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

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).

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.