International Journal of Drug Policy 35 (2016) 84–91

Contents lists available at ScienceDirect

International Journal of Drug Policy

journal homepage: www.elsevier.com/locate/drugpo

Research paper

Ethics in cryptomarket research

James Martin [a,*], Nicolas Christin [b]

[a] Macquarie University, North Ryde, NSW 2109, Australia
[b] Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, United States

ARTICLE INFO

Article history:
Received 11 September 2015
Received in revised form 12 April 2016
Accepted 24 May 2016

Keywords:
Cryptomarkets
Research ethics
Anonymous web
Online drug distribution

ABSTRACT

Background: The recent proliferation of cryptomarkets and the associated emergence of a sub-field of research on the anonymous web have outpaced the development of an ethical consensus regarding research methods and dissemination amongst scholars working in this unique online space. The peculiar characteristics of cryptomarket research, which often involves encryption, illegal activity, large-scale data collection, and geographical separation from research participants, challenge conventional ethical frameworks. A further complicating factor for reaching ethical consensus is the confluence of scholars drawn from a variety of academic disciplines, each with their own particular norms, practices and perspectives.

This paper is intended to stimulate awareness and debate, and to prompt further reflection amongst scholars studying these fascinating online phenomena. The paper explores tensions and addresses some of the more prominent and pressing ethical questions, including public vs. private online spaces, anonymity, data sharing and ownership, risks and threats to research subjects and researchers. Also discussed is how best to balance the potential harms of cryptomarket research against benefits to the public.

Introduction

This article is about the ethical dimensions of cryptomarket research. Cryptomarkets are an "online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities" (Martin, 2014a: 356). This emergent field of study comprises a rapidly growing body of cross-disciplinary research, using a diverse range of research methodologies, including quantitative surveys (Barratt, Ferris, & Winstock, 2014; Barratt, Ferris, & Winstock, this volume), qualitative interviews (Bancroft & Reid, this volume; Barratt, Maddox, Lenton, & Allen, this volume; Maddox, Barratt, Allen, & Lenton, 2016; Van Hout & Bingham, 2013a, 2013b, 2014), observational studies (Martin, 2014a, 2014b; Phelps & Watt, 2014), and digital trace analyses (Aldridge & Décary-Hétu, this volume; Christin, 2013; Dolliver, 2015; Munksgaard, Demant, & Branwen, this volume; Soska & Christin, 2015). The growth of academic interest in cryptomarkets mirrors the expansion of these sites as centres for illicit exchange involving in particular, although not exclusively, the buying and selling of illicit drugs.

As well as peaking interest amongst researchers, the recent expansion of the online drugs trade has attracted attention from law enforcement agencies, news media and the general public. This is unsurprising given the potential for moral panic surrounding topics that are often little understood and subject of misinformation – illicit drugs and the anonymous web, better known by its evocative moniker the 'dark net'. From a purely statistical perspective, the level of popular interest in cryptomarkets is somewhat disproportionate to the scale and impact of the online drugs trade. The most recent study by Soska and Christin (2015) estimates the combined annual global turnover of cryptomarkets to be in excess of USD100 million. This is a remarkable level of growth in a short space of time, but represents only a tiny fraction of an estimated 400 billion dollar global illicit drugs industry (UNODC, 2009). The latter figure is subject to caution, as it is difficult to estimate the scale of the global illicit drugs market, but its order of magnitude nevertheless highlights the vast disparity in size between online and conventional drug markets.

One explanation for the high levels of interest in cryptomarkets is novelty. For decades the global War on Drugs has seemingly been locked in stasis and characterised by internecine conflict between

* Corresponding author. Tel.: +61 298501439.
E-mail address: james.martin@mq.edu.au (J. Martin).

http://dx.doi.org/10.1016/j.drugpo.2016.05.006
0955-3959/

organised crime groups and increasingly militarised public policing agencies. This longstanding stalemate is facing disruption. The emergence of a small but significant and growing online drugs trade has effectively opened up a new and unstable digital front in the global War on Drugs. Yet, unlike the conventional drug war, the social, political and technological contours of this theatre of conflict are not well understood. Understanding the development, scale and characteristics of cryptomarkets, the impact these sites have on the conventional drug economy (including traffickers, dealers and consumers), and the tactics and strategies employed by law enforcement, are fascinating and worthy of further study.

Another explanation for public and academic interest in cryptomarkets is their visibility. In contrast to the secretive and opaque world of conventional drug markets, the online drugs trade takes place largely in the open. Protected by anonymizing technologies, online drug vendors freely advertise their products, including prices, quantities and the regions to which goods may be sent. Consumers regularly post feedback regarding the perceived quality of products and levels of customer service for other prospective customers. Customer feedback also indicates the frequency of drug sales and the popularity of respective drug vendors. Cryptomarket administrators even seek publicity for their sites through interviews with underground news sites (DeepDotWeb, 2014a, 2014b) and conventional media (e.g. Greenberg, 2013).

The unprecedented visibility of cryptomarket-facilitated drug trading is useful in a variety of ways. For news media, it represents a reliable source of titillation and 'click bait' for a crime-fixated public; for law enforcement agencies, a glaring and publicly embarrassing reminder of the limitations of state power (as well as a potentially valuable repository of evidence) and, for researchers, a veritable goldmine of data. Accompanying the scholarly enthusiasm for cryptomarket research is a latent sense of disquiet amongst researchers regarding the ethical appropriateness of studies conducted in this emergent field. This is evidenced by a number of articles concerning cryptomarket research ethics that have either recently been published or are in the process of publication (Barratt & Maddox, in press; Décary-Hétu & Aldridge, 2015; Martin, 2016). These papers explore the emergent field of study from a variety of perspectives, including digital ethnography and 'dark net' interviewing (Barratt & Maddox, in press), ethical and methodological challenges in automated cryptomarket research (Décary-Hétu & Aldridge, 2015), and the dangers and complexities of scholarly collaboration with law enforcement agencies (Martin, 2016).

These articles suggest a growing awareness of the need to grapple with and reflect upon the broader implications of research on cryptomarkets. In addition to the usual professional responsibilities to protect the welfare of research participants, scholars must remain mindful that much of the activity that takes place on these sites is illegal. There are, therefore, additional risks of significant, long-term harm to participants in cryptomarket research, including arrest and imprisonment. While these are risks that are, to some extent, faced by all researchers and participants involved in the study of illegal activity, a variety of factors further complicate their assessment in the context of cryptomarket research. Unlike conventional drug trading, the risks posed to cryptomarket traders by law enforcement are constantly changing due to the emergence of new forms of online investigative strategies that push the limits of technological understanding and innovation. Lack of knowledge regarding the effectiveness of these practices confers an additional degree of uncertainty for researchers and participants alike. Sensitivity to risk (or perceptions of risk) of exposure to law enforcement also heighten dangers specifically for researchers. Risks arise not just from law enforcement agencies, which may be tempted to seize research data as evidence, but also from users of cryptomarkets who may conclude – rightly or wrongly – that research may be used by law enforcement to crack down on the online drugs trade or even identify and prosecute individual users. We emphasize that we are not aware of any scholarly data gathered on cryptomarkets being seized by law enforcement agencies. However, the US Department of Homeland Security recently subpoenaed data from the moderators of the 'darknetmarkets' discussion forum on the 'surface web' site Reddit (Greenberg, 2015) and is an example of new problems related to the gathering and storing of online data.

The aim of the paper is to contribute to emerging discussion about the ethical complexities associated with cryptomarket research by providing an inter-disciplinary perspective on some of the key issues from both computer science and criminology. We have approached this inter-disciplinary discussion from a utilitarian perspective, one which is cognisant of, and seeks to identify the potential for harm to market participants and researchers, but argues that this may be justified where risks are minimal and public benefits are significant.

The paper begins with a general discussion of cryptomarket research ethics, situated within the broader literature of online research ethics across the 'four domains' of Internet research. This is followed by a more detailed analysis of risk assessment and mitigation regarding crawler-based cryptomarket research – a topic initially problematized by two early and influential empirical papers by Christin (2013) and Aldridge and Décary-Hétu (2014). The paper does not provide prescriptive findings, but is intended to assist individual researchers in orienting themselves within the field, and to stimulate debate and greater sense of ethical awareness. We also hope that it encourages others to depart from the traditional comfort of their disciplinary silos and to engage with researchers who hold different perspectives and who share a similar focus on an important, complex and multi-faceted topic.

Characteristics of Internet-based research

There is a large and growing body of studies examining Internet research ethics. The largest international, cross-disciplinary study is provided by the Association of Internet Researchers (Markham & Buchanan, 2012), who problematize many of the issues associated with internet-based research, and identify how long-standing ethical principles such as respect for person, justice and beneficence may be interpreted in a highly varied and unstable digital domain. Despite the existence of significant scholarship in this area, there is a paucity of formal ethical instruction from state regulators regarding internet-based research (Markham & Buchanan, 2012:2). For example, in the United States, Title 45 of the Code of Federal Regulations Part 46 (generally called the "Common Rule"), has no sections on research conducted online. In Australia, recent amendments to the Federal Government's *National Statement on Ethical Conduct in Human Research* (NHMRC 2015), include a brief reference to 'on-line research', however this is restricted to a short definition of internet-based qualitative research.

There are several possible reasons for reluctance on the part of state regulatory authorities to offer detailed guidance in this area. These include the relative novelty of internet-based research, as well as difficulties in determining which countries are responsible for studies conducted in online spaces that are not tied to any clearly defined national jurisdiction. As Eynon, Fry, and Schroeder note (2008:300) "what's different about Internet-based research in contrast to research in the offline world is that the research object is no longer clearly delineated by national boundaries and protected by national research governance".

Problems in determining national jurisdiction for research governance are compounded on cryptomarkets. This is because the precise location of users and the physical location of information hosted on server nodes are deliberately obscured. Some knowledge

may be inferred by analysis of publicly available cryptomarket data and also by details that emerge from criminal investigations. In the case of Silk Road, for example, website membership was geographically diverse, with users located in over a dozen different countries, while law enforcement agencies eventually tracked data servers hosting website content to multiple locations, including the US, Iceland, Latvia and Malaysia (Jeffries, 2014). This diversity is problematic for researchers (as well as law enforcement agencies) who traditionally have been bound by legislation and governance structures that depend upon national sovereignty.

A further related problem that impedes the development of deontological ethical standards for Internet research is the steadily expanding diversity of various forms of digital environments in comparison to more clearly fixed and familiar offline research environments. As Thelwall (2006:1773) notes, "the fact that there are so many different environments (e.g., Web pages, chat rooms, e-mail) and that there are new ones constantly emerging means that explicit [ethical] rules are not possible". This problem is evident in the field of cryptomarket research, where valuable data are stored in a variety of online spaces, including on vendor seller pages, discussion forums, as well as on 'surface web' discussion forums, such as Reddit.

Four domains of Internet research

Researchers who specialize in the study of Internet research ethics recommend the development of localised research practices that are cognizant of broader ethical norms and principles – such as beneficence, utilitarianism and respect for research participants – while also remaining sufficiently flexible to adapt to the various contingencies associated with Internet research (Eynon et al., 2008; Whiteman, 2010, 2012). This approach eschews the development of static ethical codes that may quickly be out-dated in favour of a new way of 'doing ethics', better suited to highly variable and dynamic online research environments. One notable approach is proposed by Whiteman (2012), who advocates developing ethical awareness of the 'four domains of Internet research', specifically, the 'ethics of the academy', the 'ethics of the institution', the 'ethics of the researcher' and the 'ethics of the researched'. The sections below outline the significance of these domains and how they may be used to determine insight into the ethical complexities associated with cryptomarket research.

Ethics of the academy

The 'ethics of the academy' refers to existing discourse regarding ethical issues and practices. These are expressed in literature, including national guidelines, and research reports, as well as more narrowly specified studies exploring Internet research ethics and cryptomarket research. In conventional, 'offline' research, a long-standing distinction exists between studies that are conducted in public and private spaces. Observational research, undertaken in public settings is generally regarded as involving different responsibilities on the part of researchers, particularly in terms of disclosure and obtaining informed consent (Murphy & Dingwall, 2007).

For scholars who conduct research in non-digital environments, the distinction between public and private space is relatively easy to determine. Legal as well as common sense differences between public and private property are well understood. In online spaces, however, this dichotomy often breaks down. While some online spaces are either unambiguously public (e.g. comment pages on news websites) or private (e.g. personal email or messenger services), there are many shades of grey. For example, whether an online discussion forum should be regarded as private is dependent upon a range of factors that can be subjectively interpreted by both researchers and well as participants. It is therefore incumbent upon researchers to examine the particular context of an online space, including users' attitudes, before determining an appropriate ethical position.

The practical application of research ethics is an area in which significant differences manifest between researchers from different scholarly disciplines. For example, computer security does not have as rich a history on how to address ethical questions when conducting studies of human populations, as, for instance, ethnographers. Recent efforts, e.g., by Dittrich, Bailey, and Dietrich (2009), have attempted to frame ethical questions on computer security in the context of the Belmont Report principles: respect for persons, beneficience, and justice.

Often, the decision as to whether to conduct observations may hinge on whether the data are publicly available or not, and whether studying it would actually benefit the community at large. Christin (2013) summarizes this position in his original paper on the Silk Road, arguing that collection was ethical, because:

> The data we collected is essentially public. We did have to create an account on Silk Road to access it; but registration is open to anybody who connects to the site. We did not compromise the site in any way.

Similar views have been espoused by the computer security community. For instance, databases of passwords stolen from various websites have been made public. While this, in itself, is reprehensible and even criminal behaviour, computer security researchers have subsequently taken the view that, regardless of their questionable origin, since these passwords had become public, studying them would not increase harm, and could instead help scientific advances (see, e.g., Ur et al., 2015; Weir, Aggarwal, Collins, & Stern, 2010). The large amount of recent literature on the topic suggests the computer security community have reached a broad consensus that this work is ethical.

Existing scholarship on Internet research ethics can assist researchers in further navigating these complexities. Eysenbach and Till (2001), for example, note a distinction between online forums that have large memberships and those whose communications are visible to only a few select members. Also relevant is whether or not participants are aware that outside observers may be monitoring communications, and the existence of any significant barriers to entry or group membership. In instances where group membership is large, easy to join and widely understood to be monitored, then there is a strong argument that information provided therein is essentially public in nature. By contrast, if an online forum is restricted to a small number of participants and entry to the group is tightly restricted (for example, through vetting or a complex registration process) then researchers would likely have to regard the online space as private.

For the purpose of studies involving cryptomarkets, researchers can usually determine membership with relative ease. Websites typically list the number of users registered to a site. Well-established cryptomarkets, such as AlphaBay and Dream Market, have large numbers of users, amounting to tens or even hundreds of thousands. While this does not necessarily accurately reflect the number of users (e.g. who may have multiple accounts), they remain a useful general indicator of the size of a market's user base. The presence of large numbers of users supports arguments in favour of considering vendor pages and discussion forums as public rather than private spaces, although determining precisely what threshold separates private from public remains essentially subjective. Another factor in favour of considering cryptomarkets as public is that users commonly assume that external parties, in particular law enforcement agencies, monitor communications. This latter argument is consistent with the views discussed earlier

that, from a computer security perspective, the fact that data are publicly available makes it amenable to study.

Ethics of the researcher

According to Whiteman (2012) the 'ethics of the researcher' refers to the "the personal and professional baggage that the researcher draws on when defining their ethical stance" (Whiteman, 2012:38). Relevant details include disciplinary expertise and professional experience, political affiliations as well as personal values and attitudes. The development of personal ethics is an ongoing and reflexive process that introduces an uncertain and highly variable element into scholarly research. Not only are individual experiences and dispositions often subjective, but they are also liable to change. This is not necessarily problematic, so long as researchers maintain a self-critical awareness of the potential for bias, conduct studies in as objective a manner as possible, and do not allow personal beliefs to compromise the integrity of their research, for example, by selectively interpreting data or glossing over complexities that do not fit a particular methodological, ideological or theoretical framework.

Personal ethics such as those outlined above, play an important role in motivating and informing scholarly research. In the case of Martin's cryptomarket research, a disciplinary background in critical criminology was influential in identifying the potenti al for online drug trading to offer a less harmful alternative to conventional forms of illicit drug distribution (Martin, 2014a, 2014b) (a position also articulated by others, including Aldridge & Décary-Hétu, 2014; Barratt, Lenton, & Allen, 2013; Buxton & Bingham, 2015). Whether cryptomarkets are less harmful than drug conventional markets is not just an issue of personal ethics, it is also an important empirical question, one that applies to much other illicit drug and criminological research. Nonetheless, this disciplinary perspective, in combination with personal concerns regarding the tremendous human cost of the War on Drugs, prompted further research into potentially harmful online policing strategies and the sometimes dubious motivations of law enforcement agencies intent on disrupting the online drugs trade (Martin, 2014b).

These initial studies attracted interest from law enforcement and Martin received invitations from police officers seeking information regarding the cryptomarket 'threat'. This raised personal concerns and prompted an ethical analysis of the complexities associated with scholarly collaboration with law enforcement agencies (see Martin, 2016). In this instance, requests were declined in favor of providing a more nuanced perspective regarding the potential harm reduction benefits associated with the growth of the online drugs trade. This negotiated engagement with law enforcement agencies indicates how personal ethics may be used to frame the dissemination of research findings in a way that is constructive and maintains the integrity of research. It is also consistent with a researcher's personal values – in this case, a commitment to avoiding engagement with law enforcement in a way that could assist in disrupting the online drugs trade.

Personal values may also be useful for conducting research. For example, Barratt and Maddox (2016) describe how their shared commitment to harm reduction facilitated ethnographic engagement and helped to establish trust with cryptomarket users. This commitment may be viewed as personal values that have been framed by disciplinary perspective, in this instance from the realms of drug policy and public health research and digital sociology respectively:

> Although we were not insiders to the community, we were not completely outsiders either. M.B., for example, could point to her longstanding voluntary role as administrator at Bluelight.org, a drug harm-reduction clear-web forum that was well regarded on Silk Road, and her research papers, blog posts and mainstream media contributions on the topic of Silk Road. We used this pre-existing digital presence to demonstrate our commitment to values, such as harm reduction, that we deemed likely to be shared by many community members.

This example reveals a symbiosis between the 'ethics of the researcher' and the ethical perspectives of research participants – the 'ethics of the researched'. The level of correspondence between the ethical values of researchers and research participants is perhaps more directly important to those conducting interactive ethnographic studies as opposed to those employing unobtrusive observational methods. This is because interactive ethnography is more likely to necessitate the gaining of informed consent from research participants. However, regardless of one's methodological approach, if observed populations perceive a significant divergence between their own ethics and those of researchers (for example, with regard to the ethical appropriateness of collaborating with law enforcement), then a range of additional obstacles and risks are likely to be encountered (see below for further discussion of potential risks and harms associated with cryptomarket research).

Christin's views, were informed by a disciplinary background in computer science (Christin, 2013). He argues that data collection is acceptable as long as the data are public (and no expectation that data will be kept private), it enables scientific advances, and it does not raise the possibility of harm to any party. In particular, Christin (2013) ensured that the data collected and the analysis conducted could not be used against market operators or participants. This strategy follows the "beneficience" principle outlined in the Belmont report and advocated by Dittrich et al. (2009).

Ethics of the researched

While researchers have cultivated positive relationships with users of cryptomarkets, Barratt and Maddox (in press) and Décary-Hétu and Aldridge (2015) there also instances where researchers have been the subject of personal abuse and threats from those involved with the online drugs trade. Simultaneous expressions of receptivity and hostility on the part of cryptomarket users highlight an important issue regarding the 'ethics of the researched' and the heterogeneity of research populations. Users of cryptomarkets comprise a multiplicity of sub-groups, including administrators, vendors and consumers. Each of these groups has different reasons for inhabiting a cryptomarket (e.g. selling as opposed to buying drugs), varying levels of investment in and dependence upon their ongoing operation (e.g. relying on a cryptomarket as a source of personal income vs. a convenient supplier of recreational drugs). There are also different levels of exposure to risks posed by law enforcement (i.e. administrators and vendors are much higher value targets for law enforcement than consumers, who make up the vast bulk of cryptomarket membership).

Research suggests differences even within these sub-groups. For example, observation of discussion forums reveals heated debates regarding the political dimensions of cryptomarket activity, the implications of online drug dealing, and the prospect of cooperation with researchers (Barratt & Maddox, in press; Martin, 2014). The existence of a divergent range of personal perspectives complicates the work of ethnographic researchers in particular. This is because obtaining the informed consent of one group to participate in research does not necessarily indicate that other users consent. This points to complex issues regarding 'ownership' of online space. While one may conclude that a cryptomarket administrator 'owns' their site and therefore has the authority to either allow research, this perspective is not necessarily understood by other users. Researchers should therefore remain mindful of the differences in personal ethics

amongst various sub-groups and individual users when developing their own ethical stance and methodological approach.

Ethics of the institution

One of the principal obstacles confronting researchers conducting cryptomarket research is satisfying the demands of institutional bodies, in particular, ethics review boards. These gatekeepers of academic research are typically staffed by senior academics who do not necessarily have experience with or understanding of the idiosyncrasies of Internet-based research. However, these bodies are routinely required to approve, amend or disallow studies that are conducted online. A lack of institutionalised knowledge regarding Internet research ethics is problematic; methodologies and applied ethics practices that are based upon conventional, face-to-face research often lack relevance to Internet-based research. This means that online researchers face the challenge of undertaking studies with potentially less informed and less relevant ethical guidance compared with peers working in more established fields.

The limitations of institutional ethical review are potentially serious. Ethics review boards that lack expertise may impose unnecessary or inappropriate restrictions that make research projects unfeasible (a problem that is frequently encountered and much critiqued by scholars engaged in social science research, see for example, Dingwall 2008; Schrag 2011; Van den Hoonaard 2011). A more problematic scenario is that review boards may grant approval to projects that are ethically inappropriate. This risks giving researchers a false sense of confidence in the ethical integrity of their research and potentially exposes researchers and participants to a range of avoidable and unnecessary harms. The possibility of inadequate institutional oversight indicates a need for researchers to develop awareness of ethical issues that extend beyond the minimum required at an institutional level.

The rapid pace of change inherent to cryptomarkets presents a further challenge to researchers engaged in the process of ethical review. The pace of institutional deliberation and decision-making is typically slow. This may be frustrating but is otherwise unproblematic for scholars who are undertaking research in relatively stable research environments. Cryptomarkets, by contrast, are highly unstable, with the lifespan of sites typically measured in months rather than years (at the time of publication, the longest running cryptomarket – *Dream Market* – has been operational for just over two years). There is therefore a significant possibility that by the time a researcher has identified a suitable site, formulated research questions, developed an appropriate methodology, and secured ethical approval, that the site listed in their application will no longer be operational.

Researchers can take steps to compensate for this by providing a detailed ethical rationale for their research that pre-empts as much as possible potential objections on the part of ethics review boards and avoids time-consuming revisions and resubmissions. It is also advisable that researchers build in appropriate methodological flexibility to compensate for the contingencies of the research environment. This may include gathering data from multiple cryptomarkets so that research may continue in the event that a site is closed down unexpectedly.

Assessing and mitigating risks

Research in cryptomarkets frequently involves large-scale data collection. This is particularly the case for research involving digital trace analyses. When conducting research of this nature, it is desirable for scholars to share data with others for the purposes of reproducibility and to enable meaningful comparisons. Most of the ethical discussion here is directly related to the notion of risk. Specifically, we need to determine the extent to which the research activities increase risks to certain actors (researchers, marketplace operators, customers, . . .). The ethical question is then whether any increase in risk is tolerable; and if this is affirmative, for instance based on utilitarian ethics, up to which level is that risk acceptable?

Collecting cryptomarket data

Cryptomarkets are attractive to researchers as they provide a digital footprint of transactions that can be collected with limited risk. This is in contrast to traditional, physical world criminal activity, for which quantitative measurements are often hard, and potentially dangerous, to collect. Obtaining information about, for instance, street drug prices (Heimer, 2000; Maher & Daly, 1996) or stolen goods (Cromwell, Olson, & Avary, 1993; Schneider, 2005; Stevenson, Forsythe, & Weatherburn, 2001) requires developing quantitative and qualitative assessments of data from the perspective of offenders. Such studies frequently require researchers to directly interact with offenders which can put researchers at risk of harm.

In comparison, transactions in cryptomarkets can usually be measured without direct interaction, and, using elementary precautions, generally unbeknown to sellers, buyers or marketplace operators (Christin, 2013; Soska & Christin, 2015). Even if a researcher is detected collecting data from a cryptomarket, the relatively strong anonymity guaranteed in these marketplaces protect researchers. In particular, punitive measures are limited to severing the researcher's access to the marketplace, e.g., by terminating accounts and/or providing them with incorrect data to impede researcher analysis.

Risks to researchers potentially increase after publication. At that point, researchers are identified and consequently retribution might occur. (A notable exception, related to government censorship, is the anonymous work credited to Aryan, Aryan, and Halderman (2013).) However, among all the authors who have contributed to the fledgling body of literature on cryptomarket analysis, we are only aware of one incident in which an academic was mentioned by name in chats between the Silk Road operator and one of its associates.[1] Overall, though, it appears that the risks associated with data collection are far smaller than those encountered in the 'offline' world.

Researchers have the ability to disclose their activities ahead of time. For instance, while "scraping" a cryptomarket for content with an automated tool, the tool can inform marketplace operators of its presence and purpose – e.g., by sending contact information with any request made to the marketplace. This approach is not favored by researchers from science and engineering, who argue that, akin to the Heisenberg principle, for measurements to be reliable they should not impact the measured environment (Christin, 2013; Soska & Christin, 2015). However, others, such as Munksgaard (2016) have notified marketplace operators of their intention of conducting measurements, in an effort to build trust with operators and be in a better position to conduct ethnographic studies.

Data collection – prior to analysis and publication – should pose no additional risk to marketplace operators, vendors or buyers, since it is a matter of copying existing, publicly disclosed data. However, analyzing these data could be problematic for marketplace participants. For instance, researchers have been able to infer with reasonably good precision sales volumes of individual vendors, which in turn could conceivably justify criminal proceedings against them. Does this mean that researchers should avoid conducting any analysis that could justify enforcement intervention or make the job of prosecuting agencies easier?

This is a complex question. It is arguable that because digital trace data gathered from cryptomarkets are public, anybody could

[1] See evidence GX243 in Ross Ulbricht's trial. Available at: http://antilop.cc/sr/exhibits/DX_C_le_counterintel_file.pdf (accessed 28.08.15).

perform similar analyses. This includes law enforcement agencies that may appear to lack expertise in advanced computational research. In fact, advanced research on the part of law enforcement has been done in the past: during Ross Ulbricht's prosecution and subsequent trial, the prosecution commissioned an expert witness to compute the total amount of transactions conducted on the Silk Road site (Flitter, 2015). Given that law enforcement agencies have demonstrated willingness to conduct this kind of research independent of the academy, data analysis conducted by independent researchers should not increase existing levels of risk of harm to marketplace participants.

Considered from a more general perspective, it is conceivable that in conducting any kind of analysis of cryptomarket activity, researchers run the risk of highlighting previously unknown criminal trends both to the public and to law enforcement. While not directly resulting in prosecution, publication of cryptomarket research may result in increased public awareness and policing activity targeting online criminal activity, and subsequently increase the likelihood of prosecution. While this outcome is possible, we argue that an absence of informed, independent and critical scholarly perspectives regarding cryptomarkets may also be damaging to marketplace participants. For example, exaggerated claims on the part of the FBI regarding the supposed turnover of illicit drugs sold via Silk Road were highly misleading and exaggerated the impact of the site. Analysis and commentary by Christin and others exposed these claims as disingenuous, and helped ensure that subsequent public debate was tempered by more accurate, critical analysis.

Terms of service

Numerous online businesses – search engines like Google, classified forums like Craigslist – prohibit customers from scraping data. Doing so is in breach of the Terms of Service these companies offer, and would typically result in account termination, and possible legal recourse. Related concerns include the notion of data ownership: by processing and displaying results in a certain manner, these businesses actually produce curated data, to which they may be able to assert copyrights. In fact, in the United States, as has been shown in the Lori Drew[2] and Aaron Swartz[3] cases, prosecutors have argued that violations of Terms of Service amount to unauthorized access in violation of the Computer Frauds and Abuse Act. As a result, usually, research relying on breaches of contract of this kind is frowned upon, and numerous academic institutions prohibit it.

As a corollary, an interesting question would be what the researchers should do if a cryptomarket set up some Terms of Service explicitly forbidding scraping of the contents. So far, we have not observed this in any explicit way. However, some marketplaces have been known to deploy anti-scraping technological measures (Soska & Christin, 2015), which can be construed as an implicit expression of Terms of Service. Should researchers comply with marketplace operator wishes – expressed or implied – not to allow third-party scraping of the data? From a legal standpoint, this is a murky proposition at best: most marketplaces primarily support commerce deemed illicit in most jurisdictions, and any contract entered with them would likely be unenforceable, or even invalid. An interesting nuance, here, is that a contract is only unenforceable as "against public policy" if the subject of the contract itself is illegal. This means that, if only certain transactions in the marketplace are illegal (but the marketplace itself is not, e.g., it is not a conspiracy to distribute drugs), then the Terms of Service might be enforceable since they might pertain to legal goods.

From an ethical standpoint, we can make the argument that data collection for research purposes – as opposed to, say, setting up a mirror website in hopes of capturing user login credentials fraudulently – does not cause any harm to the marketplace or its users. Considering the potential societal benefits in better understanding how these marketplaces operate and evolve, it seems the benefits greatly outweigh potential costs. As such, a utilitarian ethics view would suggest that breaching such (legally unenforceable) Terms of Service, be they stated or implied, is not unethical; and that researchers using multiple accounts or other measures to circumvent anti-scraping measures would not be acting unethically.

Sharing cryptomarket data

While we argue that the ethics of data collection are relatively clear-cut, sharing these data brings considerably thornier ethical questions.

Reproducibility

In computer science and other disciplines considered part of the 'hard sciences', an important principle is that research must be reproducible. For instance, clinical trials of new medication should be repeated several times and reach the same outcomes before the medication is deemed effective (Prinz, Schlange, & Asadullah, 2011). More generally, reproducibility means that researchers should be able to independently come to the same conclusions as those reached in prior studies. The reproducibility principle is particularly important in online crime, because deriving wrong numbers can potentially negatively impact public policy postures (Andreas & Greenhill, 2011; Graves, Acquisti, & Christin, 2016). For instance, over-estimating transaction volumes in a black market may result – if these numbers are heeded by people with decision power – in inefficient allocation of limited resources (e.g., taxpayer money); likewise, incorrectly assessing the relative size of various criminal activities may divert resources from where they would be most needed. In other words, reproducibility is important because it allows for independent verification of numbers.

In the area of cryptomarkets, data collection is fraught with difficulties which can lead to considerable error as Soska and Christin (2015) discuss. There is at least one concrete example of research that appears to have derived incorrect conclusions due to erroneous data collection. Dolliver (2015) argues that business in the Silk Road 2 marketplace was very limited. Independent research (Aldridge & Décary-Hétu, 2015; Munksgaard, Demant, & Branwen, this volume; Van Buskirk, Roxburgh, Naicker, & Burns, 2015) not only failed to replicate these findings, but also came to completely different conclusions. Unfortunately, Dolliver (2015)'s dataset is not publicly available, which means that no one can assess precisely what has gone wrong in the data collection. (All signs point to incomplete data being used as the basis for analysis.)

Resource usage

Besides reproducibility, another argument strongly in favor of sharing and reusing data pertains to responsible resource usage. Most cryptomarkets rely on the Tor (Dingledine, Mathewson, & Syverson, 2004) or i2p (I2P) anonymous networks. Illicit activity is only one of the many uses of these networks, most of which are beneficial – for instance, anonymous networks are extensively used by law enforcement and researchers to investigate certain activities without revealing their identities to possible hostile parties (see, e.g., (Leontiadis, Moore, & Christin, 2011; Leontiadis, Moore, & Christin, 2013; Leontiadis, Moore, & Christin, 2014)

[2] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[3] Superseding Indictment, US v. Swartz, 1:11-cr-10260, No. 53 (D. Mass. September 12, 2012).

which extensively make use of Tor to capture data from unlicensed pharmacies), or they have also been known to assist in circumventing censorship in certain countries (Dingledine, 2011).

At a very high level, anonymous networks rely on peer-to-peer "overlays". That is, they are supported by machines (typically, personal computers) run by volunteers. As a result of the rising popularity of anonymous networks, especially in the light of Edward Snowden's revelations, many users are competing for these resources. At the same time, scraping entire cryptomarkets can itself be resource-intensive. Soska and Christin (2015) report that some marketplaces contain in excess of 300,000 web pages, and, for those, a complete scrape may take up to five days over the Tor network, consuming significant resources in the process. Christin (2013), and Soska and Christin (2015) compensate for this by contributing fast, powerful machines to the Tor network, but more generally, it appears desirable to reduce the strain on the network due to data collection. This is one of the arguments Branwen (2015) uses in justifying his sharing large marketplace scrapes collected over relatively long time intervals. In addition, sharing a common set of website scrapes allows for a common dataset to be used for reproducing analyses and comparing the soundness of various approaches.

Arguments against sharing scrapes

There are some serious concerns associated with the sharing of website scrapes. At a technical level, as discussed by Branwen (2015) himself, soundness of the scrapes is not guaranteed since no processing or analysis took place beyond data collection; Soska and Christin (2015) echo these concerns by describing some of the many ways scraping might fail without the researchers in charge of data collection noticing anything is amiss. Thus, using a common set of scrapes may be fraught with uncertainty if the scrapes themselves are defective and could lead to biased analysis.

At an ethical level, sharing scrapes also poses certain quandaries. From a computer science perspective, any measurement research should strive to minimize the disruption to the environment being studied. Blind data dumps may violate this objective. Assume that Susie Dealer mistakenly publishes her phone number on a cryptomarket listing, and then takes it out five minutes later. If a researcher just happened to scrape the page at that time, and put it online, there is a non-zero probability the researcher is actually going to be responsible for harm to Susie Dealer. In an extreme case, the phone number might be used to de-anonymize Ms. Dealer, and put her at risk of being targeted by law enforcement. One could argue that this risk is minimal because (1) the probability of such data leaks is small, and (2) the probability that any adverse action results from a data leak is also small. Indeed, we are not aware of any such incidents. However, equating harm to the extreme case of adverse consequences (imprisonment) is in our opinion a very narrow interpretation of the concept of harm. Indeed, the mere act of making Ms. Dealer's personal information public may cause her considerable stress and can be construed as a form of cyber-harassment (Citron, 2014).

Moving forward

So, what should we do? One can argue that entire scrapes are not needed for research reproducibility, and that a thorough discussion of the methodology used in the data collection and analysis should be enough to allow others to run similar measurements independently and validate them. In fact, the discussion around the failure of others to reproduce the results obtained by Dolliver (2015) (and the fact others obtained widely diverging results while using similar collection approaches) would substantiate this argument. On the other hand, a simple methodological description may leave too many degrees of freedom in the way data are collected and analyzed; it also does not alleviate the concerns linked to excessive resource usage.

Christin sketched a possible solution in the release of the datasets linked to his 2013 paper. He set up a companion website (https://arima.cylab.cmu.edu/sr) containing data that can be used to reproduce the figures presented in the paper. Rather than sharing scrapes, he took the option to share processed data from the scrapes. To avoid identity leaks, he also obfuscated all textual information, and to prevent direct correlation between vendors in the database and vendors on the Silk Road website, he obfuscated the vendor IDs in the database. In addition, he delayed release of the data. Delaying arguably reduces the risk of interference with the environment: vendors may have rotated identities; products may not be available anymore, etc. However, on the other hand, Branwen (2015) argues that such a limited release does not allow for full reproducibility and as a result, is not particularly useful. We suggest that a potential compromise is to use a tiered system, in which partially obfuscated data would be publicly released after a delay. Full, obfuscated data may be made available to other researchers (but not the general public) after individual vetting. This is the approach Christin (2013) uses, and that Soska and Christin (2015) appear to be pursuing as well.

Conclusion

This is an exciting time for scholars engaged in the study of cryptomarkets. The sudden and unexpected opening up of this new field of inquiry presents promising opportunities for innovative and impactful research. At the same time, there remain significant uncertainties regarding the ethical dimensions of cryptomarket research. Given the novelty of cryptomarkets – and indeed, of Internet-based research more generally – there is limited institutional expertise available to assist scholars in navigating these complexities. This places an additional responsibility upon cryptomarket researchers to develop their own sense of ethical awareness regarding the idiosyncrasies of the research environment and to innovate appropriate applied ethics practices. These are achievable goals. As this paper has sought to demonstrate, ethical problems can be addressed by drawing on existing scholarship and ethical principles founded in more established fields of research, and through collaborative engagement with others involved in the study of cryptomarkets. Whiteman's (2012) four domains of internet research offer a useful conceptual starting point whereby researchers can identify and begin to manage the ethical complexities inherent to this dynamic and rapidly expanding field. We hope that more researchers will join the conversation and contribute to the development of a scholarly consensus regarding ethically appropriate ways in which to conduct research into these fascinating online phenomena.

Acknowledgements

The authors would like to thank the anonymous reviewers for their insightful comments and suggestions in critiquing this paper, and Jim Graves for his insights on the legal aspects of contract enforcement. This work was partially supported by the National Science Foundation (CCF-0424422) and the Department of Homeland Security Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD), the Government of Australia and SPAWAR Systems Center Pacific (through BAA-11.02, contract number N66001-13-C-0131). This paper represents the position of the authors and not that of the aforementioned agencies.

Conflicts of interest: There are no conflicts of interest for either of the authors of this paper.

References

Aldridge, J., & Décary-Hétu, D. (2014). *Not an "Ebay for Drugs": The cryptomarket "Silk Road" as a paradigm shifting criminal innovation (SSRN scholarly paper no. ID 2436643)*. Rochester, NY: Social Science Research Network.

Aldridge, J., & Décary-Hétu, D. (2015). A response to Dolliver's "Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel". *International Journal of Drug Policy, 26*(11), 1124–1125.

Andreas, P., & Greenhill, K. M. (2011). *Sex, drugs and body counts: The politics of numbers in global crime and conflict*. Ithaca, New York, USA: Cornell University Press.

Aryan, S., Aryan, H., & Halderman, J. A. (2013). *Internet censorship in Iran: A first look*. Washington, DC, USA: Free and Open Communications on the Internet.

Bancroft, A., & Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy, 35*, 42–49.

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research* 1468794116648766.

Barratt, M. J., Lenton, S., & Allen, M. (2013). Internet content regulation, public drug websites and the growth in hidden Internet services. *Drugs: Education, Prevention and Policy, 20*(3), 195–202.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction, 109*(5), 774–783.

Barratt, M. J., Maddox, A., Lenton, S., & Allen, M. (2016). What if you live on top of a bakery and you like cakes? – Exploring the drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy, 35*, 50–57.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24–31.

Branwen, G. (2015). *Dark Net Market archives, 2011–2015*. Retrieved from http://www.gwern.net/Black-market archives

Buxton, J., & Bingham, T. (2015). *The rise and challenge of dark net drug markets. Policy Brief 7*. Global Drug Policy Observatory, Swansea University.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd World Wide Web Conference (WWW'13)* (pp. 213–224).

Citron, D. K. (2014). *Hate crimes in cyberspace*. Cambridge, Massachusetts, USA: Harvard University Press.

Cromwell, P. F., Olson, J. N., & Avary, D. A. W. (1993). Who buys stolen property? A new look at criminal receiving. *Journal of Crime and Justice, 16*(1), 75–95.

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime, 2*(2), 122–141.

DeepDotWeb (2014a). Interview with 'Cannabis Road' lead developer. *DeepDotWeb* Retrieved from https://www.deepdotweb.com/2014/05/13/interview-with-cannabis-road-lead-developer (accessed 10.04.16).

DeepDotWeb (2014b). Interview with outlaw market admin. *DeepDotWeb* Retrieved from https://www.deepdotweb.com/2014/01/23/interview-with-outlaw-market-admin/ (accessed 10.04.16).

Dingledine, R. (2011). *Tor and circumvention: Lessons learned. Advances in Cryptology – CRYPTO 2011*. Springer.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium*.

Dingwall, R. (2008). The ethical case against ethical regulation in humanities and social science research. *Twenty-First Century Society, 3*(1), 1–12.

Dittrich, D., Bailey, M., & Dietrich, S. (2009). *Towards community standards for ethical behavior in computer security research. Technical Report 2009-01*. Hoboken, NJ, USA: Stevens Institute of Technology.

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy, 26*(11), 1113–1123.

Eynon, R., Fry, J., & Schroeder, R. (2008). The ethics of internet research. In L. Fielding (Ed.), *SAGE handbook of Internet research methods*. London: SAGE Publications.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *BMJ, 323*(7321), 1103–1105.

Flitter, E. (2015). *CORRECTED – U.S sharply reduces Silk Road's estimated sales volume*. http://www.reuters.com/article/usa-bitcoin-trial-silkroad-idUSL1N0UT1PJ20150120

Graves, J. T., Acquisti, A., & Christin, N. (2016). Big Data and bad Data: On the Sensitivity of Security Policy to Imperfect Information. *The University of Chicago Law Review*, 117–137.

Greenberg, A. (2013). *An interview with a digital drug lord: The Silk Road's dread pirate roberts (Q&A)*. Forbes Magazine.

Greenberg, A. (2015). Feds demand reddit identify users of a dark-net drug forum. *Wired*. http://www.wired.com/2015/03/dhs-reddit-dark-web-drug-forum/ (accessed 10.09.15).

Heimer, K. (2000). Changes in the gender gap in crime and women's economic marginalization. *Criminal Justice, 1*, 427–483.

Jeffries, A. (2014). *Lessons from Silk Road: Don't host your virtual illegal drug bazaar in Iceland, The Verge website*. http://www.theverge.com/2013/10/14/4836994/dont-host-your-virtual-illegal-drug-bazaar-in-iceland-silk-road (accessed 01.09.15).

Leontiadis, N., Moore, T., & Christin, N. (2011). Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. *Proceedings of USENIX Security 2011*.

Leontiadis, N., Moore, T., & Christin, N. (2013). Pick your poison: Pricing and inventories at unlicensed online pharmacies. *Proceedings of the 14th ACM Conference on Electronic Commerce (EC'13)* (pp. 621–638).

Leontiadis, N., Moore, T., & Christin, N. (2014). A nearly four-year longitudinal study of search-engine poisoning. *Proceedings of ACM CCS 2014* (pp. 930–941).

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde'. *Information Communication & Society, 19*(1), 111–126.

Maher, L., & Daly, K. (1996). Women in the street-level drug economy: Continuity or change. *Criminology, 34*, 465–491.

Markham, A., & Buchanan, E. (2012). *Ethical decision-making and internet research recommendations from the AoIR Ethics Working Committee (version 2.0)*.

Martin, J. (2014a). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. UK: Palgrave Macmillan.

Martin, J. (2014b). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice, 14*(3), 351–367.

Martin, J. (2016). Illuminating the dark net: methods and ethics in cryptomarket research. In M. Adorjan & R. Riciarrdelli (Eds.), *Engaging with Ethics in International Criminological Research*, Routledge, pp 192–211. UK: Routledge.

Munksgaard, R. (2016). *Intersections of crime and politics – A macroanalysis of cryptomarket discourse* [Master's thesis] University of Copenhagen Retrieved from https://diskurs.kb.dk

Munksgaard, R., Demant, J. J., & Branwen, G. (2016). A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network". *International Journal of Drug Policy, 35*, 92–96.

Murphy, E., & Dingwall, R. (2007). Informed consent, anticipatory regulation and ethnographic practice. *Social Science & Medicine, 65*(11), 2223–2234.

Phelps, A., & Watt, A. (2014). I shop online – Recreationally! Internet anonymity and Silk Road enabling drug use in Australia *Digital Investigation, 11*(4), 261–272.

Prinz, F., Schlange, T., & Asadullah, K. (2011). Believe it or not: How much can we rely on published data on potential drug targets? *Nature Reviews Drug Discovery, 10*(9), 712.

Schneider, J. L. (2005). Stolen-goods markets: Methods of disposal. *British Journal of Criminology, 45*, 129–140.

Schrag, Z. M. (2011). The case against ethics review in the social sciences. *Research Ethics, 7*(4), 120–131.

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14)* (pp. 33–48).

Stevenson, R. J., Forsythe, L. M. V., & Weatherburn, D. (2001). The stolen goods market in New South Wales Australia: An analysis of disposal avenues and tactics. *British Journal of Criminology, 41*, 101–118.

Thelwall, M., & Stuart, D. (2006). Web crawling ethics revisited: Cost, privacy, and denial of service. *Journal of the American Society for Information Science and Technology, 57*(13), 1771–1779.

UNODC (2009). *World drug report 2009*. Vienna: United Nations Office on Drugs and Crime.

Ur, B., Segreti, S. M., Bauer, L., Christin, N., Cranor, L. F., Komanduri, S., et al. (2015). Measuring real-world accuracies and biases in modeling password guessability. *24th USENIX Security Symposium (USENIX Security 15)* (pp. 463–481).

Van Buskirk, J., Roxburgh, A., Naicker, S., & Burns, L. (2015). A response to Dolliver's "Evaluating drug trafficking on the Tor network". *International Journal of Drug Policy, 26*(11), 1126–1127.

Van den Hoonaard, W. C. (2011). *The Seduction of Ethics: Transforming the Social Sciences*. Toronto: University of Toronto Press.

Van Hout, M. C., & Bingham, T. (2013a). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385–391.

Van Hout, M. C., & Bingham, T. (2013b). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*(6), 524–529.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183–189.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 162–175). ACM.

Whiteman, N. (2010). Control and contingency: Maintaining ethical stances in research. *International Journal of Internet Research Ethics, 3*(1), 6–22.

Whiteman, N. (2012). *Undoing ethics*. US: Springer.