International Journal of Drug Policy 41 (2017) 101–109

Contents lists available at ScienceDirect

International Journal of Drug Policy

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

Research paper

Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement

Judith Aldridge[a,*], Rebecca Askew[b]

[a] School of Law, University of Manchester, Manchester M13 9PL, UK
[b] Department of Sociology, Manchester Metropolitan University, Manchester M15 6LL, UK

ARTICLE INFO

Article history:
Received 29 August 2016
Received in revised form 9 October 2016
Accepted 19 October 2016

Keywords:
Drug markets
Cryptomarkets
Darknet drug markets
Drug dealing
Risk taking
Risk reduction
Law enforcement
Rational choice theory

ABSTRACT

Background: Cryptomarkets represent an important drug market innovation by bringing buyers and sellers of illegal drugs together in a 'hidden' yet public online marketplace. We ask: How do cryptomarket drug sellers and buyers perceive the risks of detection and arrest, and attempt to limit them?
Methods: We analyse selected texts produced by vendors operating on the first major drug cryptomarket, Silk Road (N = 600) alongside data extracted from the marketplace discussion forum that include buyer perspectives. We apply Fader's (2016) framework for understanding how drug dealers operating 'offline' attempt to reduce the risk of detection and arrest: visibility reduction, charge reduction and risk distribution.
Results: We characterize drug transactions on cryptomarkets as 'stretched' across time, virtual and physical space, and handlers, changing the location and nature of risks faced by cryptomarket users. The key locations of risk of detection and arrest by law enforcement were found in 'offline' activities of cryptomarket vendors (packaging and delivery drop-offs) and buyers (receiving deliveries). Strategies in response involved either creating or disrupting routine activities in line with a non-offending identity. Use of encrypted communication was seen as 'good practice' but often not employed. 'Drop shipping' allowed some Silk Road vendors to sell illegal drugs without the necessity of handling them.
Conclusion: Silk Road participants neither viewed themselves as immune to, nor passively accepting of, the risk of detection and arrest. Rational choice theorists have viewed offending decisions as constrained by limited access to relevant information. Cryptomarkets as 'illicit capital' sharing communities provide expanded and low-cost access to information enabling drug market participants to make more accurate assessments of the risk of apprehension. The abundance of drug market intelligence available to those on both sides of the law may function to speed up innovation in illegal drug markets, as well as necessitate and facilitate the development of law enforcement responses.

Introduction

As drug dealers draw the attention of potential customers they risk simultaneously drawing law enforcement attention (Reuter & Caulkins, 2004). As Frith and McElwee (2007, p. 281) put it, "the need not to be known as a drug-dealer [is] offset by the more pressing need [. . .] to be known as a drug-dealer." Drug cryptomarkets address this paradox by bringing together buyers and sellers of illegal drugs in an online 'hidden' and global marketplace (Aldridge & Décary-Hétu, 2014). Cryptomarkets have been defined as: marketplaces that host multiple sellers or 'vendors'; that provide participants with anonymity via their location on the hidden web and use of cryptocurrencies for payment; and that aggregate and display customer feedback ratings and comments (Barratt & Aldridge, 2016). The world's attention was brought to the first major drug cryptomarket, Silk Road, in June 2011, after a post in the blog Gawker (Chen, 2011). Drug scholars have described initial incredulity at the discovery (e.g. Barratt & Aldridge, 2016). With illegal drug sales carrying the risk of detection and arrest, how can they be bought and sold so openly?

In traditional 'offline' drug markets, a range of strategies used by drug sellers function to minimize the risk of detection and arrest by law enforcement (e.g. Fader, 2016; Jacobs, 1996; Jacobs & Miller, 1998; Jacques & Reynald, 2012; Jacques & Wright, 2011), allowing drug markets to flourish in spite of prohibition. However, the particular risk configuration for cryptomarket drug buying and selling will differ to offline drug markets, as will risk-minimization

* Corresponding author.
E-mail address: judith.aldridge@manchester.ac.uk (J. Aldridge).

http://dx.doi.org/10.1016/j.drugpo.2016.10.010

strategies. In this paper we ask: where do cryptomarket drug sellers and buyers locate law enforcement risk, and how do they seek to reduce the risk of detection when effectively operating in plain sight of law enforcement? Researchers contributing to the growing literature on drug cryptomarkets have answered by pointing to anonymity mechanisms on these marketplaces (e.g. Aldridge & Décary-Hétu, 2014; Tzanetakis, Kamphausen, Werse, & von Laufenberg, 2015; Van Hout & Bingham, 2013). Their location on the hidden, so-called 'dark' web is accessed using software like Tor, designed to enable internet users to maintain privacy and anonymity (Lewman, 2016). Coupled with the use of non-identity carrying cryptocurrencies like bitcoin for payment, these anonymity mechanisms function to allow illegal sales to occur openly, yet remain hard-to-reach by law enforcement (Cox, 2016b). But are these anonymity mechanisms enough?

We begin by reviewing the fast-growing literature on drug cryptomarkets using Fader's (2016) framework for conceptualizing drug seller risk reduction strategies in traditional 'offline' drug markets—visibility reduction, charge reduction, and risk distribution. Rational choice perspectives have been deployed effectively in understanding drug market participation, for example revealing drug dealers' attempts to reduce the risk of apprehension and arrest by law enforcement (Jacques & Reynald, 2012). Many rational choice perspectives acknowledge that the cost-benefit assessments involved in decisions to offend are 'constrained' (e.g. Akers, 1990; Cornish & Clarke, 1986). Accessing all relevant information to enable offending decisions that minimize costs (e.g. arrest) and maximize benefits (e.g. profit) may itself be an impractical and costly undertaking, with cost-benefit assessments thereby constrained by access to limited information (Jacobs & Wright, 2010). We consider the possibility that drug cryptomarkets function as communities that enable information sharing for reducing the risks posed by law enforcement to illegal drug trading. Might online settings for criminal activity function to expand otherwise constrained rational choice?

Visibility reduction

Fader (2016) identifies strategies used by drug dealers operating in traditional offline markets to reduce the visibility to law enforcement of the routine activities of drug sales. Through environmental positioning, for example, drug dealers in open markets may select locations allowing them to discern the presence of police and pre-emptively relocate their operations (Jacobs, 1996) or employ 'lookouts' (Johnson & Natarajan, 1995). Piza and Sytsma (2016) identified faster exchanges where drug transactions took place in commercial compared to residential locations, and during daylight hours, suggesting that drug sellers attuned to the increased likelihood of onlookers modify their transaction activity accordingly. An important way in which drug dealers have reduced their visibility in recent decades is connected to readily available and inexpensive mobile phones (VanNostrand & Tewksbury, 1999), allowing buyers to contact dealers to arrange transactions in less visible private locations (e.g. Fader, 2016; St. Jean, 2008). In this way, many drug markets have evolved from 'open' into 'closed', with dealers transacting only with known customers, acquiring new customers through trusted introductions (May & Hough, 2004).

Drug cryptomarkets reverse this development. Cryptomarket vendors conduct business in plain sight of law enforcement, or indeed anyone with a computer, anonymizing software such as Tor, and the cryptomarket's URL. Yet cryptomarkets enable buyers and sellers to transact with a considerable degree of anonymity by virtue of their location on the hidden web, making it difficult for law enforcement to trace marketplace activity to participants (Lewman, 2016). Cryptocurrencies, like bitcoin, are not completely anonymous, but their use obfuscates links between payments and individuals, particularly when combined with recent developments like bitcoin tumblers that further obscure payment trails (Cox, 2016b). By allowing vendors to do business with unknown customers located across the globe, cryptomarkets can be understood as 'anonymous open' drug markets (see Aldridge & Décary-Hétu, 2016b) in contrast to the 'closed' drug markets that reduce the risk of detection for many offline retail drug dealers.

A second way that cryptomarket vendors seek to reduce the visibility of their routine business activities is connected to their reliance on postal services and delivery companies. Vendors employ often ingenious so-called 'stealth' strategies to disguise drug shipments so as not to raise the suspicion of post office, delivery and customs officials (e.g. Martin, 2014; Ormsby, 2014; Tzanetakis et al., 2015; van Hout & Bingham, 2014). Given the potential risk of arrest after parcel interception, particularly where large or international shipments are concerned (Décary-Hétu, Paquet-Clouston, & Aldridge, 2016), it is no surprise that assessment of the quality of vendors' stealth packaging features so heavily in the customer feedback that generates vendor marketplace reputation metrics (Cox, 2016a).

Charge reduction

Fader (2016) documents the strategies used by drug dealers operating in offline markets calculated to reduce the severity of legal penalties in the event of arrest. A number of these strategies can usefully be compared to the cryptomarket context.

Brokers arrange deals between buyers and sellers with little or no handling of the drugs themselves, thereby reducing the risk of being apprehended in possession of contraband. Brokering can occur in retail drug markets (e.g. Fader, 2016) but appears more commonly among upper level drug market suppliers (e.g. Adler, 1993; Pearson & Hobbs, 2003). Taylor (2015) suggests that the globalizing influence of open or 'surface' web internet drug sales makes 'drop shipping' possible, whereby retailers operating in a jurisdiction where a substance is illegal arrange purchases on behalf of their customers from manufacturers or wholesalers instructed to deliver directly to their customers. A recent Interpol report (2015) concluded that there is currently insufficient evidence of the practice on drug cryptomarkets, as has been documented, for example, with illicit online pharmacies on the clear web (e.g. McCoy et al., 2012). Soska and Christin (2015), referring specifically to the cryptomarket context, suggest a possible vendor strategy of arbitrage across marketplaces that might include such arrangements, but research has yet to ascertain whether drop shipping is used on cryptomarkets.

A second charge reduction strategy employed by offline drug dealers involves carrying only small quantities of drugs at any one time. Evidence that cryptomarket vendors elect to make small shipments to reduce the risk of interception and tracing to vendors or intended recipients has been documented by Décary-Hétu et al. (2016), who found that one of the factors that predicted vendor willingness to risk shipping drugs across international borders was lower weight deals.

Selling only to known customers to avoid the possibility of transacting with undercover police is a further charge reduction strategy documented by Fader (2016). Results from a nationally representative US survey suggest that the majority of those approached by drug dealers are drug users, with only 3–4% of non-users approached in this way (Storr, Chen, & Anthony, 2004). More risky direct approaches to unknown potential customers may be more typical in contexts like raves and dance events (e.g. Coomber, 2003); dealers here may rely on knowledge of the setting to avoid selling to undercover police.

The risks for buyers and sellers in the 'open, anonymous' context of drug cryptomarkets are obvious. Law enforcement has taken advantage of the anonymity afforded to cryptomarket participants in successful efforts that closed a number of marketplaces in November 2014 with the aptly code-named Operation Onymous, which – alongside other operations resulting in arrests of cryptomarket participants documented by van Slobbe (2016) – involve this type of marketplace infiltration. Certainly vendors can be discerning in choosing customers. Just as potential customers can assess vendor reputation metrics to inform their selection of 'trustworthy' vendors, vendors, in turn, are privy to the transaction history of buyers and can refuse those new to the marketplace or with disputes associated to prior transactions (Tzanetakis et al., 2015), but this strategy may have limited utility for avoiding undercover law enforcement. Researchers have yet to identify whether and how cryptomarket vendors attempt to avoid transacting with undercover law enforcement.

The final charge reduction strategy used in offline drug markets discussed by Fader involves dealers avoiding ties to evidence that may result in successful prosecution. She notes the use of stash houses in her own (2016) and other studies (e.g. Jacobs, 1996; Jacobs & Miller, 1998; Natarajan, Clarke, & Johnson, 1995; St. Jean, 2008). Reliance on cash payment or commodity exchanges (see VanNostrand & Tewksbury, 1999) may also function to reduce law enforcement efforts to link payments to particular buyers and sellers. Salinas-Edwards (2013) in his ethnography of retail and wholesale drug dealers documented their innovative strategies when keeping 'tick lists' – records of debt owed by customers – designed to limit the evidential links between themselves and their debtors, for example disguising these as household shopping lists, left in plain sight attached to a refrigerator with a magnet, consistent with the pretense.

Cryptomarket users limit ties to the extensive and publicly available evidence of their illegal transactions through marketplace anonymity mechanisms already discussed that function to make the identification of individuals behind aliases more difficult (Cox, 2016b). The 'digital traces' left by cryptomarket transactions (see Décary-Hétu & Aldridge, 2015) provide law enforcement – and researchers – with unprecedented data on drug supply not available for offline markets. However, once a vendor's actual identity is connected to a marketplace alias through law enforcement efforts, the vendor's entire transaction history is made available as evidence to effect arrest and prosecution. It is possible that holding separate and multiple vendor accounts across marketplaces have the effect of reducing risk in the event that these online identities cannot be linked. This possibility is suggested by the observation of Soska and Christin (2015) that the practice of vendors holding multiple accounts increased after the proliferation of cryptomarkets following Silk Road's closure by the FBI in 2013.

Risk distribution

Drug dealers operating in offline markets may attempt to reduce their risk by spreading it. Some dealers in Fader's research (2016) worked in teams, or paid employees for particular tasks like delivery or the use of houses for stashing drugs or cash. Piza and Sytsma (2016) observed that dealers more commonly employed carriers or runners when operating in commercial than residential settings, suggesting that the presence of onlookers may lead dealers to divide elements of the transaction among partners.

A number of cryptomarket features may be understood to distribute risk. Cryptomarket vendors do not deliver drugs in person, instead effectively contracting-out this risky component of the transaction to delivery services. Postal deliveries carry their own risks, however, where intercepted packages are traced to senders or intended recipients (Décary-Hétu et al., 2016). The practice of holding multiple vendor accounts (Soska & Christin, 2015), discussed above in relation to charge reduction, may also distribute risk. Vendors may operate in teams, dividing the labour involved in their enterprises, although this has yet to be documented in the cryptomarket literature.

Research aims

The literature reviewed above reveals that the particular configuration of law enforcement-related risks that cryptomarket sellers and buyers face differs in key respects from those connected to offline drug markets. Our understanding of precisely how cryptomarket participants perceive and manage these risks, however, is limited. To address this gap in our understanding, we analyse two sources of data. Postings in discussion forums connected to cryptomarkets have been characterized by Martin as a "shared repository of knowledge regarding effective concealment and counter-interdiction techniques" (2014 p. 69). We analyse postings on the discussion forum associated with the first major drug cryptomarket, Silk Road, a methodology successfully deployed by Holt, Smirnova, Chua, and Copes (2015) in connection to online sales of stolen identity data.

Second, we analyse the typically lengthy vendor-generated text found in drugs listed for sale on Silk Road. When listing an item for sale, vendors complete a form to provide relevant information, including the specific drug and quantity being sold (e.g. '$^1/_4$ ounce purple kush'), the price and postage costs. In addition – and just like on legal marketplaces like eBay and Amazon – vendors are given considerable additional scope for description. These texts provide us with a valuable opportunity to understand how vendors convey to their customers the legal risks they perceive, and their customer-focused strategies for minimizing them.

The decision to base our analyses on data generated in connection to the first major drug cryptomarket, Silk Road, rather than on marketplaces that have proliferated since, is intentional. Our data were collected only weeks before Silk Road was shut down by the FBI in October 2013, and over a year before Operation Onymous that shut down a number of cryptomarkets in November 2014 (Afilipoaie & Shortis, 2015). Décary-Hétu et al. (2016) suggest that Silk Road users, whose drug transactions therefore occurred prior to these operations and resulting arrests (see Branwen, 2015), may have viewed themselves as relatively immune from law enforcement. But was this actually the case? We aim to answer two related research questions. Did Silk Road participants believe themselves to be immune from the risk of apprehension and arrest? And to the extent that they acknowledged these risks, how did they seek to reduce them?

Methods

Data from Silk Road were scraped in September 2013 using a methodology described in detail elsewhere (Aldridge & Décary-Hétu, 2014, 2016b; Décary-Hétu et al., 2016). This process generated nearly 11,000 listings placed by vendors for the sale of drugs.

Table 1 details sample selection for analyses. Listings for a range of drugs popular on Silk Road were chosen: benzodiazepines, cocaine powder, ecstasy pills, herbal cannabis, amphetamines and tryptamines. Where vendors held multiple listings for a drug in different price/quantity amounts, one was selected randomly. 100 listings were then randomly selected for each drug to generate the sample of 600 for quantitative analysis. 50 listings for each drug were selected (n = 277) for qualitative analyses (the shortfall results from the fact that there were only 27 listings for DMT, the drug selected from the tryptamine sub-sample).

Table 1
Drug listing selection.

	Listings			
	Total including multiple vendor listings	Excluding multiple vendor listings	Retained for quantitative analyses	Retained for qualitative analyses
Benzodiazepines[a]	701	103	100	50
Cocaine powder	397	106	100	50
Ecstasy pills	444	102	100	50
Herbal cannabis	1219	239	100	50
Amphetamines	385	106	100	50[c]
Tryptamines[b]	463	106	100	27[c]
Total	3609	762	600	277

[a] Name-branded benzodiazepines were included: Xanax, Valium, Clonazepam, Lorazepam and Bromazepam.
[b] Including: DMT, 5-meo-dalt, 5-meo-DMT, ayahuasca, changa, mushrooms.
[c] Methamphetamine and DMT listings were retained for qualitative analyses in these two listing categories.

To supplement this exclusively vendor-generated data, we turned to Silk Road's archived discussion forum. Because forum participants also included buyers, these data capture buyer perspectives. After extensive reading in three relevant sub-forums ('Legal', 'Security' and 'Shipping') we inductively generated relevant terms used in various combinations to search the entire discussion forum that ran for the life of Silk Road. These included appropriate variations on: *arrest, controlled deliveries, drop shipping, drop-offs, encryption, fingerprints, law enforcement, mailbox, odours, packaging, post office, post/mailman, security, signature, stealth, tracked, undercover.*

Themes were identified in both data sources deductively in connection to visibility reduction, charge reduction and risk distribution. Qualitative analysis proceeded inductively to generate emerging theory. Consistent with discourse analytic approaches (Wetherell, Taylor, & Yates, 2001) that have been deployed effectively in drug research (e.g. Askew, 2016; Riley, Morey, & Griffin, 2008), we do not treat the texts produced by cryptomarket participants as simple reflections of behaviour, but as accounts produced for a particular purpose (e.g. to generate sales), and also therefore consider competing interpretations of these accounts. Following guidelines found in the emergingliterature on ethical conduct in research enabled though the capture – via web 'scraping' – of the 'digital traces' left by online illicit activity (Décary-Hétu & Aldridge, 2015), we paraphrase quotations so that users' online identities cannot be ascertained through searching (Bancroft & Reid, 2015; Décary-Hétu & Aldridge, 2015).

Results

Visibility reduction

While cryptomarket vendors might be thought to reduce their risk of detection and arrest by contracting out the face-to-face hand-over component of transactions to postal delivery services, it was risks in connection to shipping and delivery that most concerned buyers and sellers. Over half of listings (55%) detailed delivery practices (see Table 2) connected to reducing the visibility of this aspect of cryptomarket drug trading at the 'offline' customer end of a transaction. Some vendors instructed customers to provide real, rather than fake, names when placing orders to reduce the chances of shipment interception:

> Your postman knows your name. Please give me your real name – the same name all your mail goes to. Using fake names can alert the authorities, meaning your shipment may not arrive, and may actually get seized. Neither of us wants that to happen." (Weed V343)

Buyers shared advice on the discussion forum aimed at raising the visibility of 'legitimate' routine deliveries to avoid raising the suspicion of local delivery workers:

> I like to order a lot of stuff online so my mailman doesn't suspect the illegal stuff. Always keep to your usual routine too. If you usually go for a run when the mailman comes, okay. But if you suddenly start not being home for deliveries, that's suspicious. (Forum posting)

Buyers were aware that 'controlled deliveries' by undercover law enforcement of packages identified as suspect could lead to arrest when receiving deliveries. Although 'tracked' shipping was a service provided by some vendors, buyers were often advised to avoid shipping services that may require signatures, and not to accept packages requiring an unanticipated signature, instead simply accepting the loss. This post explained how buyers could discern that a controlled delivery might be imminent:

> My research leads me to think that you can avoid CDs by becoming aware of unusual activity in your area. I'm ultra-cautious. I know exactly when my mailman arrives, I know what he looks like, and I'm friendly with him. I know where the mail trucks are and what time they unload. I watch everything carefully in my neighborhood. Look out for anything out of the ordinary happening before you expect your delivery. Is someone you don't know parked nearby in a car on a really hot day? That might be a clue that a CD is coming your way. (Forum posting)

This vendor warned international customers that package tracking could be highly risky for illegal drugs:

> For my US and Australian customers: If you want your shipment tracked, you may have to sign for it. Where drugs are concerned, your countries are almost comically strict. Sometimes it is better to take the loss than the jail time. (Ecstasy V205)

While shipping was the most common risk that vendors identified in their listings (55%), this means that nearly as many did not highlight these risks, perhaps reflecting the tension this vendor displays between acknowledging risk and gaining customer trust.

Vendors were aware of the risk of detection connected to their offline activities when making deliveries. They shared strategies

Table 2
Vendors making listing reference to service features relevant to characterizing and minimizing legal risk (n, %).

N = 600	n	%
Risks connected to shipping	**335**	**55%**
Shipping methods	283	47%
Product packaging, including 'stealth' measures	198	33%
Refund/reship policies	106	18%
Risks connected to data security	**191**	**32%**
Data and transaction security measures taken	191	32%
Use of encryption for communication (e.g. PGP, Privnote)	124	21%

designed to reduce their visibility by disrupting the routine activities involved in making shipment drop-offs to postal services:

> Rotate your mailbox drops randomly in case LE [law enforcement] are watching particular boxes. If undercover LE makes an order it can be traced to a box. All they have to do is find TOR users in the vicinity, so avoid using mailboxes near you. (Forum posting)

When one forum poster suggested drop-offs at post offices in different cities, this response was typical of the many who pointed to the risk of entering post offices at all:

> Well done. You've now been filmed on CCTV mailing packages with illegal contents. NEVER go into a post office or hand to a postal employee. (Forum posting)

Forum discussion included advice for avoiding post office drop offs, even with international shipping:

> The trick when shipping internationally from the USA is making packages appear to be business documents so that you are not required to fill in a customs declaration, and ship the usual (anonymous!) way using a mailbox. Find out the weight that counts for 'documents with no value' so you can affix the right postage yourself. (Forum posting)

It was not just in connection to the offline work of making deliveries that vendors located and sought to reduce the risk of detection by reducing their visibility:

> You can feel friendship and camaraderie here on the vendor forum, I get that. But some on here share details of their personal lives. It's not enough to hide your name if you reveal other things that might just make you more identifiable in the end. Do you really need to say what kind of job you do? Where you went to college? What you've been arrested for? What your first language is? This all might seem to you like trivial detail with no context. But it all can add up. With enough clues, anyone can narrow it down and make a correct guess, including law enforcement. (Forum posting)

An alternative strategy for reducing visibility is suggested by this vendor: vetting potential customers who may risk drawing mainstream attention to the marketplace itself:

> Google your customers, get a feel for who they are. Do they have political beliefs about this place? Do they have 1000s of facebook friends so they can spread the word? We don't want or need this kind of exposure. (Forum posting)

This tension between publicity and obscurity has also been noted by Maddox, Barratt, Allen, and Lenton (2015) in connection to their 'digital ethnography' of Silk Road.

Packaging technique designed to reduce the risk of interception was a popular topic for discussion. 'Stealth' packaging aimed to disguise suspect contents, and functioned to reduce the visibility of cryptomarket vendor activities. Small package size was often recommended, particularly for international shipments:

> Anything that will not fit in a plain letter envelope is much more likely to not make it through customs. (Forum posting)
>
> If you ship a parcel that weighs over 13oz, you need to go to a post office, be recorded on camera, and fill in a customs form. Make it fit in a bubble envelope and avoid all this. (Forum posting)

One forum poster published a link to an FBI publication (Vajgert, 1996) detailing criteria used by the US postal service for identifying suspect packages then selected for further inspection: heavily taped on seams, packages emitting odours, hand-written address labels, misspelled names or addresses, fictitious return addresses, or names with no known connection to the destination address.

Strategies used to reduce the odours emanating from packages that could trigger parcel interception were shared. This poster pointed to the possibility that a suggested 'stealth' technique designed to reduce odour might make contents more visible:

> If you seal with two or more bags and vacuum seal the innermost bag, this compresses the bud. But it's a trade off because then it's easier to 'feel'. To be honest, I'm not sure what's better here – a vapor-tight product or a thinner package. If you decide that smell is the worst risk, be careful how you handle the first layer. Removing all odour requires moving it to a staging area and swabbing carefully with alcohol before second bagging. Without doing this, molecules on the first bag can be transferred to the second. (Forum posting)

Doing stealth 'well' may have been difficult and time consuming. Considerable discussion was devoted to the perceived inadequacies of stealth techniques used by vendors:

> Some vendors on here seem to believe that vacuum sealed powder hidden between a few sheets of paper is enough. I've done my research. After only 15 minutes the bag is vapor permeable and can be detected by sniffer dogs. This might be okay for domestic shipments, but not international, and the international market is way more profitable, especially for some substances and countries. Vendors have to up their game. That's what law enforcement is doing. (Forum posting)

Charge reduction

We found evidence of 'drop shipping' methods common in legal e-commerce on Silk Road. Drop shipping allows vendors to trade without ever possessing illegal substances themselves, by placing orders with other sellers (on the marketplace or elsewhere) on behalf of their customers to whom these other sellers ship directly. One vendor provided a lengthy and in-depth guide to drop shipping as a tool for importing from China. Other vendors used the forum to promote this service:

> I am now offering worldwide sales and drop shipping. This is ideal for agents. I'm offering discounts for agents selling big volume. Note: there will be additional shipping charges when I ship to other countries. Get in touch to discuss. (Forum posting)
>
> I have new shipping options. I can ship direct from China to your drop shipping address. Or I can re-ship from China to one of my drop shipping addresses, and then re-ship to you. (Forum posting)

This buyer asked about other buyer experiences with a known drop shipper: "Anyone had any of [Vendor name]'s mephedrone drop shipped from China? Any problems with customs, receiving shipments?" with replies indicating general praise for the drop shipping vendor. However, this practice may have been viewed as problematic by some customers:

> He finally PM-ed me saying he waits until he gets enough orders so he can order the product cheap, and then he has it drop shipped. I would NEVER have ordered from him to begin with if I'd known this was his operation. (Forum posting)

Although no undercover operations had been effected against cryptomarkets at the time of our data collection, cryptomarket users were undoubtedly aware of the possibility. We observed differing opinion about the threat of undercover law enforcement. Some appeared unconcerned, particularly in connection to small quantity transactions, deemed of little interest to law enforcement. Others were less sanguine:

> The oldest tricks in the law enforcement game: infiltration and informants. Do not let your guard down. Trust no one. (Forum posting)

But how? While cryptomarket users acknowledged that it was not possible to avoid transacting with undercover law enforcement, they shared strategies to protect themselves when this happened. The key recommendation was the use of encrypted communication, typically via 'PGP' (Pretty Good Privacy), an encryption protocol allowing message encryption that only the recipient can decrypt (Zimmermann, 1995).

> Break your connection to incriminating evidence. Never use bank transfers. Don't use an email that can be traced back to you for anything here, including the forums. Don't do business with vendors unless they use PGP. (Forum posting)

This 'good practice' was not always followed. Only 21% of the vendor listings in our sample of 600 provided PGP keys or requested that their customers use other encrypted communication methods, like Privnote (see Table 2). Even among vendors advising customers to use encrypted communications, we encountered indifference:

> You don't have to encrypt your address, but you probably should. If you prefer, use Privnote instead of PGP. But up to you. (Meth V13)

> I encourage you to encrypt your address info but I don't insist on it. SR already encrypts messages. (Ecstasy V263)

> USE PGP!! (but not required). (Weed V386)

Only 32% of vendor listings (see Table 2) referred to data security methods, which in addition to encrypted communication, included letting customers know how their data would be stored and deleted:

> All your details will be kept private and names and addresses are deleted immediately after dispatch. (Ecstasy V11).

> Security/privacy: I work alone. I save no data locally. I destroy everything as soon as it's feasible. (Cocaine V14)

Vendors were commonly advised to use gloves during preparation and delivery of shipments to reduce evidential ties to their activities. But as with much 'good practice', this was not always considered practical, and could even be thought suspicious:

> They often rip. I find them uncomfortable and hot. And wearing them is certainly not discreet when you're making drop-offs. Bandaids, latex liquid or latex tape might be good alternatives. (Forum posting)

Charge reduction strategies, while undoubtedly viewed as sensible precautions by Silk Road vendors, seem likely to have been viewed by many as additional – and perhaps unnecessary – hassle, with adoption likely not uniform.

Risk distribution

As offline drug dealers may work in teams to spread the risk of detection, so too may cryptomarket vendors. We could not ascertain how many vendors worked in teams, but one clue was found in the wording of their listings. Of the 600 vendor listings, 182 (30%) referred to operations using the words 'team', 'we' and 'our' to describe their operations:

> Don't hesitate to message us:) If you're not completely satisfied, please contact us before leaving negative feedback and we'll try to fix the problem. (DMT V2)

> Ask us any questions you like before ordering, and we'll answer as fast as we can! Benny's Team. (Cocaine V45)

Alternatively, wording like this may be deployed by vendors working alone to convey the impression of operations sufficiently successful to require additional staff.

This vendor provided customers with advice to reduce – via redistribution – the risk of detection:

> For those of you who are very security conscious, this is a tip that guarantees delivery: send someone else to pick up your package, so you don't have to worry about being seen on camera or showing ID. (Benzo V180).

Drop shipping, as discussed above in connection to charge reduction strategies for reducing risk, may also be seen as a risk distribution method.

Discussion

'Stretched' transactions across time, place and handlers

In offline retail drug markets, the time period over which a drug transaction occurs may be relatively short, often involving immediate exchange of drugs and money (Piza & Sytsma, 2016). By contrast, as our analysis shows, transactions on drug cryptomarkets are 'stretched' across time, virtual and geographical space, and handlers. An order placed in the virtual location of the cryptomarket by a customer is not received in its geographical destination until packaged and shipped by the vendor, and then delivered days, even weeks, later. The payment period is similarly stretched: customer payments are held in 'escrow' by the marketplace operating as a 'third party' until the shipment is received. And, in contrast to offline retail drug markets, shipment through postal systems requires handlers not knowingly involved in the illegal transaction: post office employees, and customs officials where these shipments cross international borders.

Drug transactions stretched across time, handlers, and physical and virtual space, make the location and character of the law enforcement-related risks faced by cryptomarket users often different to those documented in offline drug markets. In offline markets, drug dealers develop relationships of trust face-to-face with customers (e.g. Zaitch, 2005), and pay considerable attention to geographical locations to reduce their visibility to law enforcement (e.g. Jacobs, 1996). Researchers referring to drug sales on cryptomarkets have been quick to point to the contrast: drug transactions occur in plain sight of law enforcement, with cryptomarket anonymizing features protecting participants from being identified. But as our analysis establishes, the 'hidden' encrypted location of these markets is insufficient: cryptomarket users identified and sought to reduce the risk of detection by law enforcement connected to these stretched transactions, and did so even before the first successful law enforcement arrests connected to the cryptomarket drug trade.

The offline activities involved in virtual drug buying and selling

Cryptomarkets can be understood as 'anchored' in offline drug markets (Aldridge & Décary-Hétu, 2016b). While some vendors may source their supply only on cryptomarkets themselves, many will make stock-sourcing purchases offline from wholesalers in the same way drug dealers selling face-to-face do. And even though vendors transact in the virtual location of the cryptomarket, additional 'offline' activities involve them in packaging up shipments and dropping these into postal networks. To this end, vendors engaged in various risk reduction strategies: they selected delivery drop-off locations at a distance from home or work; they reduced the visibility of their routine activities by rotating drop-off points; and many avoided entering post offices where they might be recorded by CCTV.

Because shipments are handled by intermediaries not privy to the illegality involved – post office employees and customs officials at international borders – vendors used strategies aimed at reducing the likelihood that parcels might be intercepted and traced to buyers or sellers. They acknowledged the advantages of shipping drugs in sufficiently small quantities to appear as ordinary business letters, and shared advice including published criteria used by law enforcement for profiling suspect packages (Vajgert, 1996). 'Stealth' packaging strategies were aimed not only at reducing suspect visual cues of package contents, but also odours that could emanate from packages, and included wearing disposable gloves, vacuum packaging, multiple wrapping layers, and alcohol wipes. Vendors described methods for removing their fingerprints from packages, thereby limiting evidential ties to them in the event of parcel interception. Nevertheless, our results suggested that use of effective stealth practices were challenging to do well and consistently, and were sometimes discussed as ineffectively employed by vendors.

Silk Road vendors often advised customers to supply their real names for delivery: the use of fake names was believed to increase the chances that parcels would be identified as suspicious by post office employees and flagged for further investigation by authorities, potentially resulting in the 'controlled deliveries' by undercover law enforcement that has been used to effect arrests (Branwen, 2015). Vendors sometimes alerted customers requesting their shipments be 'tracked' to the possibility that law enforcement may be able to access tracking data, alongside the typical requirement of then having to sign for packages, a risk also noted by Tzanetakis et al. (2015). Our analysis of data from the vendor-generated texts in the listings they placed for sale demonstrated that both shipping and security-related risks were highlighted by vendors to customers, but not by a majority. Vendors may have been reluctant to spell out these risks plainly, preferring instead to focus on securing the trust of potential customers by down-playing risk.

The risk reduction strategies we identified for vendors and buyers contrasted: vendors *disrupted* routines involved in offline activities to make these less visible; buyers instead sought to make more visible their 'ordinary' routine activities in receiving 'legitimate' deliveries allowing their illicit shipments to slip under the radar of onlookers. These contrasting strategies nevertheless both functioned to achieve the same kind of 'contextual assimilation' described by Jacobs and Miller in connection to traditional offline drug markets: both create "images of themselves and their behaviour consistent with a non-offending identity" (1998 p. 555–6).

Our findings suggest the possibility that Silk Road vendors may have worked in teams, a risk distribution practice also identified in offline markets (Fader, 2016). Further research is required to identify the particular partnership configurations cryptomarket vendors may use to reduce the risk of detection by law enforcement. For example, vendors may employ partners to source offline supply, source packaging materials and package shipments, or make drop-offs for delivery.

Interpol (2015) concluded that there is insufficient evidence of the practice of 'drop shipping' on drug cryptomarkets, whereby vendors are able to sell to their customers without the necessity of handling the drugs themselves, by placing orders from other suppliers who then ship directly to their customers. We found evidence of drop shipping vendors on Silk Road. This practice reduces the risk of being found in possession of illegal substances connected to the usual requirement of sourcing drug supply offline, as well as holding and storing illegal drugs in their homes or elsewhere. As cryptomarkets have proliferated since, so too may the opportunities for profitable arbitrage deployed in this way across cryptomarkets.

Virtual strategies for risk reduction

Lewman (2016) suggests that as criminal activity moves online to marketplaces facilitated by anonymity mechanisms like Tor, so too do law enforcement strategies to combat it, for example cryptomarket purchases by undercover police. Our results show that Silk Road participants were well aware of this possibility. Advice to both buyers and sellers for protection in this connection was to employ strict data security measures designed to reduce the opportunity for law enforcement to link transactions to real-world identities, for example communicating only via encrypted messaging like PGP. Perhaps surprisingly, only 21% of vendor listings in our sample included a PGP key or requested customers use alternatives like Privnote for direct messaging. Some vendors referred to the use of encrypted communication only as a 'preference' they acknowledged created additional hassle. Assurances by vendors of their 'good practice' in safely deleting customer information occurred only rarely in their listings. Soska and Christin (2015) note a substantial increase in PGP adoption by vendors post-Onymous, with PGP use on two marketplaces near 90%. This suggests that law enforcement responses to cryptomarkets result in continued security innovations, thereby making cryptomarkets more resilient to undercover law enforcement efforts.

'Expanding' versus 'constrained' rational choice

Rational choice theoretical approaches to understanding decisions to engage in criminal activity consider how individuals weigh up the relative costs (e.g. arrest) and the benefits (e.g. profit) of doing so. But offenders may lack access to all relevant information – especially the extent and nature of the risk-related costs involved – in making their assessments. Although rational choice perspectives may appear to cast offenders as perfectly rational information processors, many criminologists instead characterize offender choices as 'constrained': they have only limited 'data' available to them for selecting courses of action that maximize benefits while reducing risks (Akers, 1990; Cornish & Clarke, 1986). As Jacobs and Wright explain, "obtaining complete and/or perfect information is simply too costly (in terms of time, resources, and foregone opportunities)" (2010 p. 7141). But what if the cryptomarket community reduces these costs, effectively providing participants with more, and perhaps better, data to inform their decisions? In this sense, cryptomarkets may provide opportunities for 'expanded' rather than constrained rational choice.

Our results depict cryptomarkets as communities that facilitate the sharing of 'illicit capital' that drug buyers and sellers can use to reduce the risk of apprehension and arrest. This is not to suggest that cryptomarkets create the possibility of perfect rationality. But by increasing access to relevant information that drug market participants then have at their disposal when making their cost-benefit assessments, at least some of the factors that constrain rational choices may be reduced, making online drug sellers better able to settle on suitably risk-reducing actions. This development may be important for criminologists to acknowledge in understanding a range of offending domains where individuals converge in virtual locations for illegal activity. The innovation of Silk Road in this connection was substantial: the marketplace functioned as a one-stop-shop combining drug trading with intelligence sharing, an innovation step-change compared to that identified by Holt, Blevins, and Kuhns (2014) in their research on "johns'" use of websites like Craigslist to warn others seeking the services of sex workers of law enforcement activity in particular locations.

With a rational choice lens, our analysis focused only on the 'cost' side of the assessment drug buyers and sellers make, leading

us to conclude that internet-facilitated illicit communities may enable more fully-informed rational decisions than would be possible in offline counterparts. Future research could fruitfully focus on the other side of the rational choice equation: the benefits. Does the cryptomarket community allow drug sellers to maximize benefits, for example establishing how knowledge may be shared to streamline business operations and increase profits?

Do cryptomarket users face less risk of arrest than their offline counterparts?

Cryptomarket drug sellers may share some risks with those operating offline, but we identified risks unique to the cryptomarket context. What remains to be understood is which marketplace location carries more risk of detection for buyers and for sellers. We appropriately treated the texts that comprised our data as 'discourse', acknowledging therefore that statements about practice could not be read as straightforward reflections of associated activity. We are, therefore, unable to ascertain the actual extent of adherence to 'good practice' by buyers and sellers.

We may speculate. It may be, for example, that the likely considerable social and technical capital of cryptomarket vendors gives them much in common with the 'dorm room drug dealers' studied by Mohamed and Fritsvold (2010), who were rarely caught or prosecuted. These campus drug dealers, however, were relatively unconcerned about risk, keeping packages in plain sight and having drugs mailed to them on campus, in contrast to the highly security-conscious discourse we identified on Silk Road. But the availability of shared 'illicit capital' is no guarantee that vendors and buyers will adhere to these 'good practice' standards, as illustrated by the limited use of encrypted communications we found, alongside complaints about inadequate 'stealth' packaging. Alternatively, cryptomarket drug trading may be riskier than offline drug dealing if heavier penalties are handed down in the event that a vendor's real identity is connected to marketplace aliases, making entire transaction histories available as evidence in building cases for prosecution. It seems unlikely that the same level of detailed and historical evidence would be available to law enforcement constructing cases against drug dealers apprehended in offline markets.

At least one policy-relevant reason for the importance of research aimed at establishing varying risk across drug market types is connected to effects on the price of drugs. The risks taken by drug sellers – of which arrest is but one – are thought to increase the price of illegal drugs (Reuter & Kleiman, 1986), with sellers effectively compensated for accepting risk by setting higher prices. If cryptomarkets reduce these risks, drug prices in turn may fall. Only research with appropriately matched samples can establish the relative risk of apprehension and arrest across different drug market locations and configurations.

Continuing drug market innovation

We have already seen evidence that post-Onymous vendors may be evolving their strategies for minimizing the risks of illegal drug sales in the virtual and hidden location of cryptomarket, for example with increased use of encrypted communications (Soska & Christin, 2015), thereby reducing opportunities for law enforcement to link illegal activities to identities. Our data were collected before law enforcement turned the anonymity features of drug cryptomarkets to their advantage, likely creating paranoia and mistrust among participants (Aldridge & Décary-Hétu, 2016a). However, law enforcement operations appear only to have displaced vendors to alternative markets (Soska & Christin, 2015), with recent research showing sustained growth in these markets up to January 2016 (Kruithof et al., 2016). Further research is required to understand how risks are negotiated as these marketplaces continue to evolve and innovate, with results reported here providing a useful baseline for comparison.

Reliance on legitimate postal delivery services has been described as a vulnerability for the cryptomarket trade in illegal drugs (Aldridge & Décary-Hétu, 2016a). Our analyses have located the sometimes-lengthy journey of shipments from vendor to customer, stretched across time and location, as a source of some of the unique risks inherent to cryptomarket trading. One possible future development is delivery via 'dead drops' (Reddit, 2015) that may go some way to addressing this vulnerability.

The dead drop delivery model involves a 'dropman' hiding a consignment of pre-packaged and labelled drug deals, purchased from a vendor offering the service, in a number of suitably discreet offline locations, and then making available the geo-coordinates alongside a short video for each 'dropped' deal. Only once deals have been dropped are listings with this delivery option offered to buyers. Customers making a purchase in this way can immediately access the location information and pick up the deal, with funds released to the vendor – and commission to the dropman – from escrow once pick-up is confirmed. At least one cryptomarket currently allows vendors this delivery option, but it is unknown how widespread take-up is at present. The risk that a dropman may be undercover law enforcement is possible, but a marketplace offering this delivery option contends that the risk is small; undercover police posing as dropmen can only arrest their own buyers, so necessitating them committing more serious crimes (drug supply) to effect arrests in connection only to less serious crimes. Dead drops represent a further way in which drug markets generally – and drug cryptomarkets specifically – innovate in response to the risks posed by law enforcement. Researchers must track innovative developments like these in the evolution of drug cryptomarkets.

Concluding thoughts

Cryptomarket drug trading provides law enforcement with unprecedented drug market intelligence. The data derived from the 'digital traces' of advertising and sales on cryptomarkets capture near-complete populations when compared to the typically small and unrepresentative samples available in connection to offline drug markets (Barratt & Aldridge, 2016; Martin, 2014; Tzanetakis et al., 2015). But just as illegal drug trading on cryptomarkets occurs in plain sight of law enforcement, so too does the sharing among cryptomarket users of strategies for reducing their risk of detection and arrest. This abundance of intelligence available to actors operating on both sides of the law may function to speed up innovation on the part of those involved in illegal drug supply, on the one hand; and necessitate – indeed facilitate – the development of law enforcement strategies in response, on the other. Within a context of continued global prohibition, the skills and expertise required of national and international law enforcement agencies to combat these drug market innovations will inevitably expand in response, as will the associated resources for doing so. Will cryptomarket users in post-Onymous cryptomarkets continue to share risk reduction strategies in light of the certainty they must now have that law enforcement really is watching and learning from their public discussions? Or will they become more circumspect, simultaneously undermining the cooperative pay-off of crowd-sourced wisdom, in this sense re-constraining the expanded rationality made possible in the cryptomarket community? Policy-makers, researchers, and law enforcement will need to observe developments carefully.

Acknowledgements

We would like to thank Mirjana Gavrilovic Nilsson for her research assistance on the project and David Décary-Hétu for having first collected the marketplace data, and creating the discussion forum search tool. We are grateful to David Gadd and Scott Decker for their valuable feedback on earlier drafts of the paper.

Conflict of interest

There are no conflicts of interest for either author.

References

Adler, P. A. (1993). *Wheeling and dealing: An ethnography of an upper-level drug dealing and smuggling community*. Columbia University Press.

Afilipoaie, A., & Shortis, P. (2015). *Operation Onymous: International law enforcement agencies target the Dark Net in November 2014*. Retrieved from Swansea.

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *The Journal of Criminal Law and Criminology*, *81*(3), 653–676.

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for Drugs': The cryptomarket "Silk Road" as a paradigm shifting criminal innovation*. Available at SSRN: http://ssrn.com/abstract=2436643.

Aldridge, J., & Décary-Hétu, D. (2016a). Cryptomarkets and the future of illicit drug markets. In EMCDDA (Ed.), *Internet and drug markets, EMCDDA insights* (pp. 23–30).Luxembourg: Publications Office of the European Union.

Aldridge, J., & Décary-Hétu, D. (2016b). Hidden wholesale: How drug cryptomarkets may transform traditional 'offline' drug markets. *International Journal of Drug Policy*, *35*, 7–15.

Askew, R. (2016). Functional fun: Legitimising adult recreational drug use. *International Journal of Drug Policy*, *36*, 112–119.

Bancroft, A., & Reid, P. S. (2015). Concepts of illicit drugs quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *35*, 42–49.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, *35*, 1–6.

Branwen, G. (2015). *Tor Black-Market-Related Arrests: A listing of all known arrests and prosecutions connected to the Tor-Bitcoin drug black-markets*. Retrieved from http://www.gwern.net/Black-marketarrests.

Chen, A. (2011). The underground website where you can buy any drug imaginable. *Gawker* Retrieved from http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

Coomber, R. (2003). There's no such thing as a free lunch: How "freebies" and "credit" operate as part of rational drug market activity. *Journal of Drug Issues*, *33*(4), 939–962.

Cornish, D., & Clarke, R. (1986). Rational choice approaches to crime. In D. Cornish, & R. Clarke (Eds.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 1–16).New York: Springer-Verlag.

Cox, J. (2016a). Reputation is everything: The role of ratings, feedback and reviews in cryptomarkets. In EMCDDA (Ed.), *Internet and drug markets, EMCDDA insights* (pp. 49–54).Luxembourg: Publications Office of the European Union.

Cox, J. (2016b). Staying in the shadows: The use of bitcoin and encryption in cryptomarkets. In EMCDDA (Ed.), *Internet and drug markets, EMCDDA insights* (pp. 41–47).Luxembourg: Publications Office of the European Union.

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

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international. Risk taking and the willingness to ship internationally among drug cryptomarket vendors. *International Journal of Drug Policy*, *35*, 69–76.

Fader, J. J. (2016). Selling smarter, not harder: Life course effects on drug sellers' risk perceptions and management. *International Journal of Drug Policy*, *36*, 120–129.

Frith, K., & McElwee, G. (2007). An emergent entrepreneur? *Society and Business Review*, *2*(3), 270–286.

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2014). Examining diffusion and arrest avoidance practices among Johns. *Crime & Delinquency*, *60*(2), 261–283.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Interpol (2015). *Pharmaceutical Crime on the Darknet. A study of illicit online marketplaces*. Retrieved from Lyon.

Jacobs, B. A. (1996). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly*, *13*(3), 359–381.

Jacobs, B. A., & Miller, J. (1998). Crack dealing, gender, and arrest avoidance. *Social Problems*, *45*(4), 550–569.

Jacobs, B. A., & Wright, R. (2010). Bounded rationality, retaliation, and the spread of urban violence. *Journal of Interpersonal Violence*, *25*(10), 1739–1766.

Jacques, S., & Reynald, D. M. (2012). The offenders' perspective on prevention: Guarding against victimization and law enforcement. *Journal of Research in Crime and Delinquency*, *49*(2), 269–294.

Jacques, S., & Wright, R. (2011). Informal control and illicit drug trade. *Criminology*, *49*(3), 729–765.

Johnson, B. D., & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police*, *14*(3/4), 49–69.

Kruithof, K., Aldridge, J., De'cary-He'tu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands*. Retrieved from Santa Monica.

Lewman, A. (2016). Tor and links with cryptomarkets. In EMCDDA (Ed.), *Internet and drug markets, EMCDDA insights* (pp. 33–40).Luxembourg: Publications Office of the European Union.

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*1–16. http://dx.doi.org/10.1080/1369118X.2015.1093531.

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

May, T., & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research and Theory*, *12*(6), 549–563.

McCoy, D., Pitsillidis, A., Jordan, G., Weaver, N., Kreibich, C., Krebs, B., ... Levchenko, K. (2012). Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. *Paper presented at the 21st USENIX security symposium*, .

Mohamed, A. R., & Fritsvold, E. D. (2010). *Dorm room drug dealers: Drugs and the privileges of race and class boulder*. Boulder: Lynne Rienner Publishers.

Natarajan, M., Clarke, R. V., & Johnson, B. D. (1995). Telephones as facilitators of drug dealing. *European Journal on Criminal Policy and Research*, *3*(3), 137–153.

Ormsby, E. (2014). *Silk Road*. Sydney: Macmillan.

Pearson, G., & Hobbs, D. (2003). King pin? A case study of a middle market drug broker. *The Howard Journal of Criminal Justice*, *42*(4), 335–347.

Piza, E. L., & Sytsma, V. A. (2016). Exploring the defensive actions of drug sellers in open-air markets: A systematic social observation. *Journal of Research in Crime and Delinquency*, *53*(1), 36–65. http://dx.doi.org/10.1177/0022427815592451.

Reddit (2015). *Darknet future: Dead drops*. Retrieved from https://www.reddit.com/r/DarkNetMarkets/comments/3cklw1/darknet_future_dead_drops/.compact.

Reuter, P., & Caulkins, J. P. (2004). Illegal lemons: Price dispersion in cocaine and heroin markets. *Bulletin on Narcotics*, *LVI*(1 and 2), 141–165.

Reuter, P., & Kleiman, M. A. (1986). Risks and prices: An economic analysis of drug enforcement. *Crime and Justice*289–340.

Riley, S., Morey, Y., & Griffin, C. (2008). Ketamine: The divisive dissociative. A discourse analysis of the constructions of ketamine by participants of a free party (rave) scene. *Addiction Research & Theory*, *16*(3), 217–230.

Salinas-Edwards, M. (2013). *Men at work: An ethnography of drug dealing markings and youth transitions in times of austerity (PhD)*. Manchester: University of Manchester.

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Paper presented at the USENIX Security '15*, .

St. Jean, P. K. B. (2008). *Pockets of crime: Broken windows, collective efficacy and the criminal point of view*. University of Chicago Press.

Storr, C. L., Chen, C.-Y., & Anthony, J. C. (2004). Unequal opportunity: Neighbourhood disadvantage and the chance to buy illegal drugs. *Journal of Epidemiology and Community Health*, *58*(3), 231–237.

Taylor, J. (2015). The stimulants of prohibition: Illegality and new synthetic drugs. *Territory, Politics, Governance*, *3*(4), 407–427. http://dx.doi.org/10.1080/21622671.2015.1053516.

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2015). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, *35*, 58–68.

Vajgert, G. (1996). *Profiling postal packages*. Retrieved from http://www.thefreelibrary.com/Profiling postal packages.-a018447923.

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

van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*, 183–189. http://dx.doi.org/10.1016/j.drugpo.2013.10.009.

van Slobbe, J. (2016). The drug trade on the deep web: A law enforcement perspective. In EMCDDA (Ed.), *Internet and drug markets, EMCDDA insights* (pp. 7–83).Luxembourg: Publications Office of the European Union.

VanNostrand, L.-M., & Tewksbury, R. (1999). The motives and mechanics of operating an illegal drug enterprise. *Deviant Behavior*, *20*(1), 57–83.

Wetherell, M., Taylor, S., & Yates, S. J. (Eds.). (2001). *Discourse as data, a guide for analysis*. London: Sage.

Zaitch, D. (2005). The ambiguity of violence, secrecy, and trust among Colombian drug entrepreneurs. *Journal of Drug Issues*, *35*(1), 201–228.

Zimmermann, P. R. (1995). *The official PGP user's guide*. Cambridge, MA: MIT Press.