebook, YV: Yahoo Voices

Table 1: Summary of the legal/ethical issues and the justifications made by the authors for each paper. Legal issues are defined in §3, ethical issues in §2.1 and justifications in §5.1. • means that the legal issue is applicable (even if it was not discussed). ✓ means the issue was discussed or the justification was used, ✗ means it was not. ● means that the authors decided that the work could not be justified and did not use the dataset. In the REB approval column, ∅ means not applicable and E means exempt. Safeguards: SS Secure Storage, P Privacy, CS Controlled Sharing. Harms: I Illicit measurement, PA Potential Abuse, DA De-Anonymization, SI Sensitive Information, RH Researcher Harm, BC Behavioural Change. Benefits: R Reproducibility, U Uniqueness, DM Defence Mechanisms, AT Anthropology and Transparency.

that many more would apply but they were not mentioned explicitly. In general, we observe that researchers appear to be more reluctant to express the potential harms resulting from their work than their benefits.

Privacy preservation is one of the safeguards applied most frequently, since it is easy to do (e.g. by refusing to attempt to de-anomymize a data set or refusing to reveal private information). Only four of the papers discussed controlled sharing (CS). To provide the maximum benefit, papers need to be reproducible and so while open data is often not appropriate for data of illicit origin, controlled sharing of data with researchers is important. It is possible the authors would be willing to share if they were asked, but mentioning this increases the likelihood it will happen. There is a cost in controlled sharing as it places a burden on the authors of the work to put a robust legal framework in place and an ongoing cost of vetting requests to access the data. However, this cost can be delegated, for example using initiatives such as IMPACT [49] in the USA or the Cambridge Cybercrime Centre [20] in the UK.

6 CONCLUSION

It is common to see research using data of illicit origin, such as leaked databases or classified documents. The use of these data provide researchers with the opportunity to test their hypotheses against ground truth data. For example, it improves our understanding of the evolution of malware or how users re-use passwords. This in turn helps to improve cyber defenses or password policies. However, these data were originally collected by illicit means, and the research community must be aware of the ethical considerations of using such data.

By analysing current advice and previous work on ethics, we have drawn out a set of ethical issues that should be considered and reported when publishing results based on data of illicit origin. However, we have shown that there is a lack of consistency in the consideration of ethical issues, which results in cases where insufficient safeguards are used to prevent harm. Few authors consulted their institution REB, and in most cases they were exempted on the basis that there were no human subjects involved in the research. This narrow focus on whether the research involves "human subjects", rather than a risk based analysis of the potential harms to human participants is unhelpful. If research has potential to harm humans, even in absence of direct human subjects, REB approval should be sought. REBs may need to adapt to understand the possible affect on humans of research in Information Communication Technology Research (ICTR), and to provide timely and well informed responses.

In any case, papers using data of illicit origin should always have an ethics section, explaining how these data were obtained, how it has been protected, analysing the harms, benefits, and need for using such data. Conferences and journals should explicitly require such ethics sections and highlight the importance of considering ethics in their Calls for Papers. Researchers using data that has been shared with them under acceptable usage policies should, as Allman and Paxson suggest, cite the acceptable usage policy they are operating under [4]. Data providers should make their acceptable usage policies publicly available so that they can be cited. Additionally, current efforts to advise on ethics, such as the Menlo Report [28], should be updated and extended to provide a more comprehensive coverage of ICTR and legal considerations to guide researchers aiming to use datasets of illicit origin. Ethics is an issue that is receiving greater interest within ICTR and standards are improving. Hence, we are hopeful that in the future better information on current practice, and better guidance, will be available.

ACKNOWLEDGMENTS

Daniel R. Thomas is supported by a grant from ThreatSTOP Inc. All authors are supported by the EPSRC [grant number EP/M020320/1]. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect those of any of the funders. Thanks to José Jair Santanna, Alan Blackwell, Justin Schlosberg, Brian Trammell (our shepherd) and to the anonymous reviewers for helpful comments on this paper.

REFERENCES

[1] 1984. 18 U.S. Code § 1030 – Fraud and related activity in connection with computers. https://www.law.cornell.edu/uscode/text/18/1030.

[2] 2003. 18 U.S. Code § 1466A – Obscene visual representations of the sexual abuse of children. (Apr. 30, 2003). https://www.law.cornell.edu/uscode/text/18/1466A.

[3] Charu C. Aggarwal. 2005. On k-anonymity and the curse of dimensionality. In *Proceedings of the 31st International Conference on Very Large Data Bases* (VLDB '05). VLDB Endowment, Trondheim, Norway, 901–909. ISBN: 1-59593-154-6.

[4] Mark Alllman and Vern Paxson. 2007. Issues and etiquette concerning use of shared measurement data. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. ACM, 135–140.

[5] Julian Assange. 2017. Vault 7: CIA hacking tools revealed. WikiLeaks. (Mar. 2017). Retrieved Mar. 7, 2017 from https://wikileaks.org/ciav7p1/, https://archive.fo/iK4kO.

[6] Associated Press in Manila. 2016. Kill drug dealers and I'll give you a medal, says Philippines president. theguardian. Retrieved Sept. 28, 2017 from https://www.theguardian.com/world/2016/jun/05/kill-drug-dealers-medal-philippines-president-rodrigo-duterte, https://perma.cc/5KTA-VR5R.

[7] James Ball. 2011. Unredacted US embassy cables available online after WikiLeaks breach. theguardian. (Sept. 2011). Retrieved Feb. 24, 2017 from https://www.theguardian.com/world/2011/sep/01/unredacted-us-embassy-cables-online, https://archive.fo/ozPM7.

[8] James Ball, Julian Borger, and Glenn Greenwald. 2013. Revealed: How US and UK spy agencies defeat Internet privacy and security. theguardian. (Sept. 2013). Retrieved Feb. 23, 2017 from https://www.theguardian.com/world/2013/sep/05/nsa-

gchq-encryption-codes-security, https://archive.fo/960QN.

[9] Tjaart Barnard. 2016. *A cold relationship: United States foreign policy towards South Africa, 1960–1990*. Ph.D. Dissertation. Stellenbosch University.

[10] Richard Barnes, Bruce Schneier, Cullen Jennings, Ted Hardie, Brian Trammell, Christian Huitema, and Daniel Borkmann. 2015. RFC 7624: Confidentiality in the face of pervasive surveillance: A threat model and problem statement. Informational RFC. Internet Architecture Board (IAB), (Aug. 2015), 1–24.

[11] Randy Barnett. 2015. Why the NSA data seizures are unconstitutional. *Harvard Journal of Law & Public Policy*, 38, 1, 3–20.

[12] Andrea Berger. 2015. North Korea in the global arms market. *Whitehall Papers*, 84, 1, 12–34. Taylor & Francis.

[13] Joseph Bonneau. 2012. Guessing human-chosen secrets. Tech. rep. 819. University of Cambridge, Computer Laboratory, (May 2012). http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-819.html.

[14] Gwern Branwen et al. 2015. Dark net market archives, 2011-2015. (July 2015). Retrieved Mar. 14, 2017 from http://www.gwern.net/DNM%20archives, https://perma.cc/2Z76-JJ6W.

[15] Aaron J. Burstein. 2008. Conducting cybersecurity research legally and ethically. In *Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET)*. USENIX, 8:1–8:8.

[16] Aylin Caliskan-Islam, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi, and Rachel Greenstadt. 2015. De-anonymizing programmers via code stylometry. In *24th USENIX Security Symposium (USENIX Security), Washington, DC*.

[17] Alejandro Calleja, Juan Tapiador, and Juan Caballero. 2016. A look into 30 years of malware development from a software metrics perspective. In *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. Springer, 325–345.

[18] 2013. Carna Botnet Scans. CAIDA website. (May 28, 2013). Retrieved Feb. 17, 2017 from https://www.caida.org/research/security/carna/, https://archive.fo/uTygt.

[19] Jonathan Cave. 2016. The ethics of data and of data science: an economist's perspective. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 374, 2083. The Royal Society. ISSN: 1364-503X. DOI: 10.1098/rsta.2016.0117.

[20] Richard Clayton, Julia Powles, and Cambridge University Legal. 2016. Cambridge Cybercrime Centre: Legal framework. Retrieved Sept. 28, 2017 from https://www.cambridgecybercrime.uk/data.html, https://perma.cc/6KM5-K4Q3.

[21] 1990. Computer Misuse Act. http://www.legislation.gov.uk/ukpga/1990/18/contents.

[22] Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union, (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[23] British Society of Criminology. 2015. Statement of ethics. Retrieved Sept. 28, 2017 from http://www.britsoccrim.org/ethics/, https://perma.cc/K3MY-UG5U.

[24] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse. In *Network and Distributed System Security Symposium (NDSS)*, 23–26. DOI: 10.14722/ndss.2014.23357.

[25] Jessica Deahl. 2011. Professors differ on ethics of using WikiLeaks cables. NPR. (Feb. 7, 2011). Retrieved Mar. 29, 2017 from http://www.npr.org/2011/02/07/133334302/professors-differ-on-ethics-of-using-wikileaks-cables, https://archive.fo/Q6782.

[26] David Dittrich, Michael Bailey, and Erin Kenneally. 2013. Applying ethical principles to information and communication technology research: A companion to the Menlo Report. Tech. rep. U.S. Department of Homeland Security, (Oct. 2013). DOI: 10.2139/ssrn.2342036.

[27] David Dittrich, Katherine Carpenter, and Manish Karir. 2014. An ethical examination of the Internet Census 2012 dataset: A Menlo report case study. In *IEEE International Symposium on Ethics in Science, Technology and Engineering (ETHICS)*. IEEE, (May 2014). DOI: 10.1109/ETHICS.2014.6893416.

[28] David Dittrich and Erin Kenneally. 2012. The Menlo Report: Ethical principles guiding information and communication technology research. Tech. rep. U.S. Department of Homeland Security, (Aug. 2012). DOI: 10.2139/ssrn.2445102.

[29] David Dittrich, Felix Leder, and Tillmann Werner. 2010. A case study in ethical decision making regarding remote mitigation of botnets. *International Conference on Financial Cryptography and Data Security (FC)*, LNCS 6054, 216–230. DOI: 10.1007/978-3-642-14992-4_20.

[30] John E. Dunn. 2013. AT&T hacker 'Weev' sentenced to 41 months for iPad leak. techworld. (Mar. 2013). Retrieved Feb. 17, 2017 from http://www.techworld.com/news/security/att-hacker-weev-sentenced-41-months-for-ipad-leak-3435985/, https://archive.fo/NCASE.

[31] Markus Dürmuth, Fabian Angelstorf, Claude Castelluccia, Daniele Perito, and Abdelberi Chaabane. 2015. OMEN: Faster password guessing using an ordered Markov enumerator. In *International Symposium on Engineering Secure Software and Systems*. Springer, 119–132.

[32] Serge Egelman, Joseph Bonneau, Sonia Chiasson, David Dittrich, and Stuart Schechter. 2012. It's not stealing if you need it: A panel on the ethics of performing research using public data of illicit origin. In *International Conference on Financial Cryptography and Data Security (FC)*. Vol. LNCS 7398, 124–132. DOI: 10.1007/978-3-642-34638-5_11.

[33] Charles Ess and AoIR ethics working Committee. 2002. Ethical decision-making and Internet research. Association of Internet Research Ethics Working Committee. (Nov. 2002). Retrieved Sept. 28, 2017 from http://aoir.org/reports/ethics.pdf, https://perma.cc/69UY-ETC7.

[34] Rob Evans, Ian Cobain, and Nicola Slawson. 2017. Government accused of 'full-frontal attack' on whistleblowers. theguardian. (Feb. 2017). Retrieved Sept. 28, 2017 from https://www.theguardian.com/uk-news/2017/feb/12/uk-government-accused-full-frontal-attack-prison-whistleblowers-media-journalists, https://archive.fo/ZwdDK.

[35] Luciano Floridi and Mariarosaria Taddeo. 2016. What is data ethics? *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 374, 2083. The Royal Society. ISSN: 1364-503X. DOI: 10.1098/rsta.2016.0360.

[36] Barton Gellman. 2015. I showed leaked NSA slides at Purdue, so feds demanded the video be destroyed. arstechnica. (Oct. 2015). Retrieved Feb. 9, 2017 from https://arstechnica.co.uk/tech-policy/2015/10/i-showed-leaked-nsa-slides-at-purdue-so-feds-demanded-the-video-be-destroyed/, https://archive.fo/Fkc87.

[37] 2013. German criminal code Section 184b: Distribution, acquisition and possession of child pornography. (Oct. 10, 2013). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1659.

[38] 2013. German criminal code Section 202a: Data espionage. (Oct. 10, 2013). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1749.

[39] 2013. German criminal code Section 263a: Computer fraud. (Oct. 10, 2013). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2187.

[40] 2013. German criminal code Section 303a: Data tampering. (Oct. 10, 2013). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2479.

[41] 2013. German criminal code Section 303b: Computer sabotage. (Oct. 10, 2013). https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2479.

[42] Guardian Reporters. 2016. Panama Papers: a special investigation. theguardian. (Apr. 2016). Retrieved Feb. 23, 2017 from https://www.theguardian.com/news/series/panama-papers, https://archive.fo/g13Sn.

[43] Thorsten Holz. 2005. A short visit to the bot zoo [malicious bots software]. *IEEE Security & Privacy*, 3, 3, 76–79. IEEE. DOI: 10.1109/MSP.2005.58.

[44] Troy Hunt. 2017. Thoughts on the LeakedSource take down. troyhunt.com. (Jan. 2017). Retrieved Mar. 1, 2017 from https://www.troyhunt.com/thoughts-on-the-leakedsource-take-down/, https://archive.fo/xSMBe.

[45] Alice Hutchings and Richard Clayton. 2017. Configuring Zeus: A case study of online crime target selection and knowledge transmission. In *APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Scottsdale, AZ, USA. DOI: 10.1109/ECRIME.2017.7945052.

[46] Alice Hutchings and Richard Clayton. 2016. Exploring the Provision of Online Booter Services. *Deviant Behaviour*, 37, 10, 1163–1178. Taylor & Francis. ISSN: 0163-9625. DOI: 10.1080/01639625.2016.1169829.

[47] Alice Hutchings and Thomas J. Holt. 2015. A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55, 3, 596–614. ISSN: 14643529. DOI: 10.1093/bjc/azu106.

[48] M. Ilešič, A. Prechal, A. Rosas, C. Toader, and E. Jarašiūnas. 2016. Breyer v Germany: Judgement of the court (Second Chamber). InfoCuria - Case-law of the Court of Justice. (Oct. 2016). Retrieved Feb. 21, 2017 from http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN&cid=1095511, https://archive.fo/kl3m7.

[49] 2017. IMPACT cyber trust. Retrieved May 15, 2017 from https://www.impactcybertrust.org/, https://perma.cc/Y7FG-9QU7.

[50] Information Commisioners Office (ICO). 2017. Overview of the General Data Protection Regulation (GDPR). (2017). Retrieved Aug. 11, 2017 from https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/, https://perma.cc/LZ9W-UQNR.

[51] Nigel Inkster. 2014. The Snowden Revelations: Myths and misapprehensions. *Survival*, 56, 1, 51–60. ISSN: 0039-6338. DOI: 10.1080/00396338.2014.882151.

[52] Mark Israel. 2004. Strictly confidential? Integrity and the disclosure of criminological and socio-legal research. *British Journal of Criminology*, 44, 5, 715–740. DOI: 10.1093/bjc/azh033.

[53] Shayana Kadidal. 2014. NSA surveillance: The implications for civil liberties. *I/S: A Journal of Law and Policy for the Information Society*, 10, 2, 433–480. Heinonline.

[54] Mohammad Karami and Dammon McCoy. 2013. Rent to pwn: Analyzing commodity booter DDoS services. *Usenix login;* 38, 6, 20–23. USENIX.

[55] Mohammad Karami, Youngsam Park, and Damon McCoy. 2016. Stress testing the Booters: Understanding and undermining the business of DDoS services. In *Proceedings of the 25th International Conference on World Wide Web (WWW)*. ACM, 1033–1043. DOI: 10.1145/2872427.2883004.

[56] Brian C. Keegan and J. Nathan Matias. 2015. Actually, it's about ethics in computational social science: A multi-party risk-benefit framework for online community research. In *CSCW workshop on human centered data science*.

[57] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. 2012. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *IEEE Symposium on Security and Privacy (SP)*. IEEE. San Francisco, CA, USA, 523–537. DOI: 10.1109/SP.2012.38.

[58] Vadim Kotov and Fabio Massacci. 2013. Anatomy of exploit kits. In *International Symposium on Engineering Secure Software and Systems (ESSoS)*. Springer, 181–196. DOI: 10.1007/978-3-642-36563-8_13.

[59] Brian Krebs. 2010. Fraud bazaar Carders.cc hacked. KrebsonSecurity. (May 2010). Retrieved Apr. 10, 2017 from https://krebsonsecurity.com/2010/05/fraud-bazaar-carders-cc-hacked/, https://perma.cc/P2JT-HJGJ.

[60] Brian Krebs. 2016. Source code for IoT botnet 'Mirai' released. KrebsonSecurity. (Oct. 2016). Retrieved Feb. 23, 2017 from https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, https://archive.fo/cNPLI.

[61] Brian Krebs. 2017. Who ran Leakedsource.com? KrebsonSecurity. (Feb. 2017). Retrieved Feb. 17, 2017 from https://krebsonsecurity.com/2017/02/who-ran-leakedsource-com/, https://archive.fo/9ZHIQ.

[62] Thomas Krenc, Oliver Hohlfeld, and Anja Feldmann. 2014. An Internet census taken by an illegal botnet — A qualitative assessment of published measurements. *ACM SIGCOMM Computer Communication Review*, 44, 3, 103–111. ACM. DOI: 10.1145/2656877.2656893.

[63] Susan Landau. 2014. Highlights from making sense of Snowden, Part II: What's significant in the NSA revelations. *IEEE Security & Privacy*, 12, 1, 62–64. IEEE. DOI: 10.1109/MSP.2013.161.

[64] Susan Landau. 2013. Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, 11, 4, 54–63. IEEE. DOI: 10.1109/MSP.2013.90.

[65] David Leigh. 2010. US embassy cables leak sparks global diplomatic crisis. theguardian. (Nov. 2010). Retrieved Feb. 23, 2017 from https://www.theguardian.com/world/2010/nov/28/us-embassy-cable-leak-diplomacy-crisis, https://archive.fo/TQz0I.

[66] George R. Lucas. 2014. NSA management directive #424: Secrecy and privacy in the aftermath of Edward Snowden. *Ethics & International Affairs*, 28, 1, 29–38. DOI: 10.1017/S0892679413000488.

[67] Samuel D. Lustgarten. 2015. Emerging ethical threats to client privacy in cloud communication and data storage. *Professional Psychology: Research and Practice*, 46, 3, 154. American Psychological Association.

[68] Ewen MacAskill. 2017. WikiLeaks publishes 'biggest ever leak of secret CIA documents'. theguardian. (Mar. 2017). Retrieved Mar. 7, 2017 from https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance, https://archive.fo/Ce80x.

[69] Mitch MacDonald, Richard Frank, Joseph Mei, and Bryan Monk. 2015. Identifying digital threats in a hacker web forum. In *Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on*. IEEE, 926–933.

[70] Erwan Le Malécot and Daisuke Inoue. 2014. The Carna Botnet through the lens of a network telescope. *Foundations and Practice of Security*, LNCS 8352, 426–441. Springer. DOI: 10.1007/978-3-319-05302-8_26.

[71] Annette Markham and Elizabeth Buchanan. 2012. Ethical decision-making and Internet research: Recommendations from the AoIR Ethics Working Committee (Version 2.0). AOIR, (Aug. 2012), 1–19. http://www.aoir.org/documents/ethics-guide.

[72] James Martin and Nicolas Christin. 2016. Ethics in cryptomarket research. *International Journal of Drug Policy*, 35, 84–91. Elsevier. DOI: 10.1016/j.drugpo.2016.05.006.

[73] Ciara McCarthy. 2017. Chelsea Manning thanks Barack Obama for 'giving me a chance'. theguardian. (Jan. 2017). Retrieved Feb. 24, 2017 from https://www.theguardian.com/us-news/2017/jan/19/chelsea-manning-thanks-barack-obama-commuted-sentence, https://archive.fo/jFtmJ.

[74] Susan E. McGregor, Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Kelly Caine, and Franziska Roesner. 2017. When the weakest link is strong: Secure collaboration in the case of the Panama Papers. In *26th USENIX Security Symposium (USENIX Security)*. USENIX, Vancouver, BC, Canada, (Aug. 2017), 505–522. ISBN: 9781931971409.

[75] Tyler Moore and Richard Clayton. 2012. Ethical dilemmas in take-down research. *Financial Cryptography and Data Security (FC 2011)*, LNCS 7126, 154–168. DOI: 10.1007/978-3-642-29889-9_14.

[76] Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. An analysis of underground forums. In *Proceedings of the ACM SIGCOMM Internet measurement conference (IMC)*. ACM, 71–80.

[77] Richard Murphy. 2015. *The Joy of Tax*. Bantam Press. ISBN: 978-0593075173.

[78] Arvind Narayanan and Bendert Zevenbergen. 2015. No encore for Encore? Ethical questions for web-based censorship measurement. *Technology Science*, 1–23. ISSN: 1556-5068. DOI: 10.2139/ssrn.2665148.

[79] James O'Donovan, Hannes Wagner, and Stefan Zeume. 2017. The Value of Offshore Secrets – Evidence from the Panama Papers. https://ssrn.com/abstract=2771095.

[80] Shu-Yi Oei and Diane M. Ring. 2018. Leak-driven law. *UCLA Law Review*, 65. DOI: 10.2139/ssrn.2918550.

[81] Paul Ohm, Douglas C. Sicker, and Dirk Grunwald. 2007. Legal issues surrounding monitoring during network research. *Proceedings of the 7th ACM SIGCOMM Internet measurement conference (IMC)*, 141–148. DOI: 10.1145/1298306.1298307.

[82] Jim Omartian. 2016. Tax information exchange and offshore entities: Evidence from the Panama Papers. DOI: 10.2139/ssrn.2836635.

[83] Craig Partridge and Mark Allman. 2016. Ethical considerations in network measurement papers. *Communications of the ACM*, 59, 10, 58–64. DOI: 10.1145/2896816.

[84] David Pegg. 2016. Panama Papers: Europol links 3,500 names to suspected criminals. theguardian. (Dec. 2016). Retrieved Feb. 23, 2017 from https://www.theguardian.com/news/2016/dec/01/panama-papers-europol-links-3500-names-to-suspected-criminals, https://archive.fo/NGkLj.

[85] Nathaniel Poor and Roei Davidson. 2016. The ethics of using hacked data: Patreon's data hack and academic data standards. Data and Society. Tech. rep. Council for big data, ethics and society, (Mar. 2016), 1–7. Retrieved Sept. 28, 2017 from http://bdes.datasociety.net/council-output/case-study-the-ethics-of-using-hacked-data-patreons-data-hack-and-academic-data-standards/, https://perma.cc/H8T6-QPYK.

[86] Rebecca Portnoff, Sadia Afroz, Greg Durrett, Jonathan Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko, and Vern Paxson. 2017. Tools for automated analysis of cybercriminal markets. In *Proceedings of 26th International World Wide Web conference (WWW)*. ACM, 657–666. DOI: 10.1145/3038912.3052600.

[87] Sören Preibusch. 2015. Privacy Behaviors After Snowden. *Communications of the ACM*, 58, 5, 48–55. ACM. DOI: 10.1145/2663341.

[88] 1978. Protection of Children Act. http://www.legislation.gov.uk/ukpga/1978/37/contents.

[89] Ronald E. Rice and Christine L. Borgman. 1983. The use of computer-monitored data in information science and communication research. *Journal of the American Society for Information Science and Technology*, 34, 4, 247–256. DOI: 10.1002/asi.4630340404.

[90] Risk-based-security. 2016. Nulled.IO: Should've expected the unexpected! Risk Based Security. (May 2016). Retrieved Apr. 28, 2017 from https://www.riskbasedsecurity.com/2016/05/nulled-io-shouldve-expected-the-unexpected/.

[91] Bob Rudis and Deral Heiland. 2016. From Carna to Mirai: Recovering from a lost opportunity. DarkReading. (Dec. 8, 2016). Retrieved Feb. 22, 2017 from http://www.darkreading.com/endpoint/from-carna-to-mirai-recovering-from-a-lost-opportunity/a/d-id/1327633, https://archive.fo/2hGOt.

[92] Sagar Samtani, Ryan Chinn, and Hsinchun Chen. 2015. Exploring hacker assets in underground forums. In *IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 31–36.

[93] José Jair Santanna, Romain Durban, Anna Sperotto, and Aiko Pras. 2015. Inside booters: An analysis on operational databases. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 432–440. DOI: 10.1109/INM.2015.7140320.

[94] William E. Scheuerman. 2014. Whistleblowing as civil disobedience: The case of Edward Snowden. *Philosophy & Social Criticism*, 40, 7, 609–628. DOI: 10.1177/0191453714537263.

[95] Bruce Schneier. 2013. Attacking Tor: how the NSA targets users' online anonymity. *The Guardian*, (Oct. 2013). Retrieved Apr. 3, 2017 from https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, https://archive.fo/gpShR.

[96] Bruce Schneier. 2014. Metadata = Surveillance. *IEEE Security and Privacy*, 12, 2, 84. IEEE. ISSN: 1540-7993. DOI: 10.1109/MSP.2014.28.

[97] Khadija Sharife. 2016. Out of luck: The fall of Banco Espírito Santo. *World Policy Journal*, 33, 3, 107–111. World Policy Institute. DOI: 10.1215/07402775-3713077.

[98] Tom Simonite. 2012. Jail looms for man who revealed AT&T leaked iPad user e-mails. MIT Technology Review. (Nov. 2012). Retrieved Feb. 17, 2017 from https://www.technologyreview.com/s/507661/jail-looms-for-man-who-revealed-att-leaked-ipad-user-e-mails/, https://archive.fo/s35I8.

[99] Timur Snoke, Deana Shick, and Angela Horneman. 2013. Working with the Internet Census 2012. CERT/CC Blog. (Oct. 2013). Retrieved Feb. 17, 2017 from https://insights.sei.cmu.edu/cert/2013/10/working-with-the-internet-census-2012.html, https://archive.fo/gOO7R.

[100] Christopher Soghoian. 2008. Legal risks for phishing researchers. *eCrime Researchers Summit*. IEEE. ISSN: 1556-5068. DOI: 10.1109/ECRIME.2008.4696971.

[101] Kyle Soska and Nicolas Christin. 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *24th USENIX Security Symposium*, August, 33–48.

[102] Eugene H. Spafford. 1992. Are computer hacker break-ins ethical? *The Journal of Systems and Software*, 17, 1, 41–47. DOI: 10.1016/0164-1212(92)90079-Y.

[103] Brett Stone-Gross, Thorsten Holz, Gianluca Stringhini, and Giovanni Vigna. 2011. The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns. *Large-scale exploits and emergent threats (LEET)*.

[104] Alexandra Strigunkova. 2015. "To whom it's not concern" (ethical problems of information leaks research). PasswordsCon. Retrieved Feb. 23, 2017 from https://www.youtube.com/watch?v=XM5MO07fvtM. Video.

[105] Luca Talarico and Luca Zamparini. 2017. Intermodal transport and international flows of illicit substances: Geographical analysis of smuggled goods in Italy. *Journal of Transport Geography*, 60, 1–10. Elsevier.

[106] Ryan Tate. 2010. Apple's worst security breach: 114,000 iPad owners exposed. Gawker. (June 2010). Retrieved Feb. 17, 2017 from http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed, https://archive.fo/XqVE8.

[107] Ryan Tate. 2010. FBI investigating iPad breach (update). Gawker. (June 2010). Retrieved Feb. 17, 2017 from http://gawker.com/5560542/fbi-investigating-ipad-breach, https://archive.fo/P1A9d.

[108] 2000. Terrorism Act. http://www.legislation.gov.uk/ukpga/2000/11/contents.

[109] The International consortium of Investigative Journalists (ICIJ). 2016. The Panama papers: Politicians, criminals and the rogue industry that hides their cash. ICIJ website. (Apr. 2016). Retrieved Feb. 23, 2017 from https://panamapapers.icij.org/, https://archive.fo/aC51M.

[110] Daniel R. Thomas, Richard Clayton, and Alastair R. Beresford. 2017. 1000 days of UDP amplification DDoS attacks. In *APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Scottsdale, AZ, USA. DOI: 10.1109/ECRIME.2017.7945057.

[111] Lawrence J. Trautman. 2016. Following the money: Lessons from the Panama Papers. *Penn State Law Review*, 1–77. https://ssrn.com/abstract=2783503.

[112] United Nations General Assembly. 1948. Universal Declaration of Human Rights. United Nations. http://www.un.org/en/universal-declaration-human-rights/.

[113] Universities UK. 2012. Oversight of security-sensitive research material in UK universities: guidance. (Oct. 2012), 16 pages. Retrieved Sept. 28, 2017 from http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2012/oversight-of-security-sensitive-research-material.pdf, https://perma.cc/U8N7-KG6X.

[114] Blase Ur et al. 2015. Measuring real-world accuracies and biases in modeling password guessability. In *USENIX Security*, 463–481.

[115] Liis Vihul, Christian Czosseck, Katharina Ziolkowski, Lauri Aasmann, Ivo A. Ivanov, and Sebastian Brüggemann. 2012. Legal Implications of Countering Botnets. Tech. rep. NATO Cooperative Cyber Defence Centre of Excellence, the European Network, and Information Security Agency (ENISA), 1–67. Retrieved Sept. 28, 2017 from https://ccdcoe.org/sites/default/files/multimedia/pdf/VihulCzosseckZiolikowskiAasmannIvanovBr%C3%BCggemann2012_LegalImplicationsOfCounteringBotnets_0.pdf, https://perma.cc/6FH6-UGRU.

[116] Wagas. 2016. Hacking, Trading Forum worm.ws Hacked; Exploit Kits, Database Leaked. HackRead. Retrieved Sept. 28, 2017 from https://www.hackread.com/hacking-forum-worm-ws-hacked-data-leaked/, https://perma.cc/V3SU-EUWX.

[117] Maciej Walkowski. 2016. The problem of mounting income inequalities in the world vis-a-vis the phenomenon of harmful tax competition. The ICIJ tracking down the greatest financial scandals of the 21st century. *Przegląd Politologiczny*, 2, 137–154. DOI: 10.14746/pp.2016.21.2.11.

[118] Patrick F. Walsh and Seumas Miller. 2016. Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, 31, 3, 345–368. Routledge. DOI: 10.1080/02684527.2014.998436.

[119] Patrick L. Warren. 2016. Research with leaked data. Society for Institutional & Organizational Economics. (May 2016). Retrieved Apr. 10, 2017 from https://www.sioe.org/news/research-leaked-data, https://archive.fo/F90KP.

[120] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security (CCS)*. ACM, 162–175.

[121] Matt Weir, Sudhir Aggarwal, Breno De Medeiros, and Bill Glodek. 2009. Password cracking using probabilistic context-free grammars. In *30th IEEE Symposium on Security and Privacy*, 391–405.

[122] David Murakami Wood and Steve Wright. 2015. Before and after Snowden. *Surveillance & Society*, 13, 2, 132–138. ISSN: 1477-7487.

[123] Michael Yip, Nigel Shadbolt, and Craig Webber. 2013. Why forums? An empirical analysis into the facilitating factors of carding forums. In *Proceedings of the 5th Annual ACM Web Science Conference*. ACM, 453–462. DOI: 10.1145/2464464.2464524.

[124] Ben Zhao. 2015. Is it legal, ethical and publishable to do academic research using data from the Ashley Madison leak? Quora. (Nov. 2015). Retrieved Apr. 10, 2017 from https://www.quora.com/Is-it-legal-ethical-and-publishable-to-do-academic-research-using-data-from-the-Ashley-Madison-leak.