Ethics in Cryptomarket Research[1]

James Martin
Macquarie University
North Ryde, NSW 2109
Australia
james.martin@mq.edu.au

Nicolas Christin
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
United States
nicolasc@cmu.edu

Abstract

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 involve encryption, illegal activity, large-scale data collection, and geographical separation from research participants, challenge conventional ethical frameworks developed over many decades in more familiar and transparent offline environments. Further complicating the emergence of ethical consensus regarding research methods is the confluence of scholars drawn from a variety of academic disciplines and specializations each with their own particular norms, practices and perspectives.

This paper explores these tensions and addresses some of the more prominent and pressing ethical questions currently facing researchers investigating cryptomarkets. Debates on a range of ethics related topics are analyzed and situated with broader discussions regarding Internet-based research. Issues addressed include 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. Rather than issuing prescriptive findings, this paper is intended to stimulate awareness and debate, and to help prompt further ethical considerations and reflection amongst scholars studying these fascinating online phenomena.

Keywords

cryptomarkets, research ethics, anonymous web, online drug distribution

---

[1] This is an author preprint, made available for timely dissemination of the material. The final version is to be published by The International Journal of Drug Policy.
DOI: http://dx.doi.org/10.1016/j.drugpo.2016.05.006

This research was partially supported by 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 via contract number N66001-13-C-0131. This paper represents the position of the authors and not that of the aforementioned agencies.

Introduction

This article is about the ethical dimensions of cryptomarket research. Cryptomarkets are a type of "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 quickly growing body of cross-disciplinary research utilising a diverse range of research methodologies, including quantitative surveys (Barratt, Ferris and Winstock, 2014; Barratt, Ferris and Winstock, this volume), qualitative interviews (Van Hout and Bingham 2013a, 2013b, 2014; Maddox, Barratt, Allen and Lenton, 2016; Barratt, Maddox, Lenton and Allen, this volume; Bancroft and Reid, this volume), observational studies (Martin 2014a, 2014b, Phelps and Watt 2014), as well as digital trace analyses (Christin 2013; Aldridge and Décary-Hétu 2014, this volume; Dolliver 2015; Soska and Christin 2015; Munksgaard, Demant and Branwen, this volume). The growth in academic interest in cryptomarkets mirrors the expansion of these sites as centres for illicit exchange involving particularly, though 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 also attracted widespread attention amongst law enforcement agencies, news media and the general public. This is not surprising given the potential for moral panic surrounding two topics that are often little understood and also the subject of much misinformation – illicit drugs and the anonymous web, perhaps better known by its evocative moniker the 'dark net'. From a purely statistical perspective, the level of popular interest in cryptomarkets is perhaps 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 is 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). This latter figure is subject to caution, as it is very difficult to accurately 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.

At least one explanation for the currently 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 organised crime groups and increasingly militarised public policing agencies. This longstanding stalemate is now 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, characteristics of cryptomarkets, the impact these sites have upon the conventional drug economy

(including traffickers, dealers and consumers), as well as the tactics and strategies employed by law enforcement, are therefore fascinating and worthy topics for scholarly inquiry.

Another explanation for high levels of public and academic interest in cryptomarkets is their public visibility. In contrast to the secretive and opaque world of conventional drug markets, the online drugs trade takes place largely out in the open. Protected by anonymizing technologies, online drug vendors freely advertise information about their products, including prices, quantities and the regions to which goods may be sent. Consumers of illicit drugs that are purchased online regularly post feedback regarding the perceived quality of products and levels of customer service for other prospective customers. Customer feedback also provides an indication regarding the frequency of drug sales and the popularity of respective drug vendors. Cryptomarket administrators even seek publicity for their respective 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 that may be gathered, sifted through and studied. 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 are either recently published or in the process of publication (Décary-Hétu and Aldridge 2015, Barratt and Maddox In press, Martin In press). These papers explore this emergent field of study from a variety of perspectives, including digital ethnography and 'dark net' interviewing (Barratt and Maddox In press), ethical and methodological challenges in automated cryptomarket research (Décary-Hétu and Aldridge 2015), and the dangers and complexities of scholarly collaboration with law enforcement agencies seeking to crack down on the online illicit drugs trade (Martin In press).

The emergence of these studies is an encouraging trend that suggests a growing awareness on the part of researchers involved in the study of cryptomarkets of the necessity to grapple with and reflect upon the broader implications of their work. These are important issues. In addition to the usual professional responsibilities that researchers carry in order to protect the welfare of research participants, scholars engaged in the study of cryptomarkets must also 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 involved 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 accurate 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 heightens 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 in general or even identify and prosecute individual users. We emphasize that we are not presently 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). This information could be used by state authorities to reveal the identities of contributors to this discussion forum, and is an example of new problems related to the gathering and storing of online data.

The aim of this paper is to contribute to the emerging discussion regarding the ethical complexities associated with cryptomarket research. It differs from existing studies in this area by providing an inter-disciplinary perspective regarding some of the central issues surrounding this topic from both computer science and criminology. We have approached this inter-disciplinary discussion of cryptomarket research ethics 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 in circumstances where risks are minimal and public benefits are significant.

The paper begins with a general discussion of cryptomarket research ethics which is 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 rather 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 areas of expertise and who share a similar focus on an important, complex and multi-faceted topic of mutual interest.

Characteristics of Internet-based research

There is a large and growing body of studies examining Internet research ethics. The largest international, cross-disciplinary study in this context is provided by the Association of Internet Researchers (Markham and 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 and 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 that refer specifically to research that is 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 the apparent 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 exactly which countries are responsible for studies conducted in online spaces that are not tied to any clearly defined national jurisdiction. As Eynon et al 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 in research regarding cryptomarkets. This is because the precise location of users as well as the physical location of information hosted on server nodes are deliberately obscured. Some degree of 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 Thewall (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". Again, this problem is evident in the field of cryptomarket research, where valuable data are stored in a variety of different 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

In response to these issues, 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' that is better suited to highly variable and dynamic online research environments. One notable approach in this vein is proposed by Whiteman (2012), who advocates researchers 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 each of these domains and how they may be used to determine insights into the ethical complexities associated with cryptomarket research.

Ethics of the Academy

The 'ethics of the academy' refers to existing scholarly discourse regarding ethical issues and practices. These are expressed in a diverse range of 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 that is undertaken in public settings is generally regarded to involve different responsibilities on the part of researchers, particularly in terms of disclosure and the necessity to obtain informed consent (Murphy and Dingwall 2007).

For scholars who conduct research in non-digital environments, the distinction between public and private spaces is relatively easy to determine. Legal as well as common sense differences between public and private property are well understood by both researchers and members of the broader public. In online spaces, however, the clear dichotomy between public and private 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 in between. 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 closely examine the particular context of an online space, including the attitudes of the users of the space, before determining an appropriate ethical position.

The practical application of research ethics is one area in which significant differences manifest between researchers from different scholarly disciplines. For example, computer security does not have as rich a history and community standards on how to address ethical questions when conducting studies of human populations, as, for instance, ethnographers. Recent efforts, e.g., by

Dittrich et al. (2009), have attempted to frame ethical questions in computer security in the context of the Belmont Report principles: respect for persons, beneficience, and justice.

Often, the decision of whether to conduct observations may simply 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 Silk Road measurement paper, 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 in other studies. For instance, databases of passwords stolen from various website have been leaked and made public. While this, in itself, is certainly 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 would instead help scientific advances (see, e.g., Weir et al. (2010), Ur et al. (2015)). The large amount of recent literature on the topic suggests the computer security community reached a relatively broad consensus this type of work is ethical.

Existing scholarship focused specifically 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 by external parties, then a strong argument can be made 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 a vetting or 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 the membership of groups 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 given 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 essentially public is that users commonly assume that external parties, in particular law enforcement agencies, monitor their 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, professional experience and 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 also liable to change over time. This is not necessarily problematic, however, 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 potential 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 other researchers, including (Barratt, Lenton et al. 2013, Aldridge and Décary-Hétu 2014, Buxton and Bingham 2015). Whether cryptomarkets do indeed offer a less harmful alternative to conventional drug markets is not just an issue of personal ethics. It is also an important empirical question, one that also similarly 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).

Interestingly, these initial studies attracted interest from law enforcement agencies and Martin received invitations from police officers seeking information regarding the cryptomarket 'threat'. This raised a number of personal concerns and prompted an ethical analysis of the complexities associated with scholarly collaboration with law enforcement agencies (see Martin In press). In this instance, requests for assistance on the part of law enforcement agencies 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

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 either directly or indirectly assist in disrupting the online drugs trade.

Personal values may also be useful in the process of conducting research. For example, Barratt and Maddox (in press) describe how their shared commitment to harm reduction facilitated ethnographic engagement with cryptomarket users. This commitment to harm reduction may be viewed as an expression of 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. For Barratt and Maddox (in press), overt demonstrations of personal ethical values assisted in establishing trust amongst research participants:

> *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 an intriguing 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 the final sections of the paper for further discussion of potential risks and harms associated with cryptomarket research).

Christin's views, which are informed by a disciplinary background in computer science, were primarily summarized in his original paper (Christin, 2013), in which he argues that data collection is acceptable as long as the data are public (and there is thus 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 subsequently 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 some researchers have successfully cultivated positive relationships with users of cryptomarkets, Barratt and Maddox (in press) and Décary-Hétu and Aldridge (2015) also cite several instances where researchers have been the subject of personal abuse as well as 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' – the heterogeneity of research populations. Users of cryptomarkets are not a monolithic group, but rather one that comprises a multiplicity of sub-groups, including administrators, vendors and consumers. Each of these sub-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 an important 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 conducted on cryptomarkets suggests a range of differences even within these sub-groups. For example, observation of cryptomarket 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 (Martin 2014, Barratt and Maddox, in press). The existence of a divergent range of personal opinions and 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 also consent. This points to complex issues regarding 'ownership' of online spaces. While one may logically conclude that a cryptomarket administrator 'owns' their site and therefore has the authority to either allow or disallow research, this perspective is not necessarily understood or shared 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 to conducting cryptomarket research.

Ethics of the institution

One of the principal obstacles confronting researchers conducting cryptomarket research is satisfying the demands of institutional bodies, in particular those of ethics review boards. These important gatekeepers of academic research are typically staffed by senior academics who do not necessarily have any significant 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 scholarly inquiry. This means that online researchers face the challenge of undertaking studies with potentially less informed and less relevant ethical guidance when compared with peers working in more established fields of inquiry.

The limitations of institutional ethical review are potentially serious. Ethics review boards that lack adequate expertise may impose unnecessary or inappropriate restrictions that make valuable 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). An even more problematic scenario is that review boards may grant approval to research projects that are ethically inappropriate. This scenario risks giving researchers a false sense of confidence in the ethical integrity of their research and potentially exposes both researchers and participants to a range of avoidable and unnecessary harms. The possibility for inadequate institutional oversight indicates a need for researchers involved in the study of cryptomarkets to develop their own awareness of ethical issues that extends beyond the minimum required at an institutional level.

The rapid pace of change inherent to cryptomarkets presents a further significant 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 and tested an appropriate methodology, and secured approval from an ethics review board, that the site listed in their ethics application will no longer be operational.

Researchers can take steps to compensate for the mismatch between the instability of the research environment and slow moving pace of institutional ethical review. 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, researchers may expedite the review process and avoid 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 collected data with others for a variety of purposes, ranging from research reproducibility to the ability of providing provide meaningful comparisons. In this section, we discuss some of the ethical quandaries posed both by the collection, and the subsequent sharing of data gathered via digital trace analysis. Most of the ethical discussion here is directly related to the notion of risk. Specifically, we need to determine to which extent 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 we answer affirmatively, for instance based on utilitarian ethics, up to which level is that risk increase acceptable?

Collecting Cryptomarket Data

Cryptomarkets are particularly attractive to researchers, since they provide a digital footprint of transactions that can be collected with very limited risks. This is in stark 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 (Maher and Daly 1996, Heimer 2000) or stolen goods (Cromwell, Olson et al. 1993, Stevenson, Forsythe et al. 2001, Schneider 2005) requires developing quantitative and qualitative assessments of the data, from the perspective of offenders. Such studies frequently require researchers to directly interact with offenders — either buyers or sellers of illicit goods — which in turn potentially puts researchers at increased risk for harm.

In comparison, transactions in cryptomarkets can usually be measured without direct interaction, and, using elementary precautions, generally unbeknownst to sellers, buyers or marketplace operators (Christin 2013, Soska and Christin 2015). Even if a researcher is detected while collecting data from a cryptomarket, the relatively strong anonymity guarantees marketplaces offer by design to all of their customers protect researchers as well. In particular, punitive measures are basically limited to severing the researcher's access to the marketplace, e.g., by terminating accounts associated with them, and/or providing them with incorrect data to impede researcher analysis.

Risks to researchers potentially increase after publication. At that point, researchers are publicly identified and consequently potential retribution might occur. (A notable exception, related to government censorship, is the anonymous work credited to Aryan et al. (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.[2] Overall, though, it appears that the risks associated with data collection are far smaller than those encountered in the offline world.

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

Mere data collection – prior to analysis and publication – should pose no additional risk to marketplace operators, vendors or buyers, since it only is a matter of copying existing, publicly disclosed data. However, analyzing these data could potentially result in problematic outcomes 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 therefore avoid conducting any analysis that could potentially justify law enforcement intervention or make the job of prosecuting agencies easier?

This is an interesting and complex question, worthy of further examination. It is arguable that because digital trace data gathered from cryptomarkets are public, or at least publicly accessible, anybody could be performing similar analyses. This includes law enforcement agencies that may seemingly lack expertise in advanced computational research. In fact, similarly 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 therefore 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 general public and to law enforcement. While not directly resulting in prosecution, publication of cryptomarket research may result in increased public awareness and policing

[2] See evidence GX243 in Ross Ulbricht's trial. Available at: http://antilop.cc/sr/exhibits/DX_C_le_counterintel_file.pdf. Last accessed August 28, 2015.

activity targeting online criminal activity, and subsequently increase the likelihood of prosecution. While this outcome is indeed 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

Forgetting about cryptomarkets for a moment, numerous online businesses – search engines like Google, classified forums like Craigslist are all but two examples – prohibit their 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 potential additional 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[3] and Aaron Swartz[4] cases, prosecutors have argued that violations of Terms of Service amount to unauthorized access or "access exceeding authorization" in violation of the Computer Frauds and Abuse Act. As a result, usually, research relying on breaches of contract of the 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 any of the contents. So far, we have not observed any marketplace specifying such Terms of Service explicitly. However, some marketplaces have been known to deploy anti-scraping technological measures (Soska and 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 actually 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 following argument. As discussed above, data collection for research purposes—as opposed to, say, setting up a

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

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 any 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 and much more interesting 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 et al. 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 and Greenhill 2011, Graves, Acquisti et al. Forthcoming). 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 a number of difficulties which can lead to considerable errors as Soska and Christin (2015) discuss. There unfortunately exists 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, Soska and Christin 2015, Van Buskirk, Roxburgh et al. 2015, Munksgaard, Demant, and Branwen, This volume) not only did not manage 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 seems to have 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 et al. 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 et al. 2011, Leontiadis, Moore et al. 2013, Leontiadis, Moore et al. 2014) 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 resource usage 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 collection of 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 compare soundness of various approaches.

Arguments against sharing scrapes

There are however 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 and imprisoned. 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 incident having taken place. 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 in fact, 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 still 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 most of the figures presented in the paper. Rather than sharing scrapes, he took the option to share processed data from the scrapes. To avoid possible identity leaks as outlined above, he also obfuscated all textual information, and to prevent direct correlation between vendors in the database and vendors on the Silk Road website, obfuscated the vendor IDs present in the database. In addition, he delayed release of the data to the end of 2012, while the data were collected at least six months earlier. Delaying the release of data arguably reduces the risk of interference with the environment: vendors may have rotated identities; products may not be available anymore, etc. 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 and well-founded uncertainties regarding the ethical dimensions of cryptomarket research. Given the novelty inherent to cryptomarket studies – and indeed, 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, novel and rapidly expanding field of study. We hope that more researchers will join this conversation and contribute to the development of a new 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.

References

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: Characterizing the supply side of drug cryptomarkets. *International Journal of Drug Policy*, *This Volume*.

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.

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*.

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

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

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*, *This Volume*

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*, *This Volume*

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

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., 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. and A. Maddox (In press). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research*

Branwen, G. (2015). "Dark Net Market archives, 2011-2015." Retrieved August 28, 2015, from http://www.gwern.net/Black-market archives.

Buxton, J. and T. Bingham (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)*. Rio de Janeiro, Brazil: 213-224.

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

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. and 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 10/4/16]

DeepDotWeb (2014b). Interview with Outlaw Market Admin. *DeepDotWeb*. Retrieved from: https://www.deepdotweb.com/2014/01/23/interview-with-outlaw-market-admin/ [accessed 10/4/16]

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router *Proceedings of the 13th USENIX Security Symposium*. San Diego, CA.

Dingledine, R. (2011). Tor and circumvention: Lessons learned. *Advances in Cryptology–CRYPTO 2011*, Springer: 485-486.

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

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.

Ess, C. (2002). Ethical decision-making and Internet research: Recommendations from the aoir ethics working committee. In Buchanan (ed.) *Readings in virtual research ethics: Issues and controversies*. Information Science Publishing, Hershey, PA, USA.

Eynon, R., Fry, J., & Schroeder, R. (2008). 'The ethics of internet research', in Fielding, Lee (eds.) *SAGE Handbook of Internet Research Methods*, SAGE Publications, London

Eysenbach, G. and J. E. Till (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. (Forthcoming). "Big Data and Bad Data: On the Sensitivity of Security Policy to Imperfect Information." *University of Chicago Law Review.*

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 10/9/15]

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 1/9/2015]

Lavorgna, A. (2014). "Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics." *Trends in Organized Crime* 17(4): 250-270.

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*. San Francisco, CA.

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). Philadelphia, PA, USA.

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). Scottsdale, AZ, USA.

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. and K. Daly (1996). "Women in the street-level drug economy: Continuity or change." *Criminology* 34: 465-491.

Markham, A. and Buchanan, E. (2012) Ethical Decision-Making and Internet Research Recommendations from the AoIR Ethics Working Committee (Version 2.0)

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

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

Martin, J. (In press). "Illuminating the dark net.", in Adorjan, Riciarrdelli, Chui (eds.) *Engaging with Ethics and Method in Criminological Research*, Routledge, UK

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*, *This Volume*

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

National Health and Medical Research Council (2007). National statement on ethical conduct in human research, Australian Government, Canberra.

Phelps, A. and A. Watt (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), 712-712.

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

Soska, K. and N. Christin (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14)*. Washington, DC: 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.

US Government Publishing Office, 2016. Electronic Code of Federal Regulations. Title 45 subtitle A subchapter A part 46. Retrieved from http://www.ecfr.gov/cgi-bin/text-idx?node=pt45.1.46&rgn=div5

Ur, B., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., Komanduri, S., Kurilova, D., Mazurek, M.L., Melicher, W. and Shay, R., 2015. Measuring real-world accuracies and biases in modeling password guessability. In 24th USENIX Security Symposium (USENIX Security 15) (pp. 463-481).

Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E., Sindicich, N., Matthews, A., Butler, K., & Burns, L. (2016). Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. *International Journal of Drug Policy*, *This Volume*

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 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.

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.

Weir, M., Aggarwal, S., Collins, M. and Stern, H., 2010, October. 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 (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*, Springer US.

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