Information Protection in Dark Web Drug Markets Research

J. Tuomas Harviainen
Tampere University
tuomas.harviainen@tuni.fi

Ari Haasio
Seinäjoki University of Applied Sciences
ari.haasio@seamk.fi

Teemu Ruokolainen
Tampere University
teemu.ruokolainen@tuni.fi

Lobna Hassan
Tampere University
lobna.hassan@tuni.fi

Piotr Siuda
Kazimierz Wielki University
piotr.siuda@ukw.edu.pl

Juho Hamari
Tampere University
juho.hamari@tuni.fi

Abstract

In recent years, there have increasingly been conflicting calls for more government surveillance online and, paradoxically, increased protection of the privacy and anonymity of individuals. Many corporations and groups globally have come under fire for sharing data with law enforcement agencies as well as for refusing to cooperate with said agencies, in order to protect their customers. In this study, we focus on Dark Web drug trading sites as an exemplary case of problematic areas of information protection, and ask what practices should be followed when gathering data from the Dark Web. Using lessons from an ongoing research project, we outline best practices for protecting the safety of the people under study on these sites without compromising the quality of research data gathering.

1. Introduction

In recent years, there have increasingly been conflicting calls for more government surveillance online and, paradoxically, increased protection of the privacy and anonymity of individuals. Many corporations and groups globally have come under fire for sharing data with law enforcement agencies, as well as for refusing to cooperate with said agencies in order to protect their customers. Most recently, in an effort to balance both goals, the EU enforced a wide range of privacy protection regulations under the GDPR umbrella [1], the effects of which are still debated and are to materialize over the coming years and decades.

While we might debate the balance between the need for monitoring and studying online activity and individuals' rights, the Dark Web is, arguably, an online corner where this debate has heightened implications on individuals' lives as well as on law enforcement and research into various subcultures, such as, drug users. The Dark Web represents free speech in both its anonymity and in the potential darker sides of what can be created when anonymity and uncontrolled speech – including marketing of illegal substances and services – connect. We could endlessly debate the legality or lack thereof of narcotics, or the issues of personal liberty and substance use, but that would be beside the point. What is important for this paper is that the drug subculture is, arguably, one of those with the most significant impact on individuals' lives. As a result, it has been the subject of increased research and surveillance.

Dark Web marketplaces are a growing trend in drug culture, due to issues of both novelty and perceived safety [2]. They are also currently the leading business trend on the Dark Web (see e.g., [3]). On such sites, dealers are openly promoting their wares, in environments where it is often also possible to leave vendor feedback, based on safety of the trade, price/quality ratio and so forth. These are online environments that are, furthermore, open for anyone able to locate them and use a modified browser [4]. Both of these criteria take some skill to apply, as for example search engines tend not to list drug trading Dark Web sites, but in fact not much skill is required beyond curiosity [3]. Due to the ways in which popular media has been covering such sites, curiosity by a sufficient number of users can almost certainly be guaranteed. Alongside direct social media and app use (see [5]), Dark Web sites are nowadays a key channel of access for many people wanting to sell or purchase narcotics.

In this paper, we look into how research conducted on Dark Web cryptomarkets and drug trading imageboards, particularly machine-based research, should protect data and the communities being researched while carrying our needed research around, for example, drug policy (e.g., [6;7]), understanding anonymity technologies (e.g., [3;4]), disnormative

URI: https://hdl.handle.net/10125/71184
978-0-9981331-4-0

information practices (e.g., [8;9;10]), or user name selection (e.g., [11]).

The challenges in these lines of research are varied but interconnected. First and foremost, the population being studied is anonymous, cannot be reached by "standard" means, and takes care of their lifestyles and/or addictions by using disnormative information and dark knowledge. People may take pride in being part of a drug subculture, but from a research perspective, this is not sufficient as the sole reason for sheltering any respondents. Understanding the complexity of their situation and their subculture is necessary.

Our research question is therefore *"what practices should be employed when gathering data from anonymous Dark Web drug forums?"* While earlier research has engaged with the relevant ethics in this area for the purposes of helping other researchers orient on the topic, it has not produced prescriptive lists for studying the Dark Web [2;13]. We approach the topic with a "best practices" viewpoint, rather than an angle of ethics discourse as has been previously done. Accordingly, we contribute guidelines for the ethical data gathering on Dark Web drug trading websites. These guidelines were utilized during and emerged out of an extensive research project, carried out by the authors. This three-university research project, ENNCODE, consists of deploying machine learning techniques for gathering and analyzing data from Dark Web sites, implemented in 2020-2022. This research work first gathered 9300 image board posts, coded and analyzed by the participating researchers. The posts were taken during a single night in January 2018, using copy-paste by Haasio to a Word document, and thereby represent an average vertical slice of typical discourses on a drug-trading image board.

This data set is further supported by another set consisting of over two million posts made on the same site, the structure and collection conventions of which were checked via random sampling, in order to confirm that our initial sample was sufficiently representable. To solidify our knowledge of the topic, we also interviewed four persons engaged in drug trading on the studied image board. Using knowledge acquired from dealing with our sample, we demonstrate how and why additional practices, including ethical proofreading [12], are necessary in researching this topic. With this research, we contribute to the study of Dark Web research (see [2; 3;13], as well as to information systems research that discusses online commerce.

2. The Dark Web

The so-called Dark Web is a part of the Internet, but requires specialized software to access [3]. The best known of these tools is the Tor (The Onion Router) network, but others such as the Invisible Internet (I2P), also known as "garlic routing", also exist. The idea behind these technologies is, roughly put, to peel layers of routing from the traffic, so that only the previous and next node are known. This makes the online browsing and file transfer much harder, but not impossible, to monitor.

Onion routing was originally developed for safer military communication, but it has since become a small but stable collection of web sites in which anonymity is expected and supported (see e.g., [4]). These sites contain everything from whistleblower data dumps to journalists, spousal abuse victims' support groups, and democracy movements' hidden forums, to drug trading and the sharing of child exploitation images.

Even social media companies such as Facebook now provide a Tor-based access to them [3]. The most well-known use of the technology, however, is the establishment of drug trading sites. The now-defunct online marketplaces such as the original Silk Road (2011-2013) and Alpha Bay (2014-2017) are the most famous, but numerous local variations exist.

Some of them, like the aforementioned former giants, are so-called cryptomarkets, where one could use cryptocurrencies such as Bitcoin to mail order narcotics and hormones from sellers advertising on those sites. Others are image boards where people report what they have for sale or what they want to buy, and people then set up face to face (f2f) sales using an instant messaging service such as Wickr [9].

Scholars have used mostly five types of approaches to data gathering, together or separately, but we are increasingly seeing also other alternatives. The core idea behind all of these methods is not to disturb the activities of the people who are being observed. Each of them, however, comes with its own challenges.

3. Approaches to the study of the Dark Web

Several approaches exist for gathering Dark Web data. The first approach, used by both scholars and some Law Enforcement Agencies (LEAs), is lurking. Earlier work on the ethics of Dark Web data gathering has identified this as a particularly suitable approach, due to it being non-intrusive and non-offensive (e.g., [2;13]). As many of the sites are based on anonymity, the researcher have no real way to identify themselves to the communities being studied, nor is there usually an identifiable sysop from whom they could ask for permission (see [14]).

Therefore, in contrast to the people who live-action researched drug users and their subcultures in past decades (e.g., [15;16]), the researchers are identified as researchers only when their work gets published. This sets the process apart from also many of the standard

practices of netnography (see e.g., [3;17]). As noted by Ferguson [13], lurking can be seen as breaking ethical regulations, so it is good to understand that the image boards and cryptomarkets are generally anonymous sites that do not require registration of any kind. As stated by Christin ([18]; see also [2]) in their work on the original Silk Road:

"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."

As noted by Nurmi et al. [4], the second and third approaches to the study of the Dark Web have included more traditional methods such as surveys and interviews [19;20;21;22]. Given the voluntary nature of answering such research, many of the ethical issues are alleviated, but as organizational ethnography has shown decades ago (e.g., [23]), people are not always honest informants. This is particularly the case in situations where they are protecting their professional or communal identities. This issue has been raised by scholars such as Barratt and colleagues [24] and Ferguson [13], also regarding global drug surveys' reliability. Furthermore, such open research may also create hostile reactions from the community being studied, but has sometimes also been known to be an efficient approach (see e.g., [25]).

The fourth approach to the study of the Dark Web is data scraping, in which web crawlers are used to automatically collect data from the sites. Some of the sites actively destroy all older posts beyond a certain time or quantity limit, so in order to gather any complete set of data, technical options have to be used (see e.g., [9]). The idea of scraping is to gather up digital traces left, unsolicited by the researcher, by the sites' users, and to treat those as anonymous data (see [7]). There have been significant examples of these types of studies in the last half decade (e.g., [26]), but they have also received significant critique due the selection of data involved, as well as challenges in replication (e.g., [27;28;29;30]).

If conducted without sufficient respect and/or care, scraping has the possibility to cause serious problems for both the researchers and the site's user. The sites' systems operators tend to be highly competent programmers and will note any significant intrusion in their site's traffic. Since we can presume that some LEAs are already conducting lurking and scraping on the same sites, careless scrapers also holds the potential to disrupt police or customs operations, while causing possible damage to the users of the site. LEA presence does not excuse the researchers from needing to avoid causing harm. It is therefore necessary not to attempt too much or too soon, even on sites that destroy older posts.

The central advantage of these types of studies is that they are, if properly executed, able to access the actual practices taking place on the sites, particularly cryptomarket-type sites where more or less complete transactions can be found and followed, up to and including user feedback to particular sellers or buyers. They are less useful on f2f trading sites, because the sites themselves tend to contain just advertisements but no recorded transactions, as the actual trading arrangements are conducted via instant messaging services. They do, however, sometimes contain verbal feedback on successful and failed trades, which can be recorded and studied. Cryptomarkets, in turn, may contain even start ratings similar to legal webstores [3].

Such sites bring us therefore to option five, which has been the manual taking of vertical slices from the trading sites. For example, Haasio, Harviainen and Savolainen [9] copy-pasted an anonymous image board's content during a single night to Word documents, which were then individually and together coded manually by the researchers over the course of two months. The resulting sample of messages could thereafter be analyzed as a representative sample, even if the authors also had to note some inconsistencies due to e.g., market changes created by New Year.

4. Permissions and Intellectual Property

For some sites, research permissions are however available. Some sites, such as Bluelight, have policies that openly support academia [7]. This can either be an explicit open policy or it may be the possibility to contact the systems administrator(s) for access to the content. Many designers of cryptomarkets and drug trading image boards are at the core idealists (e.g., libertarians or agorists; see [3]) with high technical skills, and very proud of their work. They may for instance just provide the platform, but do not partake in any trading and do not gather a commission. Therefore, they commit no crimes themselves, even as they provide a platform for criminal commerce. Others, however, profit directly from the trades (as did the owners of Silk Road and Alpha Bay, and the owner of Evolution, which vanished in an exit scam while $12 was held in escrow). They therefore have strong reasons not to permit researchers any access.

An extremely advantageous side of such provided data sets is that they remove not only issues related to permissions, but also those concerning intellectual property. In many cases this is highly important, because while research ethics may permit data gathering from an anonymous site that has no mandatory registration, the posters on those sites can still in some cases be considered owners of the text which they have written on that site. Oftentimes, reproducing content and

explaining its coding for academic review requires that sufficient examples are provided. These can create challenges for research, should any posters wish to identify themselves and seek reparations for intellectual property breaches. For example, a seller identified by a LEA due to reasons not relating to the research, may have nothing to lose and might seek to simply cause extra damage. Sites that explicitly permit research use of the material sidestep these problems completely, with their in-built end-user license agreements, which are visible on the site.

Another option is getting a permission from LEAs, after court proceedings are complete and confiscated servers become open evidence for further study. This is a promising avenue for research in many cases and can be done using the same kinds of scraping technologies. It is however also a proverbial can of worms: LEAs are interested in getting more data for crime prevention or criminal investigation purposes, and this can be seen by drug traders as a breach of etiquette by the researchers. It is therefore best not to apply this strategy in most cases, if one wants to also continue researching active sites.

5. How to Do No Harm: Guidelines for Drug Study of the Dark Web

In our own work, we have identified a set of policies with which to assist the safe treatment of the topic while holding on to participant safety. We have in many ways expanding on the points raised by especially Ferguson [13] and Martin and Christin [2]. This was done after discussion with the people we interviewed on their information practices on the studied sites. They all emphasized that we are here dealing with a vulnerable population that engages in disnormative and illegal practices, and thus needs special protection. Therefore, while the practices described here are typical of Internet research in general, the nature of the studied communities requires extensive care and the extension of existing safety protocols.

The first of these is a sufficiently thorough data management plan. In scraping, the gathered data has a tendency to become so massive that third-party cloud services are necessary to store and process it. Iron-clad contracts are therefore required to make sure that everything stays safe. The data management plan must contain descriptions of these contracts. All of the data should furthermore be heavily encrypted, to avoid all possibility of third-party use of it - or even interference of any kind by third parties.

The second line of protection is early-stage hashing. If possible, automated systems should be used for the purpose of one-direction hashing of all usernames from the posts, so as not to implicate any poster with a particular post. This however needs to be done with consistency, so that the same hash is recognizable as the same person throughout the material, in order to recognize different posts by the same person.

All real names need to be completely removed from the material, in cases such as e.g., the doxing of known "rats" (users who are stated as cheating in deals or as police informants). Stylometric means, in turn, can be used to remove repeated posts by human spammers and spambots, both of which are notably active on such sites. All of this is particularly important in the case of data obtained by site owners.

Two major exception to the above-mentioned process exist. The first of these is the case of username research, as conducted by e.g., Hämäläinen [11] and Harviainen, Haasio and Hämäläinen [31]. In such cases, the usernames should be removed into a separate file and analyzed without connection to the actual posts. The second exception are posts that directly relate to risks to national or international security, in the form of e.g., money laundering or terrorist funding. In such cases, should they be identified though either researcher analysis or machine-based stylometry, legal regulations in many countries may override data privacy. This is because pseudo-anonymous posters are not covered by the informant confidentiality that would protect interviewees, whistleblowers, or survey respondents.

An interesting extra complication is caused by the fact that some of the anonymous posters on drug-related image boards are underaged. The forums are hostile to such posters, who are regarded as unwelcome by the rest of the drug trader community. Reasons for this include an avoidance of extra attention from LEAs, the more severe legal penalties involved in selling to minors - and also an ideological view that one should not take drugs before a certain age [9]. Yet some youths continue posting. This would normally require an ethics board permission, and we of course recommend obtaining one whenever possible for any sort of data scraping. In some cases, however, it is possible to remove all of the posts that mention details suggesting that the poster is underage, or of someone (e.g., a LEA officer) pretending to be underage. We recommend combining both options in most situations.

It should also be noted that if one is not researching a native-language site, the user base of especially a cryptomarket may be international [2]. Local legislation and the rights of institutional review boards (IRBs) may therefore be insufficient for the task at hand. And in some cases, even native language sites may cross country lines. Examples of this include e.g., trading sites in Russian, but even the small Finnish site studied by Haasio, Harviainen and Savolainen [9] contained trading coming from Sweden. By engaging in

information safety practices, researchers significantly increase the likelihood of this not being a problem.

Interestingly, cryptomarket scholarship is often distinguished by a broad international participation and cross-disciplinary research teams [32]. Presented practices may help in this regard, setting the research framework for academics coming from different traditions and preferring the guidelines of different review boards.

On the other hand, the presented steps are general to the degree that they may respond to growing trends in the expansion of cryptomarkets. Although most studies today address English-language sites, we are dealing with the increase in the proportion of smaller scale domestic and regional trading at the expense of international ones [4;32;33;34]. This turn towards locality is due to the changing preferences of transnational vendors who are increasingly seeking to operate within their home countries. In addition, there is a growth of small, particularly non-English language cryptomarkets directed to single countries or regions.

At the same time, Dark Web markets increasingly intersect with offline drug markets. Online markets change patterns of drug consumption in a given country or the structure and organization of drug markets, as they exist outside the Dark Web [35]. This does not deny the usefulness of the presented guidelines, which – if applied accordingly – may result in data that could be the starting point for in-depth qualitative research aimed at discovering the specifics of local markets.

In our own work, we have applied all of the aforementioned measures, excluding research conducted on LEA-seized servers. They have arisen from the best practices reported by other researchers, but also from the interviews we conducted. By discussing the principles with drug users and LEA representatives, we have chosen to curate the data to a maximal extent. This is one of the two key areas – when researching the Dark Web - where understanding community members' views on how data on them may be gathered is important to inform research practices and protect the identities and lives of research subjects. Very interestingly, the interviewed community members have been highly supportive of the research, as long as they feel that they are treated with respect. The second key area, discussed in the following section, pertains to publishing of results, which, similar to data gathering from the Dark Web, requires sensitivity.

6. Publishing Research on the Dark Web

Even as e.g., Munckgaard, Demant and Branwen [30] recommend opening data sets to other researchers, we partially disagree, as have Martin and Christin [2] before us. Raw datasets contain personal information and identifiers, including outright doxing of individuals by name. With massive amounts of data, as in our case and most cases facilitated by emerging Big Data techniques, scraping and automatic name removal are bound to produce errors and leave identifiers behind. The material has to be manually curated at least once before it is released to other scholars, in order to make sure that it is compliant with e.g., local privacy laws and the EU's General Data Protection Regulation and other future regulations. It may also need to be withheld until statutes of limitations for at least non-serious crimes have passed. We acknowledge that this effectively makes some data impossible to use. On the other hand, with new Dark Web drug trading sites immediately appearing to replace the ones closed by LEAs where statutes of limitations are a concern, data and new data source are likely to remain abundant with little fears of running out of research material due to that reason in particular.

All of the material that gets published from this type of research needs to go through maximal ethical proofreading (as per [12]). In it, the researcher assumes that the subjects will be identified despite the researcher's best efforts to the contrary. Therefore, the process requires the minimization of any potential harm that could come to the subjects because of the published results.

The aforementioned techniques all contribute to minimizing risks to the studied populations, in addition to assisting e.g., data security. These techniques have all been successfully used before, in slightly less advanced forms, by researchers such as Christin [17], as well as ourselves [9]. Available machine learning methods and increased researcher awareness of Dark Web's properties allow us to do the same and more, to much larger data sets. Those datasets can then be shared with other scholars in a sufficiently curated form. This will, for example, be eventually done with our two million post dataset, once we have refined the one-directional name-hashing techniques.

Under the current climate, a thorough ethical proofreading may also require hiding data from one's research partners, especially in cases of LEA cooperation, should the data have arrived via a research agreement with an image board or a cryptomarket. And in many cases, the researcher has to choose in advance whether they want to work with the sites' open data or with LEAs, as the latter option may offend and cause risks to the users of the sites being studied.

Finally, and crucially, while it is recommended that even as the research work may be conducted at times under a pseudonym (as per e.g., [3;13], the project itself should be made visible and contactable. This may mean a project website, a user account on Wickr, or the publication of an early research paper on the topic, with

some form of contact information included. We recommend all three, as that will enable the researchers to both negotiate the boundaries of ethical issues with concerned parties in the community and to establish premises on how to deal with the interests of LEAs. For example, an early publication may, as with us, practically establish and showcase the extent to which authors are (or are not) treating the subject with respect and can lead potential partners to join in or even provide mores data or potentially re-negotiate the terms of collaboration. Work by e.g., Barratt and colleagues [24;36], like ours [31], shows that establishing a solid, positive presence as community outsiders, but not as complete outsiders, can produce positive reactions from the researched groups, as well as good quality research. We have, for instance, received the best results when we have made our identities openly known to the studied communities of drug users.

7. Conclusions

Dark Web marketplaces exist on the borderline of legality, and many of them contain criminal activities. They represent the ways in which the darker sides of privacy may come into play, yet also avoid government surveillance and contest many of the common policies for ethical research, by their practices, content and customs. In this paper, we have sought to establish principal guidelines for data collection on certain criminal activities on the Dark Web. Our main goal has been to expand from earlier research on the topic, but on a practical level, so that future researchers will be able to replicate such works, and to argue to institutional review boards that this can be done. It appears that when a suitable rapport is established between the researchers and community members, whether by interviews, personal contact, or high-quality publications, the communities' members may actually appreciate the fact that they are taken seriously and treated with respect. As pointed out by e.g., Bilgrei [37] and Enghoff and Aldridge [7], many of them are practical experts on the technical topics of the boards studied and support emic ways of harm reduction within their chosen lifestyle. They should therefore first and foremost be treated as such experts by researchers, instead of seeing just a deviant population of criminals.

By establishing guidelines and best practiced such as the ones listed in this article, it is possible to deploy new methods of data gathering to a marginal population that has largely been ignored as professional-level subjects who actively engage in online trading. As noted by Markoff [38], legend has it that the first ever online commerce transaction was the sale of a small quality of Cannabis over the ARPAnet between students in the participating universities. Studying these Dark Web sales environments in a careful manner, noting how they sometimes are similar to massive web shop giants like Amazon or eBay, how they differ [39], and how they sometimes also just functions as contact points for tiny trades [9], teaches us more about online trading in general than about drug trading in the specific. Earlier research [remove for review] has already shown that these image boards are far more heterogenous than cryptomarkets typically are, and contain very different information needs, information sharing, and also peer support, in addition to their basic function of drug trading. The accentuated, disnormative nature of these trading sites furthermore makes certain business practices more visible than they are on legal sites. This includes, for example, a very different type of customer-seller trust than what is common in other online markets.

The central challenge in all of these approaches is that they are, at the end, almost all about visible practices. The researchers, using the online data, are able to observe what is taking place, but not usually the users' motives. We therefore recommend that despite the challenged listed in this article, researchers eventually also engage in the traditional interviews or surveys, for the purpose of improved triangulation. At that stage, if they have done the earlier work with care and respect, and published signs of doing so, they will have a much easier time to locate informants willing to share their experiences, instead of hostile people who will think that the scholars are directly assisting law-enforcement agencies and should therefore be seen as a threat, and only a threat. By mitigating risks to the studied community, researchers will also reduce risks to themselves.

Acknowledgments

Parts of this research were supported by the Academy of Finland project: ENNCODE, Finnish Foundation for Economic Education (grants: 12-6385 and 14-7824), and the Academy of Finland project: Centre of Excellence in Game Culture Studies (CoE-GameCult).

References

[1] European Union, *"General Data Protection Regulation"*, (EU) 2016/679.

[2] J. Martin and N. Christin, "Ethics in Cryptomarket Research", *International Journal of Drug Policy*, 35, 2016, pp. 84–91.

[3] R. W. Gehl, *"Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P"*, MIT Press, Cambridge, MA, 2018.

[4] J. Nurmi, T. Kaskela, J. Perälä, and A. Oksanen, "Seller's Reputation and Capacity on the Illicit Drug

Markets: 11-Month Study on the Finnish Version of The Silk Road", *Drug and Alcohol Dependence*, 178, 2017, pp. 201–207.

[5] A. Oksanen, B.L. Miller, I. Savolainen, A. Sirola, J. Demant, M. Kaakinen, and I. Zych, "Illicit Drug Purchases via Social Media Among American Young People", in Meiselwitz, G. (ed.), *Social Computing and Social Media. Design, Ethics, User Behavior, and Social Network Analysis*, Springer,.New York, NY, 2020, pp. 278-288.

[6] D.S. Dolliver and J.L. Kenney, "Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison", *Victims and Offenders*, 11, 2016, pp. 600–620.

[7] O. Enghoff and J. Aldridge, "The Value of Unsolicited Online Data in Drug Policy Research", *International Journal of Drug Policy*, 73, 2019, pp. 210-218.

[8] A. Haasio, "What is Disnormative Information?", *Information and Communication Sciences Research*, 23(1), 2019, pp. 9-16.

[9] A. Haasio, J.T. Harviainen, and R. Savolainen, "Information Needs of Drug Users on a Local Dark Web Marketplace", *Information Processing & Management, preprint*, 2019.

[10] S. Burnett and A. Lloyd, "Hidden and Forbidden: Conceptualising Dark Knowledge", *Journal of Documentation*, EarlyCite, 2020.

[11] L. Hämäläinen, "User Names of Illegal Drug Vendors on a Darknet Cryptomarket", *Onoma*, 50, 2019.

[12] R.M. Lee, *"Doing research on sensitive topics"*, Sage, London, 1993.

[13] R-H. Ferguson, "Offline 'Stranger' and Online Lurker: Methods for an Ethnography of Illicit Transactions on the Darknet", *Qualitative Research*, 17(6), 2017, pp. 683–698.

[14] A. Grimani, A. Gavine, and W. Moncur, "An Evidence Synthesis of Strategies, Enablers and Barriers for Keeping Secrets Online Regarding the Procurement and Supply of Illicit Drugs", *International Journal of Drug Policy*, 75, 2020.

[15] M.H. Agar, *"The Professional Stranger"* (2nd ed.), Academic Press, San Diego, CA, 1996.

[16] H.S. Becker, *"Outsiders: Studies in the Sociology of Deviance"*, MacMillan , New York, NY, 1963.

[17] R. Kaufmann and M. Tzanetakis, "Doing Internet Research with Hard-to-reach Communities: Methodological Reflections on Gaining Meaningful Access", *Qualitative Research*, OnlineFirst, 2020.

[18] N. Christin, "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, 2013, pp. 213-224.

[19] M.J. Barratt, J.A. Ferris, and A.R. Winstock, "Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the United States", *Addiction*, 109, 2014, pp. 774–783.

[20] M.C. Van Hout and T. Bingham, "'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences", *International Journal of Drug Policy*, 24, 2013, pp. 385–391.

[21] M.C. Van Hout and T. Bingham, "'Surfing the Silk Road': A Study of Users' Experiences", *International Journal of Drug Policy*, 24, 2013, pp. 524–529.

[22] S.A. Bakken and J.J. Demant, "Sellers' Risk Perceptions in Public and Private Social Media Drug Markets", *International Journal of Drug Policy*, 73, 2019, pp. 255-262.

[23] J. Van Maanen, "Fact of Fiction in Organizational Ethnography", In Van Maanen, J. (ed.), *Qualitative Methodology*, Sage, Beverly Hills, 1983 [1979], pp. 37–55.

[24] M.J. Barratt, A. Maddox, S. Lenton, and M. Allen, "'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, 2016, pp. 50-57.

[25] R. Munksgaard*, "Intersections of Crime and Politics - A Macroanalysis of Cryptomarket Discourse*", Master's thesis, University of Copenhagen, 2016.

[26] D.S. Dolliver, "Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel", *International Journal of Drug Policy*, 26, 2015, pp. 1113–1123.

[27] J. Aldridge and D. Décary-Hétu, "A Response to Dolliver's 'Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel*", International Journal of Drug Policy*, 26, 2015, pp. 1124–1125.

[28] D.S. Dolliver, "A Rejoinder to Authors: Data Collection on Tor*", International Journal of Drug Policy,* 26, 2015, pp. 1128–1129.

[29] J. Van Buskirk, A. Roxburgh, S. Naicker, and L. Burns, "A Response to Dolliver's 'Evaluating Drug Trafficking on the Tor Network'", *International Journal of Drug Policy* 26, 2015, pp. 1126–1127.

[30] R. Munksgaard, J. Demant, and G. Branwen, "A Replication and Methodological Critique of the Study 'Evaluating drug trafficking on the Tor Network'", *International Journal of Drug Policy*, 35, 2016, 92–96.

[31] J.T. Harviainen, A. Haasio, and L. Hämäläinen, "Drug Traders on a Local Dark Web Marketplace", *Proceedings of the 23rd International Academic Mindtrek Conference,* January 2020, ACM, New York, NY, pp. 20-26.

[32] J. Martin, J. Cunliffe, and R. Munksgaard, *"Cryptomarkets: A Research Companion",* Emerald, Bradford, 2019.

[33] J. Demant, R. Munksgaard, D. Décary-Hétu, and J. Aldridge, "Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime", *International Criminal Justice Review*, 28(3), 2018, pp. 255–274.

[34] J. Van Buskirk, S. Naicker, A. Roxburgh, R. Bruno,

and L. Burns, “Who Sells What? Country Specific Differences in Substance Availability on the Agora Cryptomarket”, *International Journal of Drug Policy*, 35, 2016, pp. 16–23.

[35] J. Martin, J.D. Cunliffe, D. Décary-Hétu, and J. Aldridge, “The International Darknet Drugs Trade—A Regional Analysis of Cryptomarkets”, in Smith, R.G. (ed.), *Organised Crime Research in Australia 2018*, Australian Institute of Criminology, Canberra, 2018, pp. 95-103.

[36] M. Barratt, J. Ferris, and A. Winstock, “Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence”, *International Journal of Drug Policy*, 35, 2016, pp. 24–31.

[37] O.R. Bilgrei, “Broscience. Creating Trust in Online Drug Communities”, *New Media & Society*, 20(8), 2018, pp. 2712–2727.

[38] J. Markoff, *“What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*”, Viking Press, New York, NY, 2005.

[39] J. Aldridge and D. Décary-Hétu, “*Not an ‘Ebay for Drugs’: The Cryptomarket ‘Silk Road’ as a Paradigm Shifting Criminal Innovation”*, SSRN, 2014.