Shedding Light on the Dark:
The Impact of Legal Enforcement on Darknet Transactions*

Jason Chan[1], Shu He[2], Dandan Qiao[3], and Andrew B. Whinston[4]

[1]Carlson School of Management, University of Minnesota,

[2]School of Business, University of Connecticut,

[3]School of Computing, National University of Singapore,

[4]McCombs School of Business, The University of Texas at Austin

ABSTRACT

Darknet markets have been increasingly used for the transaction of illegal products and services in the last decade. In particular, it is estimated that drugs make up two-thirds of darknet market transactions. The growth of illicit transactions on darknet markets have led enforcement agencies to invest greater proportion of time and efforts to monitor and crack down on criminal activities on the darknet websites. Despite the successes in convicting perpetrators, it is unknown whether these policing efforts are truly effective in deterring future darknet transactions, given that the identities of the transacting parties are well protected by the markets' features and that these participants may migrate to other darknet platforms to transact. To this end, this study attempts to empirically evaluate the susceptibility of darknet markets breaking down upon successful policing of participants on the platform. Using drug review data from three largest darknet markets, we rely on a difference-in-difference procedure to assess the impact of policing on future transaction levels, by contrasting various outcomes from the policed site with those from the non-policed sites. Our analyses found that enforcement efforts produce a negative effect on subsequent transactions on the policed site, for both vendors in the same country and in different countries as that of the arrested perpetrators. Not only do the average number of transactions per vendor decreased, we also found that the number of active vendors that remained on the site dropped significantly. This dampening effect cannot be explained by migratory behaviors, to which we interpret as evidence of a deterrence effect at work. Furthermore, we find heterogeneity effects in the enforcement effort, wherein small vendors and vendors with short site tenure are relatively more affected by the arrest shock. Study findings have policy and theoretical implications to law makers, enforcement agencies, and academicians.

INTRODUCTION

Globally, transactions on darknet markets have been growing steadily over the last few years. Specifically, a recent report documented an increase in the volume of cryptocurrency transactions on darknet markets, by which an average of $2 million worth of goods and services were transacted daily using bitcoin in 2018 (Irrera 2019). The majority of darknet transactions involves drug trading, which is estimated to account for two thirds of all transactions in this market.[1] Compared to the traditional sales of drugs on the streets, the risks of detection and violence involved in online drug transactions are lower. As such, greater market participation and transactions of illicit products/services are likely to ensue in this online economy (Chan et al. 2019). This upward trend is concerning because darknet drug transactions increases the level of international crimes as the digital nature of the Internet breaks down the geographical frictions of drug trafficking across national boundaries (Overby and Forman 2015). In addition, by connecting buyers to a wider set of drug dealers on darknet markets, these online platforms provide access to broader set of products that are not be readily available elsewhere (Brynjolfsson et al. 2003), including powerful and highly addicting specialized designer drugs which have dangerous and unpredictable side effects.

The willingness of sellers and buyers to participate in drug trading on darknet markets is spurred by a combination of protection and anonymization features of these platforms. First, darknet sites are run as "hidden services" via Tor, which conceals identifying information such as user location and IP address, making these transactions anonymous (Dingledine et al., 2004, Benjamin, et al., 2019). Second, the rise of crypto-currencies in recent years enables payments to be made for these online transactions (Nakamoto, 2008). Payments made via these crypto-currencies offer some level of user anonymization. Third, advanced privacy-enhancing techniques (e.g., Invisible Internet Project) are available to further mask the identities of the transaction parties and hide the existence of the darknet transactions (Moore and Rid, 2016). Finally, communications between vendors and consumers on the darknet are encrypted using Pretty Good Privacy

[1] https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy

which reduces the ability of third parties to surveil and monitor darknet transactions. Jointly, these techniques offer multiple levels of protection for illicit traders, which in turn facilitates the increased usage and steady growth of these markets (Soska and Christin 2015). The expansion of this illicit market requires the urgent attention of enforcement authorities. Yet, the policing of these illegal transactions is met with some difficulties. Specifically, the concealment of transactions and protection of the identities of market participants via darknet techniques have made it hard to detect and prosecute the market participants. Furthermore, the cross-national nature of darknet transactions poses legal challenges to enforcement agencies, given that the prosecutorial reach of authorities is constrained by geographic boundaries.

Despite these challenges, the enforcement agencies have attempted to monitor and prosecute darknet crimes, both through local arrests and multi-national crackdowns. Till date, these policing efforts have seen some success, by which a few darknet marketplaces were successfully infiltrated, leading to the revelation and arrest of the perpetrators and the closure of these sites (e.g., Silk Road). Although initial efforts have paid off, critics argue that such policing efforts are ultimately ineffective in deterring buyers and sellers in making future transactions (Popper 2019). Following the closure of darknet sites and arrest of users, remaining users might start new sites elsewhere in the darknet network or join other existing sites and continue transacting. Thus, enforcement may simply be driving participants deeper into the darknet instead of deterring future participation. This possibility brings up the natural question of the impact of policing efforts on darknet transactions, and whether it is beneficial to even police these sites.

On a deeper analysis, there are three possible outcomes of policing darknet transactions. First, it is possible that market participants continue in their existing level of transactions on the policed site, if they perceive a low chance of apprehension and persecution, should they deem the security and anonymization techniques of the darknet platform to be highly robust. The second outcome contrasts against the first, in that the market participant reduces or halts the transactions on the policed darknet platform, and do not engage in further transactions. This outcome is plausible, given that the general trust on darknet environment is not high (Llyod 2019). Finally, the third possibility is similar to the second in that the

participant reduces/halts transactions on the affected site, but continues to transact in the darknet environment at large, by migrating to alternative sites to avoid detection.[2] Given multiple possibilities and that darknet markets bear substantial differences to offline drug markets (Décary-Hétu and Giommoni 2016), it is empirically unclear whether the enforcement of darknet participants would deter drug trading behaviors, even in the short run. Empirical answers to this question are crucial inputs for informing policy and decision makers towards the topic of darknet enforcement.

To provide answers to the above research questions, we rely on a unique dataset on darknet transactions on three of largest darknet sites in the first half of 2014. We rely on the exogenous shock of police arrests of participants on one of these sites to understand its subsequent impacts on the transactions on the affected market. Specifically, we examine whether the policing effort affects transaction volume and the number of active vendors on the site, under a difference-in-differences (DID) framework. These analyses would allow us to infer which of the three possibilities are at work following legal enforcement. We further investigate if the police arrests would affect the users in prosecutorial jurisdictions different from arrestees. We do so by evaluating the change in transaction levels of 1) darknet participants who reside in the same country by which the enforcement agency that made the arrests, and 2) darknet participants who reside in countries different from that of the enforcement agency that made the arrests. Finally, we also analyzed whether heterogeneity effects are present across different vendor types.

Our analyses show that the arrests of darknet participants put a downward pressure on the total transactions, average transaction per vendor, and number of active vendors on the affected site. This result is also supported by analysis conducted at the vendor-level. Within the time frame of our study, we do not find evidence of vendors migrating to alternative darknet markets. Interestingly, we find that news of the arrests of US vendors can have a dampening effect on non-US vendors. Furthermore, we find heterogeneity effects in the enforcement effort, wherein small vendors and vendors with short site tenure are relatively

[2] While one of these possibilities is likely to dominate the overall outcome of darknet markets, we acknowledge that combinations of these three possibilities may also manifest.

more affected by the arrest shock. We interpret this collective set of results as a presence of deterrent effect from the darknet policing efforts, which largely affects the risk-adverse sellers who are not engaged in large scale illicit trading on the darknet markets.

This work makes a few contributions. First, it adds to the literature on darknet markets by showing insights on the nature of darknet markets and their participants. Given the novelty of darknet marketplaces, literature on this topic has been sparse. Among this thin set of literature, past works have mainly focused on documenting the transactional details of these markets, in terms of vendor characteristics, types of drugs transacted, and user network structure (e.g., Dolliver and Kenney 2016, Hardy and Norgaard 2016). Despite the pressing need to curb the growth of this underground economy, there is surprisingly little effort till date that are spent to examine the efficacy of enforcement efforts on darknet transactions. Extant work on the topic focused mainly on deriving accurate counts of transactional activities on darknet sites, and contrasting these figures before and after enforcement efforts to arrive at correlational results (Décary-Hétu and Giommoni 2016, Soska and Christin 2015, Van Buskirk et al. 2017). Building on these methods of these past works, we add to this emerging literature by undertaking the first effort of estimating the short run causal impact of police enforcement on darknet transaction levels, and to explore related questions pertaining to the extent and heterogeneous effects of enforcement.

Second, findings of this paper contribute to the body of work on two-sided markets and online platforms (Parker and Van Alstyne 2005; Rysman2009*)*. Past works in this literature have derived insights on how transactions may be affected on these marketplaces (e.g., Landsman and Stremersch 2011, Gu and Zhu forthcoming, Song et al. 2018), how the introduction of these digital platforms might create spillover effects on outcomes in alternate domains (e.g., Burtch and Chan 2019, Seamans and Zhu 2014, Wen and Zhu 2019, Krijestorac et al. forthcoming, Zervas et al. 2017), and how users derive value from platforms and their associated characteristics (e.g., Li and Agarwal 2017, Lin et al. 2018, Overby and Forman 2015). While these set of studies have generated a wealth of knowledge on markets with lawful, normal products, we continue to know very little about the nature of digital platforms for illicit products (Chan et al. 2019).

Given that darknet markets bear important characteristics that differentiate them from traditional markets, it is unclear if the insights generated from past studies would apply to the context of darknet markets. Our work aims to fill this gap by providing a first set of empirical insights on illicit darknet market which could help generate a more comprehensive theoretical understanding of how these unique markets work. Instead of following the traditional style of providing insights on how transactions may be facilitated on digital platforms, we contribute to this literature uniquely by looking whether transactions on these online markets may be disrupted by external events. By doing so, we derive a special set of knowledge pertaining to the fragility of the market transactions within illicit online platforms.

Finally, our work contributes broadly to the literature on the societal impacts of online intermediaries and the Internet in general (Chan and Ghose 2014; Chan et al. 2016; Weber 2019). With the myriad of online applications permeating into various aspects of life over the last decade, our understanding of the effects of digitalization has lagged behind the pace at which offline transactions and processes are being performed online. Consequently, the unwarranted effects of digitalization are not kept in check with appropriate interventions and policies. By studying and exposing the relationships underlying the enforcement and darknet markets, our work serves to provide a better understanding of the effects of enforcement in a digital environment, such that law makers, enforcement agencies, and academicians could generate informed and meaningful policies and further research.

LITERATURE REVIEW

Darknet Markets

Darknet sites, also referred to as "crypto-markets", are commercial websites operating on darknets via anonymity networks. They resemble regular ecommerce platforms like eBay or Amazon, except that they anonymize transactions to conceal participants' identities and prevent their online interactions from surveillance by third-parties. This property of darknet markets facilitates illicit transactions involving drugs, weapons, stolen cards, child-pornography, and other illegal goods/services on darknet markets. The fundamental driver for the emergence and proliferation of the darknet markets can be traced to the release

of Tor (Dingledine et al., 2004) and the invention of cryptocurrencies (Satoshi 2009). When a buyer makes a purchase request on a darknet market, Tor nodes route its traffic through a distributed network. The buffer built between the request client and the website server via relay nodes makes it extremely difficult to pinpoint the geographical location of the website operators and the users. After a purchase request is received, a decentralized escrow system is then used to complete the transaction. Here, the buyer does not pay the vendor directly, but instead funds a separate escrow account. The payment is only released to the seller after the buyer confirms the receipt of the item and finalizes the purchase. Under this payment process, buyers and sellers are unable to derive the personal identity and financial information of the darknet user they are transacting with, making it more difficult for undercover agents to perform investigative actions.

With the rise of the darknet markets, there is increasing academic interest on the topic. The majority of extant work have taken two main approaches to study darknet markets. The first approach analyzes the data available on the darknet sites and makes inferences about the various variables found on the platforms. For instance, Dolliver and Kenney (2016) examined the characteristics of drug vendors and contrast them across different darknet sites. Norgaard et al. (2018) studied the network structure of darknet markets, and find that their interaction network structure is less hierarchical and slightly more monopolistic than that of the traditional black markets. In a related vein of work, Broséus et al. (2017) examined trafficking flow of illicit products across countries transacted on darknet markets. Finally, Hardy and Norgaard (2016) explored whether sellers' reputation determines the prices of the goods sold in these illicit online markets.

The second approach attempts to draw a relationship between the activity levels on darknet sites and offline trends. Rhumorbarbe et al. (2016) examined the accuracy of the information posted on darknet sites by contrasting it with the physical characteristics of the transactions. Through actual drug purchases made on a darknet site, the authors found that the digital information offered on such markets (e.g., concealment methods and shipping country) is accurate, but the purity of the drugs transacted is found to be different from the information indicated on their respective listings. In a large-scale study, Dittus et al. (2018) looked at the darknet trading geography of three plant-based drugs across four of the largest darknet

markets, and compared them to the global footprint of production and consumption for these drugs. They found that cannabis and cocaine vendors are primarily located in a small set of consumer countries, rather than producer countries. Van Buskirk et al. (2016) surveyed drug users to understand the factors associated with drug purchase from darknet markets. They found that participants who purchased from dark net marketplaces tend to be younger, more likely to be involved in recent property crime, and to have used more classes of drugs in the preceding six months, relative to other users of psychostimulant drugs. Given the difficulty in linking offline observations with the obscured online data from darknet sites, there is understandably fewer studies of the second type. As a result, our knowledge of the economic interactions of darknet transactions with real world events are limited.

Of particular interest is a small set of papers within this second stream of work that explicitly studies how darknet markets are affected by law enforcement events. Soska and Christin (2015) devised a series of steps to collect and clean the darknet data from a few darknet sites. Using this data, they compared the count of darknet transactions before and after site enforcement operations. Décary-Hétu and Giommoni (2016) added to this set of findings by considering the changes to drug listing prices on darknet sites before and after Operation Onymous, a major darknet site crackdown event. Van Buskirk et al. (2017) examined the rate of increase in vendors by regressing darknet vendor count on time. These studies found correlational evidence of a fairly resilient darknet ecosystem in response to legal enforcement operations. Despite these findings, authors of these works noted that "[t]he effect of law enforcement take-downs […] is mixed at best" (Soska and Christin 2015: 41) and "the lack of evidence on an effect of law enforcement take-downs is not proof that there were no impact at all." (Décary-Hétu and Giommoni 2016: 60). Though the insights based on a count of user activity across various darknet sites across time is informative of the impact of policing on the overall market size, it does not capture the micro insights on whether enforcement is effective in deterring existing users who were transacting actively when the policing takes place. This is because an aggregated count of darknet activity includes the natural inflow of new users who join darknet sites over time due to an overall increased awareness of the darknet and greater availability of information

on how to connect to these sites. In addition, the existing literature continues to have a gap in the finer nuances of the effectiveness of enforcement, including its scope and heterogeneous impacts.

Deterrence Effects

To understand the potential impacts of enforcement on subsequent market behavior on darknet sites, it is prudent to consider the literature on the deterrence effect of policing efforts. Early work on the topic is centered on identifying the presence of a deterrence effect. Erlich (1975) has found a deterrent effect of capital punishment, while Hoenack et al. (1980) and Layson (1985) raised doubts about this finding. Subsequent works have continued to empirically validate the presence of a deterrence effect under stronger identification strategies (e.g., Cover and Thistle 1988; Kessler and Levitt 1999). Apart from the economic estimation of the deterrence effects, scholars have also attempted to theorize the possible factors that could influence the potency of policing efforts on deterring criminal behavior. One of the earliest works found that the perceived certainty of punishment, level of conformity to legal norm, and the offense type are crucial factors that can influence the likelihood of a deterrence effect materializing (Silberman 1976). On top of certainty, Beccaria (1986) and Bentham (1988) further proposed that the severity and celerity of punishment are key ingredients to deterrence. These concepts, particularly the certainty and severity of punishment, form the foundation of nearly all contemporary theories of deterrence (Nagin et al. 2015). Recent reviews of the deterrence literature concluded that the certainty of punishment, through the certainty of apprehension provides the strongest evidence for deterrence effectiveness (Apel and Nagin, 2010, Durlauf and Nagin, 2011, Nagin, 2013).

When the deterrence literature is considered under the context of darknet markets, it is theoretically unclear if a deterrence effect would ensue. Past studies on traditional illicit markets provide little guidance towards enforcement of cryptomarkets, as the past settings are quite different from that of darknet markets (Décary-Hétu and Giommoni 2016). The technological affordances of darknet platforms drastically reduce the likelihood of detection and identification of transacting parties, making them markedly different from the traditional drug trading markets. Coupled with differences in legislative punishment across countries

and the limitations of jurisdiction reach of national enforcement agencies, the perceived certainty of apprehension and punishment of transacting parties on darknet markets are further reduced. Moreover, the sales and the use of certain drugs may not always be deemed as a criminal activity in some countries and locations (Kilmer et al. 2007; Babcock and Byrne 2010). The inconsistencies in such perceptions meant that transacting parties may find it ethically acceptable to buy and sell drugs on the darknet. Taken jointly, these reasons seem to suggest that enforcement efforts on the darknet may not deter subsequent illicit drug trading.

Observations of the aftermath of crackdown operations appear to support this view. Following the closure of Silk Road in October 2013, a series of alternative markets sprung up on the darknet, including Silk Road 2.0 which is the direct successor of the old site with improved security. Furthermore, following the takedown of several darknet sites via *Operation Onymous*, sites that are unaffected by the crackdown quickly became the top markets in the darknet ecosystem. Despite these observations, there are reasons to doubt that the enforcement is ineffective in deterring future transactions. Although alternative sites have sprung up after the takedown of major darknet markets, deterrence effects might still be at play if the size of these new markets and activity levels are smaller than that of their predecessors. Specifically, it is unclear if these existing users who experienced the policing are willing to transact at the previous level conducted on the policed platforms. Given that the trust towards the website and digital commerce in general is necessary for inducing market participation and transactions (Corbitt et al 2003), existing users may not be willing to transact on alternative darknet sites under the knowledge that darknet sites have previously executed exit scams, wherein the transacting platforms had disappeared along with the escrowed cryptocurrencies. Compounding on this barrier is the difficulty in establishing trust towards websites in general (Patton and Jøsang 2004; Pavlou and Gefen 2004), which can in turn prevent transactions on these alternative sites from reach critical mass to enjoy the economics of scale of two-sided markets. Consequently, darknet users are met with high levels of uncertainty and risks, especially when they are

transacting on a new platform. Given these counterarguments, the question of whether deterrence effects would follow from legal enforcement on the darknet platforms is largely empirical in nature.

Digital Platforms

Like other commerce websites, darknet markets are digital intermediaries that facilitate the transactions between two or more sets of participants, by which the decisions of each set of participants could influence the outcomes of other sets of participants (Rysman 2009). These marketplaces are distinct from traditional markets in that participatory decisions are influenced by network effects, wherein increased value accrues to users based on the number of other market participants they can interact with (Rochet and Tirole, 2003). Based on this unique feature of online platforms, early works on digital platforms have looked at the strategies that firms can deploy to take advantage of direct and indirect network effects in these marketplaces (Eisenmann et al. 2006, Parker and Van Alstyne 2005*).* Subsequent studies investigate the micro user behavior on digital platforms, including how sellers distribute supply (Overby and Forman 2015), how buyers react to reputational information of vendors (Lin et al. 2018), and whether buyers choose to disintermediate from platforms (Gu and Feng forthcoming). In addition, scholars have also provided insights on the impact of decisions of platform owners, such as the integration with other applications (Li and Agarwal 2017), platform governance (Song et al. 2018), and the entry threat of platform owner (Wen and Zhu 2019), on user behaviors and market outcomes.

A theme that unifies most extant works on platforms is its focus on studying the effects and mechanisms occurring within the platform. While the literature is replete with the internal influences operating within platforms, the literature is largely silent on how external events may affect the market outcomes on digital platforms. However, past works have examined the opposite relationship, i.e., the impact of platforms on external trends (e.g., Burtch and Chan 2019, Chan and Ghose 2014, Seamans and Zhu 2014). Of relevance and value to the platform literature is the understanding of the stability (or fragility) of transactional relationships on platforms in face of external shocks that are not instituted by the platform ecosystem. Based on the current knowledge from the platform literature (Gu and Feng forthcoming), trust

is likely to play a role in determining whether transactional relationships on darknet platforms will continue to hold in light of policing shocks. Despite this knowledge, we do not have a full picture of the impact of external shocks on darknet market outcomes due to the theoretical ambiguity on whether participants of these markets would trust darknet platforms in performing the roles of 1) securing and masking their identities and transactions, and more importantly, 2) fulfilling the basic responsibilities of a payment intermediary to hold and release monies involved in their transactions. This uncertainty can be attributed to the fact that the nature of the transactions involved on darknet markets are illicit (Chan et al. 2019), to which public courses of redressing foul play are not available. By addressing the focal research question in this paper, we seek to fill a gap in the platform literature on the impact of external shocks on the market outcomes and stability of digital platforms, dealing with illicit products.

STUDY CONTEXT & DATA DESCRIPTION

To address our research question, we conduct analyses on the transactions taking place on Silk Road 2.0. Silk Road 2.0 (abbreviated as SR2 henceforth) came online a month after the first Silk Road site was taken down. The new site was similar to the original site in the way it appeared and functioned, except that it has a new security feature that allows user to employ PGP encryption as an additional authentication measure. To preserve user anonymity and evade detection by law enforcement, SR2 operated exclusively on the Tor network and required all its transactions to be paid for in Bitcoins. Following the initial launch of SR2, some users expressed that they were skeptical of the new site, and would wait and see before transacting on the platform. Despite this uneasiness among some users, many users were reassured by the fact that SR2 was managed by the administrators from the original Silk Road who were trusted and were known to have the experience and knowledge to evade detection and enforcement (Greenberg 2013). In less than a year since its launch, the SR2 platform grew to be the leading darknet marketplace, and was estimated to be generating monthly sales of at least USD $8 million and had approximately 150,000 active users in

September 2014.[3] The majority of the listings on SR2 were for controlled substances, including, among others, 1,783 listings for "Psychedelics", 1,697 listings for "Ecstasy", 1,707 listings for "Cannabis", and 379 listings for "Opioids".

In May 2014, the leader of a large industrial illegal drug manufacturing operation was arrested. The perpetrator, Jeremy Donagal (who goes by the nickname of "Xanax King") was arrested for producing and distributing significant quantities of illegal alprazolam (Xanax), gamma-Hydroxybutyric acid (GHB), steroids, and other drugs, on darknet sites including Silk Road (defunct during our study period) and SR2. Donagal and his associates were accused of stamping trademarks on the manufactured pills to make them look like they were produced by the pharmaceutical company, Pfizer Inc. The user account under Xanax King was run by a team of nine people and the account was involved in approximately sixty transactions each week, on average, between December 2013 and May 2014. This team of drug sellers specializes in the sales of benzodiazepines and anti-depressants, by which their sales constituted a 0.3 percent share of all weekly transactions on SR2. Following the arrest of Donagal and his associates, his SR2 account was used by enforcement agencies to engage in controlled deliveries to drug buyers on the darknet market, which subsequently led to the arrest of close to sixty other individuals in the United States. This arrest incident represents the first successful enforcement effort on SR2, by which legal agencies had infiltrated a vendor account to identify other active participants in the underground marketplace. After the series of arrests was completed, it was made known to be public in early June 2014.[4]

Data Description

In our empirical assessment of the policing impact on darknet transactions, we rely on data from three major darknet markets in 2014. Specifically, we focus on SR2, *Agora*, and *Evolution* in our analysis for a few reasons. Among all darknet markets, these three platforms ranked the highest in terms of product offerings

[3] See https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court .
[4] See https://www.gwern.net/DNM-arrests#data for further details of the arrest.

(see Figure 1). Thus, analysis results derived from these websites are likely to be representative of market behavior from other darknet platforms that are of interest (i.e., sizable darknet markets). The second reason relates to the fact that Agora and Evolution were in operation during the period when SR2 was online. In particular, our study period goes from April 2014 to October 2014, during which only one major police arrest took place on SR2, while Agora and Evolution were free from legal enforcement events. In addition, within our study period, there were no known legal enforcement activities conducted on SR2 after the arrest of Xanax King (Branwen et al. 2015)[5]. This time window enables us to avoid confounding influences from other arrests or police crackdowns, making Agora and Evolution suitable counterfactual platforms for contrasting the impact of policing shock on SR2 against. At the same time, by setting our analysis to being from April 2014, we are looking at a study period in which the sites have matured and stabilized, which reduces the chance that our estimation is picking up effects of site growth. We chose the study period to end at Oct 2014 as the SR2 was shut down a month later in a large-scale police raid, Operation Onymous, to avoid any potential anticipation effects.[6]

Our analysis focuses on the trading activities of drugs transacted on these three platforms, as this is the largest class of transactions across the darknet markets. Our data source is from a darknet scrape performed by a group of darknet researchers (Branwen et al. 2015), which have provided the approach for crawling data (Munksgaard et al., 2016). This dataset has been used by several past studies for a variety of purposes, including drug component analyses (Rhumorbarbe et al., 2016), descriptives on darknet drug trading (Demant et al., 2016), and darknet webpage structure analyses (Ghosh et al., 2017). From the archive, we rely on the scraped data of the three-top ranked darknet sites, SR2, Agora, and Evolution that goes from the beginning of 2014 to early 2015, with over twelve months' worth of transaction data. Specifically, the

[5] In our study period, a group of researchers actively monitored the arrest events across different darknet markets. We also verified such arrest events by checking the news coverage on DeepDotWeb, which is one of the most popular news sites on dark web events. (https://en.wikipedia.org/wiki/DeepDotWeb)

[6] Given that the police operation is conducted in secrecy, it is very unlikely that market participants are aware of it to take preemptive actions. Despite this, we do not completely rule out the possibility that a small set of participants might have suspected a large-scale police operation is about to take place close to the actual date of the raid. For that purpose, we adopt a conservative stance of moving the study period away from it. Empirical checks that include the weeks close to Operation Onymous yielded qualitatively similar results.

scrapes for these three websites were conducted on a daily basis to minimize the risks of missing data due to intermittent crawling blocks. Specifically, the frequent scrapes allow for the recovery of a complete set of feedbacks for each vendor, as we can rely on the data captured on other mirrors even the crawling was blocked on a particular day. Following the approach in Soska and Christin (2015), we relied on regular expressions to parse out the vendor information, product information and buyer feedback information for transactions from the scraped html pages[7]. As the values in the "*shipped from"* field are based on free responses, we further recruited an RA to manually check and label the origin information. Based on past works that utilized this dataset (e.g., Rhumorbarbe et al., 2016; Demant et al., 2018), we identify duplicate feedbacks, using Vendor ID, Product ID, Rating, Review Text and Review Date. These duplicates are removed from our dataset. On top of these steps, we further corroborate the reliability of the scraped data by comparing the scraped data with the search results of a widely used darknet search engine, GRAMS. The comparison revealed that the number of products from the two sources are not significantly different, suggesting the scraped data are of acceptable quality.

Darknet markets are unique in that these platforms would transfer crypto-payments to the vendor only after the consumer verified that he/she has received the ordered product and has left a review for the vendor (Christin 2013, Armona 2018, Dittus et al. 2018). Several darknet sites have required this procedure in the effort of making fraudulent behavior costly and to incentivize vendors to transact honestly, so that moral hazard problems on this digital marketplace can be reduced (Bhaskar et al., 2017). Relying on this fact, past works have associated the number of feedbacks with the number of transactions on darknet markets (e.g., Christin 2013; Soska and Christin, 2015). Furthermore, through an empirical validation with court evidence, Soska and Christin (2015) found the number of feedback correlate strongly with sales volume on darknet sites, making this variable an excellent proxy for darknet transactions. Similarly, we followed the approach of utilizing the number of feedbacks as a proxy to the volume of transactions on each of the sites. The summary statistics of our dataset is reported in **Table 1**. Given that the arrest event on

[7] Following past works, the country of origin for each vendor is deduced using the "shipped from" field.

SR2 targeted US perpetrators, we further split our dataset into US and non-US vendors, which is subsequently used in our analyses to understand the differences in deterrence effect across user groups.

Empirical Strategy

To assess the impacts of police enforcement on darknet transactions, we rely on the news release of the abovementioned police enforcement effort as a treatment shock to the SR2 marketplace. The use of this arrest event is appropriate for assessing the impact of enforcement on future market behavior, as the timing and success of this policing effort are likely to be exogenous. Given that the enforcement efforts on the perpetrators was conducted in secrecy, the arrested vendors and buyers would not have foreknowledge of the planned crackdowns and were unable to preemptively react to them. Furthermore, being the first successful infiltration and enforcement of SR2, the remaining participants on the marketplace were not exposed to prior arrest incidents made on this darknet platform. This scenario is beneficial for deriving a clean identification of the policing effect as it allows us to abstract away from anticipation effects that users may have should they be exposed to other policing efforts on SR2.[8] We also note that the approach of utilizing police arrest of some users as a shock to understand the deterrent effect of enforcement is superior compared to the website seize and shutdown operations. The police arrest of some users would allow undeterred users to continue transacting on the same darknet site, while the shutdown of a site would meant the undeterred users would move to alternative site to continue transacting, which may not be perfectly observed in the darknet environment. Thus, by avoiding the situation of imperfectly capturing of undeterred users transacting in alternative sites, our approach is able to arrive at a more accurate estimate of the deterrent effect of legal enforcement.

We rely on a difference-in-differences (DID) model to estimate the impact of the police arrest shock on transaction activities on the focal darknet markets. In our DID setup, we contrast the impact of the

[8] While it is possible that users may have experienced other policing incidents in other darknet sites, we argue that the effects of these prior exposures were immaterial to our estimation. The strong security and anonymization features of darknet markets made it such that information learnt from one darknet site does not inform enforcement agencies of activities of other darknet sites.

enforcement on transactions of treated vendors on SR2 with that of control vendors on Agora and Evolution. To avoid the potential confounding effect of sellers participating on multiple websites, we remove vendors on Agora or Evolution which have the same vendor names as those on SR2. Given that vendors on the control darknet sites were not policed during the same time period and that each darknet market is well protected by security and anonymization features, vendors on Agora and Evolution are unlikely to be affected by the arrest incident on SR2. Despite this, one might argue that news of the arrest of US sellers and buyers on SR2 may reach market participants in these alternative sites, which may in turn affect their decision to continue trading on their platforms. This may true for the participants based in the US, as they are in the same prosecutorial jurisdiction as the arrested vendors and sellers from SR2, making it more likely that they might also be persecuted. It might be plausible that market participants from SR2 might migrate to Agora and/or Evolution following the police arrest, making these transactions on two control sites vary systematically across the pre- and post-shock periods, invalidating the properties that the counterfactuals should bear.

Cognizant of these issues, we adopt two countermeasures in our estimation procedures. First, we restrict our control sample to include only the non-US vendors transacting on Agora and Evolution.[9] Doing so reduces the chance that the control sample are affected by the arrest incident on SR2, because these market participants are beyond the scope of US prosecutorial jurisdiction and would consequently be less susceptible to reducing their transactions on the control darknet sites. Second, we conduct statistical tests to contrast the transaction levels on Agora and Evolution before and after the police shock to see if the SR2 policing shock produced a systematic shift in transaction levels on these control sites. On top of this check, we further assess if migrating behavior took place between SR2 and the control sites by examining the trend of new users that join the control sites after the shock and contrasting it to the pre-shock trend to see if there was a significant spike. Our main regression specification is as follows:

[9] Vendors with missing information on their origin is not included in our analysis. This vendors with missing information form a small percentage of the full sample.

$$y_{ijt} = \alpha_0 + \alpha_1 * PolicingEffort_{it} + website_i + drug_j + week_t + \varepsilon_{it}, \quad (1)$$

where y_{it} is the logarithm transformed dependent variables, including the total number of reviews, average review count per vendor, number of vendors with active transactions each week, and number of remaining vendors at site *i* for each drug *j* sold in week *t*. The total number of reviews at each site provides us with insights on how the overall transaction volume have shifted as a result of the enforcement. While an analysis of this outcome variable tells us the overall efficacy of enforcement on darknet sites, it does not tell us how the exact role of enforcement in the darknet context. As a result of the policing shock, vendors might become more cautious by 1) decreasing their transaction levels and/or 2) exiting the treated site altogether. To get insights on these two possibilities, we rely on three other outcome measures, namely the average weekly count of reviews per vendor, the count of vendors with active transactions each week[10], and the number of remaining vendors. We were able to see if a vendor remains on the site based on the date he/she receives his/her last review on the darknet site. In the case where the last review was posted within a month of the end of our study period, we perceive the vendor to be active throughout the study period. The first two outcomes provide a sense of whether each vendor is decreasing the intensity of their transactions, while the third outcome tells use if vendors are exiting the market.

The *PolicingEffort* variable in Equation 1 is used to indicate drug listings on SR2 after the news release of the policing event, i.e., June 2nd, 2014, and is '0' otherwise. This term is our main estimate of interest and is the DID estimator that captures how the transactions of vendors on SR2 change before and after the policing event, relative to the change in transaction levels on the alternative darknet markets over time. Because of potential differences across the various darknet sites under consideration, we include a Website fixed effect to account for potential heterogeneity. A drug fixed effects is included in these DID specifications to account for heterogeneity across the demand and supply patterns for different drugs. In

[10] A vendor may be inactive in one week and be active in a subsequent week. This measure serves to capture the amount of transactional activity each week.

addition, we include a week fixed effects to account for temporal changes in demand and supply conditions in the drug market.

While these site-drug level analyses allow us to quantify how the aggregate transactional activities might change across treated and control sites due to the arrest event, we also wanted to get insights on how the enforcement might influence individual trading behavior at the vendor level. Analysis at the individual level is also able to capture the finer heterogeneous effects, resulting in more precise estimates. For this purpose, we restructured our dataset to perform an additional set of vendor-level analysis. Specifically, we estimate the following model.

$$y_{kt} = \beta_0 + \beta_1 * PolicingEffort_{kt} + vendor_k + week_t + \varepsilon_{kt}, \quad (2)$$

where the dependent variable is the number of reviews each vendor *k* has in each week *t*. For the vendor level analysis, the *PolicingEffort* variable is '1' for vendor *k* who transacts on SR2 after the news release of the arrest event, i.e., June 2nd, 2014, and is '0' otherwise. A vendor fixed effects is included in the model to account for heterogeneous effects across vendors and a week fixed effects is included to account for systematic temporal shifts in the drug market in each week. Given that Equation 2 is conducted at a finer level, it might appear to be more superior compared to Equation 1. However, we note that the vendor level analysis is unable to produce insights on the average transaction per vendor and the count of vendors, which is why Equation 2 is used as a supplementary specification to affirm the robustness of the results in Equation 1. We estimate all models using an OLS specification, but also rely on a fixed effects negative binomial specification to assess the robustness of these results, given that the outcome variables are of a count nature. For analyses in Equation 1 and 2, we focus on the transactions of US treated vendors, as these participants are most directly affected by the treatment shock. Subsequent sub-analyses look at non-US treated vendor to derive further insights on the scope of the enforcement effect.

RESULTS

Main Results

We first report the results of Equation 1 in Table 2. Across Columns 1-4 of **Table *2***, we see that the DID coefficient is negative and significant, indicating that the number of total reviews, average reviews per vendor, number of vendors transacting each week, and the remaining vendors for treated drug transactions decrease significantly after the policing efforts on SR2, relative to those of the counterfactual drug transactions. Specifically, news of the arrest of US-based participants on SR2 led to a 76.6% decrease in total number of transactions on SR2 (Column 1). We further learn that this drop is result of both a decrease in the transaction intensity of vendors and a decline in the number of remaining vendors. Specifically, we see a decrease of 36.2% in average transaction volume per vendor (Column 2) and a decline of number of vendors with active transactions in each week by 58.9% (Column 3). The size of the remaining vendors on SR2 has dropped by 58.9% (Column 4). The coefficient magnitudes for Columns 1 and 4 indicate the weekly drop in transaction levels (~14,522) and vendor count (~65) are much larger than the weekly transactions of the arrested vendor (~60) and the arrested vendor account (1 account). Given that the arrest led to a decrease in transactions and vendors beyond that of the arrested market participants, these regression results are indicative of the presence of deterrence effects emanating from the arrest incident.

We next look at results from the vendor level analysis. Results of this analysis is documented in Column 5 of **Table *2***. We see that by analysis at a finer vendor level yields a similar conclusion in that policing efforts induce a deterrent effect on subsequent transactions. In particular, treated vendors decrease their transactions by 58.1% relative to their counterfactual vendors on alternative sites after the release of news of the arrest incidence. This figure corresponds to a reduction of 12.5 transactions on average. Taken jointly, results from the site and vendor level analyses indicate a decrease in drug transactions on the treated vendors after the policing event, further pointing towards the presence of a deterrence effect.

Parallel trend test

A fundamental assumption for the DID analysis is the parallel trend assumption (Angrist and Pischke 2008), which requires the difference between the control and treatment groups to be constant over time, in the absence of treatment. Violation of this assumption can lead to biased estimates. This assumption is generally

not testable because we cannot observe the counterfactual, post-treatment outcome of the treatment group. Existing literature on the DID partially assess the validity of assumption by examining whether there is a pre-shock trend. A common approach to this check is to include estimates of the leads and lags of the treatment effect (Autor 2003). Should the parallel trend assumption be satisfied, the interaction with the lead terms should yield nonsignificant coefficients.

Using this procedure, we derive the estimated coefficients for the leads and lags for all of outcome measures (**Figure *2***). Generally, the coefficients before the arrest shock are not statistically different from zero. This test indicates that the parallel trends assumption is satisfied and the DID approach is likely to be valid. In addition, we see the coefficients in the post-shock period are negative and significant, which signifies that the impact of the enforcement effort shows up strictly after the shock. More revealing in the figure, the negative effect increases in magnitude over time in general, suggesting that the deterrence effect of the policing effort grows.

Validity of Control Platforms

A concern with the approach taken above is that vendors might leave SR2 upon knowledge of the police arrests and migrate to the control darknet sites. If this happens, then the chosen control sites, Agora and Evolution, would not be appropriate counterfactuals as the arrest event has an indirect influence on the transactional activity on these sites. To explore the possibility on whether the number of new vendors increase significantly on Agora and Evolution in the post-treatment period, we perform two empirical assessments. First, we plotted the weekly number of new vendors on the control sites using at the number of vendors in *t-1* period as a reference group. In ***Figure 3***, we see that the number of new vendors on the two control websites in the post shock period is not significantly different from that in the reference period, in general. We note that the number of new vendors were lower in t+4 and t+14 after the arrest news

disclosure. Given that there are only two drops and they are spaced apart in time, we interpret as a natural perturbation of the inflow of new vendors on the two darknet sites.[11]

Since the time of gaining trust from buyers can be lengthy, migrating vendors are motivated to use the same username (or at least a similar sounding username) on the alternative darknet platform, so that they can be recognized by their customers on SR2 so that they can continue transacting with them on Agora and Evolution. Relying on this fact, we conduct a second set of tests where we assess if vendors are migrating to these two control sites. Specifically, we tabulate the number of vendors across SR2 and the control sites and count the vendors with the exact same name. As seen in **Figure *4***, the number of new vendors on the control sites that bear the similar username as that on SR2 very few (dotted lines), relative to the number of new vendors joining the sites each week (solid lines). Furthermore, the trend of new users with similar usernames were similar before and after the policing incident, suggesting that the treatment shock is unlikely to induce any migratory behavior from SR2 to Agora.[12] In sum, this set of tests did not indicate issues of utilizing Agora and Evolution as counterfactuals in the DID setup.

Robustness Checks

Placebo test

To assess if the estimated significant treatment effects arose by chance, we perform a placebo test by randomly assigning vendors from the three darknet sites as the treated vendors. Specifically, we randomly selected 50% of all vendors across all sites to be treated units and reran the main DID analysis. This procedure was performed for 10,000 times, to which we took the average values of the coefficients and standard deviations. If the reported results arose coincidentally, then the estimates under this placebo test should yield negative and significant coefficients on the DID estimate. Results of this test are reported

[11] We see that there is a pre-shock week (t-7) that also had a relatively lower number of new vendors. The presence of dips in new vendors in weeks before and after the shock suggests that these are likely to be coincidental shifts in vendors. We conducted a robustness check where we remove those two time periods where there is a significant drop in vendors on the control sites from our main analyses. Results remain qualitatively similar to in those analyses.
[12] We perform a further robustness check where we employ a stricter criterion by removing vendors with similar sounding names (based on a difference of 1-2 characters from the original SR2 username) in a formal regression.

Table *3*.[13] As seen in the table, the estimated treatment effects are not statistically significant from zero, indicating that the observed negative treatment effects are unlikely to arise by chance.

Matching

One concern on the above analysis is that there might be differences between the vendors on control darknet platforms (i.e., Agora or Evolution) and the vendors on the treated platform (i.e., SR2). To alleviate this potential issue, we match vendors in the control group and treatment group based on their characteristics before the arrest event. Specifically, we consider the following covariates in the matching process using coarsened exact matching (CEM):[14] the number of reviews, total dollar sales earned, total number of drug categories transacted, total number of unique drugs transacted, tenure on the site, and the number of weeks with active transactions. After performing the matching procedure, we conduct t-tests and Kullback–Leibler divergence test to verify that the vendors in the control and treated groups are statistically equivalent across all matching covariates. As reported in ***Table 4*****,** we see that CEM has arrived at a balanced set of treated and control vendors. Using these matched vendors, we re-performed the main analyses for the site and vendor level analyses. The results in ***Table 5*** show that results from the matched sample are qualitatively similar to those reported earlier.

While CEM provides us with some confidence that the static differences across vendors are not driving the main results, it is possible that time varying confounders may be influencing the results. As such, we further rely on synthetic matching to construct a statistically comparable control units, through the weighting of counterfactual vendors' information over each period so that time-varying characteristics can also be accounted for (Abadie et al. 2010). To this end, we employ a generalized synthetic control method (Xu 2017) with both time and drug level fixed effects. The corresponding estimated treatment effects of the synthetic matching methods are presented in ***Table 6***. The results are consistent with those derived from the unmatched analysis. This provides us further confidence in our main empirical results. A

[13] A visual representation of this simulation is documented in Figure A1.
[14] We adopt the k2k matching option for the CEM matching.

visual presentation of the treated and control group's total reviews, average review per vendor, and number of active vendors before and after the treatment shock is presented in ***Figure 5.*** In particular, *Figure 5A* shows the results under the synthetic control method with total number of reviews for each drug type on each site as the dependent variable; *Figure 5B* shows the results with the average number of reviews as the dependent variable; *Figure 5C* shows the results using number of vendors with active transactions each week; *Figure 5D* shows the result using the number of remaining vendors. As seen in these figures, the synthetic matching method is successful in producing highly comparable trends for the treatment group and the constructed "control groups" in the pre-arrest period. After the arrest, we observe that various measures of the treatment group were significantly lower than those of the control group, supporting the results in the main analyses.

Negative Binomial Model

As our main dependent variables are all count variables with over dispersed distribution, we perform another set of robustness checks to which we use the negative binomial specification. The estimated results are reported in **Table *7***. Overall, the results are consistent with our main results, in that the policing incident brought about negative and significant impacts on the various measures of transaction intensity and vendor count. These tests indicate that our results are robust towards alternative model specifications.

Multihoming Vendors

In our main analysis, we remove vendors on control websites which share the exact same vendor names to exclude the potential confounding effect of multihoming. Sellers multihoming on SR2 and the control sites, may decide to transact more on Agora and Evolution, after learning about the policing activity of a SR2 vendor. While a formal test has been conducted earlier to ascertain the validity of our control sites, we wanted to conduct a further robustness check to see if our main results are affected when we adopt a stricter approach in accounting for multihoming vendors with switching behaviors. It is possible that the same seller may transact on different websites using similar but not the exact same usernames. Following the common-substring method (Soska and Christin 2015; Van Buskirk et al., 2017), we conducted a pairwise comparison

on vendors' names across different websites, by measuring their between-string Levenshtein edit-distance. Vendors that operate on multiple markets tend to use the same or similar aliases with tiny variations to accumulate their reputation among consumers. The pairwise match by edit-distance hence allows us to capture the potential variations and identify these multi-homing vendors. To account for such multihoming vendors, we drop all vendors on control websites whose usernames differ from those on SR2 by two characters.[15] The estimated results under this stricter approach are reported in ***Table 8***. Overall, the results under the stricter sample are consistent with our main results, in that the policing incident brought about negative and significant impacts on the various measures of transaction intensity and vendor count, indicating that our results are robust even after accounting for the possibility of multihoming sellers.

Vendors with Unclear Origins

In our main analysis, vendors on Agora and Evolution who did not specify U.S. as their origin (based on their "Shipped from" variable) are treated as control vendors. Within the data, some vendors specified that the their "Shipped from" information as "Worldwide". Since "Worldwide" may include vendors from originate from the U.S., a stricter approach would be to exclude control vendors that specified "Worldwide" in their "Shipped from" location when conducting the analysis. We did so and repeated our main analysis under this stricter sample. Results under this sample is presented in ***Table 9***, to which we find that they are qualitatively similar to our main findings.

MECHANISMS

Thus far, our analyses have established a negative effect of legal enforcement on the subsequent transactions of vendors on the policed darknet site. This deterrent effect is found to hold for vendors who are within the same prosecutorial location as the arrested users (i.e., the U.S.). Our checks have also found that this decrease is unlikely due to treated users migrating to alternative darknet sites, as we do not see

[15] For example, "white_shark" is one character different from "whiteshark".

evidence of a significant increase in transactions at the other top two darknet sites after the shock.[16] Despite these findings, the extent of the uncovered deterrence effect remains unclear. In particular, two open questions remain. First, when considering the policed darknet site, it is plausible that the enforcement effort might also deter participants who are from different prosecutorial jurisdictions but are transacting on the same policed platform. Specifically, the above analyses were limited to only US based vendors on SR2, but non-US based vendors may also be affected by the arrest event. Second, we do not have a clear idea on the profile of vendors that are deterred by the policing effort. In particular, we do not know which type of vendors are more sensitive towards legal enforcement and are affected by it. We conduct further tests below to provide insights to these two questions.

Effects on vendors from other countries

A common belief is that the deterrent effects of policing are constrained to reducing criminal activities within the local prosecutorial jurisdiction, as varying legislative regulations and a lack of coordination across policing units in different geographies would undermine the probability of arrest of criminals in other regions. Despite this general trend, drug trafficking on darknet markets is considered an international crime to which the policing agencies in different countries have agreed to collaborate on cracking down. In our context, it is plausible that the arrest of U.S. vendors might also have a deterrent effect on other vendors from different countries, given that the successful enforcement at SR2 is evidence that the darknet market is not foolproof and that enforcement agencies in countries other than the U.S. have an interest in cracking down such activities.

We repeat the main analyses above by using non-U.S. vendors as the treated sample, in place of the U.S. vendors. The results of this analysis are reported in the Columns 1-4 of ***Table 10***. Interestingly, we observed that the arrest event led to a negative and significant impact on transaction volumes and vendor count for non-U.S. vendors on SR2. The results show that the number of total reviews from non-U.S.

[16] Given the large drops we see on SR2, should migration to the two alternative sites happen, we would see huge spikes in the new user count on Agora and Evolution. Figure 3 shows that this is not the case.

vendors decrease by about 69.4% (Column 1), the average review per vendor decrease about 25.2% (Column 2), the number of vendors with active transaction each week decrease about 55.8% (Column 3), and the number of remaining vendors on the site dropped by 55.1% (Column 4). Compared with results based on U.S. vendors on SR2, the raw magnitude of the deterrent effect appears to be smaller for non-U.S. vendors, though these differences are not statistically significant. Based on these results, it appears that the deterrence effect of the policing effort has the ability to impact transactional behavior of vendors that are beyond the prosecutorial jurisdiction of the enforcement agency. We further repeat the analysis using vendor level data, which produced a similar conclusion (Column 5).

Heterogeneous effect across Vendors

Certain vendors may have more to lose from the halting their transactions on the darknet site compared to other vendors. In particular, vendors who have been successful in making large volumes of drug sales on the market may lose the opportunity of benefitting from a great amount of profit, which can be considered a greater loss compared to the potential of legal persecution. In this sense, smaller vendors are more likely to be affected by enforcement efforts, relative to the large vendors. To test if such an intuition is true, we divide all vendors into two groups based on a median split of their pre-treatment number of transactions (based on review count). Small scale vendors have a transaction volume lower than the median value of all vendors, and vice versa. We further tabulated the number of small and large vendors for each drug type on every website. Based on the split sample of small and large vendors, we conduct the same regression analysis from our main specification. From ***Table 11***, we see that although both types of vendors experience a negative and significant impact from the arrest shock, the magnitude from the small-scale vendors are at least four times larger than that of the large-scale vendors (Columns 1-2, and 4-5). This trend holds true for both US-based vendors and non-US based vendors. We repeat this test by including a dummy term that indicated whether if the vendor was a small-scale vendor, and its interaction with the DID term, in a regression model on the full sample of all vendors. In this specification, we find that the newly added interaction term is negative and statistically significant for both the US and non-US vendors (Columns 3

and 6), which goes to indicate that the enforcement impact does have a significantly larger effect towards deterring small-scale vendors, relative to large-scale vendors.

Furthermore, vendors who have been in the market for a longer time with a greater sunk cost of market participation may be less willing to reduce transaction levels and/or exit the platform. Specifically, it is more costly for vendors with longer tenure to abandon their profile which they took time and effort to build up their reputation and connections. Thus, they are more likely to disregard the policing shock and continue to operate as before in the post shock period. To assess for this possibility, we divide all vendors based on a median split of their user tenure on the platform and understand how each group of vendors are affected by the policing shock. The results are reported in ***Table 12***. We see that although both types of vendors experience a negative and significant impact from the arrest shock, the magnitude from the new vendors are at least four times larger than that of the old vendors (Columns 1-2, and 4-5) for both US-based vendors and non-US based vendors. This result shows another user dimension of vendors that experience heterogeneous effects of the enforcement effort on the darknet platform.

DISCUSSION & CONCLUSION

In this study, we assess and quantify the short-term impact of legal enforcement on darknet transactions using a unique dataset that contained transactions of three prominent darknet sites. Relying on an exogenous shock of a police arrest of a segment of darknet participants on SR2 during our study period, our difference-in-difference analyses revealed that enforcement efforts produce a negative effect on subsequent transactions on the policed site. This downward impact manifested in two ways, namely 1) reduced transaction levels, and 2) decreased number of vendors transacting on the site. Through our leads-lags model, we see that this effect increases in magnitude over time, and the transaction levels and vendor count do not recover to its pre-shock levels even after twenty weeks. A comparison of the coefficient magnitudes indicates that the the drop of market activity is not attributed to the removal of the arrested participants and is unlikely due to further arrests of active participants on SR2. Furthermore, we did not find evidence of migration behavior from the policed website to the other two alternative darknet sites during the study

period. We interpret these observations as an indication of a deterrent effect emanating from the enforcement efforts on a darknet site. We find that the observed effect is robust towards alternative modeling specifications and is unlikely arise due to coincidental effects. Further analyses show that the policing efforts on a darknet site can also lead to deterrent effects towards vendors from different prosecutorial jurisdiction. The extent of the deterrent effect is largely efficient at reducing the transacting activities of small-scale vendors and those who have a relatively short tenure on the site.

This study bears several theoretical and practical implications. Here, we discuss the finer theoretical possibilities and insights, along with the policy relevant guidelines of the study results. First, being one of the first studies to unveil a causal relationship between legal enforcement and darknet transactions, our study findings provide empirical validation to a question that bears multiple theoretical possibilities. Contrary to popular belief that enforcement is not effective, our study found that the police arrests of participants on a darknet site is capable of inducing a deterrent effect at least in the short-term horizon (i.e., half a year). This deterrent effect is not accompanied by substantial migratory behaviors from the policed site to the other two alternative sites within the same time period. This finding suggests that darknet markets may not be that different from other underground economy in terms of user reactions towards legal enforcement, wherein successful policing instances demonstrate that darknet sites are not infallible which would subsequently influence the decisions of existing participants to continue transacting on the site. However, we reiterate that our finding of the deterrent effect is short-term in nature, to which causal claims of long-term effectiveness needs to be evaluated by subsequent studies. Our finding serves as important inputs in informing practice, particularly enforcement agencies and policy makers. In light of the empirical evidence showing that darknet sites can be penetrated and effectively policed, enforcement agencies and policy makers should not shun attempts to crackdown these underground digital markets. Even if the policing does not lead to a long term suppression of darknet transactions, frequent crackdowns can prove to be helpful in halting the growth of these markets, given that short-term effectiveness of enforcement in deterring darknet transactions and the fact that alternative darknet platforms do need time to grow to critical

mass. That said, the successful enforcement of darknet sites does not come easily and is likely involve an extended amount of time before results can be observed, given the security and anonymization features makes it difficult to trace the identities of the perpetrators. Thus, more resource should be devoted towards the design of effective enforcement strategies and crackdown operations to keep darknet crimes in check. Initial insights on the profile of users that are more sensitive towards enforcement efforts uncovered in this work can serve as a starting point for the design of future enforcement strategies.

Second, on top of the broad relationship between enforcement and subsequent transactions, our study provides finer theoretical insights on why enforcement deters market participation on darknet markets. The news of the successful arrests of participants on SR2 serve as a counter-signal against the belief that darknet markets are guarded by foolproof security, thereby undermining the faith that market participants have towards their ability of avoiding apprehension and persecution. Having an updated belief on their arrest susceptibility, SR2 vendors would reconsider whether it is worth taking the risk of continuing their drug transaction in exchange for financial returns. Under a cost-benefit consideration, undertaking the risk of persecution over a small financial return is unlikely to be appealing to small scale vendors. Similarly, the costs of losing one's reputation and established set of buyers are relatively lower for vendors who have a shorter tenure on the darknet site. Thus, compared to their counterparts, small vendors and vendors with shorter tenure perceive the greater certainty of legal apprehension to be a larger cost relative to the payoffs they can get by maintaining their existing transacting levels. These reasons explain why them more sensitive to the policing effort. The finding of small vendors displaying the largest deterrence effect is in also line with the past criminology literature on the certainty of apprehension as a major factor explaining deterrence effectiveness (e.g., Apel and Nagin, 2010, Durlauf and Nagin, 2011, Nagin, 2013). In addition to validating the soundness of past theory, this finding also contributes to the understanding of the criminal mindsets of drug traffickers operating on this digital underground economy. In particular, we show that these perpetrators do behave rationally with respect to the risk of apprehension that evolve over time. In other

words, the theoretical possibility of darknet vendors having an over-confidence in evading enforcement efforts via the darknet security features is not supported in our assessment.

Third, our study uncovered an interesting nuance underlying the deterrence effect on darknet sites. In particular, we find that police arrests of darknet participants results in a successful deterrence effect, i.e., vendors do not migrate to alternative sites to continue transacting. This finding is worth discussing further, given the theoretical richness it adds to the understanding of how deterrence effects play out in the context of darknet markets. Darknet vendors are not only deterred by the possibility of apprehension on alternative sites but are also deterred by the possibility of being scammed by administrators of other darknet sites. Several administrators of darknet markets have executed exit scams by shutting down their sites and disappearing with the buyers' escrowed cryptocurrency (Woolf 2015). For instance, the administrators of the site, *Atlantis*, abruptly announced it would be going offline for "security" reasons, absconding with all the bitcoins that users had stored in their accounts. Similarly, the Silk Road alternative site, *Project Black Flag*, had disappeared with its administrator posting a message admitting that he or she had stolen the site's bitcoins. The anonymous and illicit nature of darknet markets prevent scammed users from taking remedial actions, making the risk of transacting at an alternative darknet site non-trivial. Vendors may have upheld their side of the transaction by sending the ordered drugs to buyers but may end up making huge losses should they fail to receive buyers' payment as a result of these darknet scams. The established line of ecommerce research further supports the view that existing users would have low intention of migrating to alternative darknet sites to transact, as it was found that the user's trust in a website is fundamental to spurring online purchase intentions and willingness to transact with other users on the website (Cyr 2008, Gefen 2000). In sum, vendors may not be better off in new marketplaces, should they choose to migrate. These reasons could explain why we are not seeing instances of migratory behavior in our study context.

Fourth, it is worthwhile discussing why deterrence effect is not limited by the prosecutorial jurisdiction of the enforcement agency. The extended scope of deterrence uncovered in our study could well be a unique characteristic of the policing agency involved. With the US FBI involved in the

investigation of the underground transactional activities at SR2, remaining users on the darknet platform were aware they were under the scrutiny of the world's most powerful law enforcement agency. The US FBI has a dedicated international operations team that had built relationships with principal law enforcement, intelligence and security services worldwide. As such, this enforcement agency is capable of prompt and continuous exchange of information with other international enforcement services and is in a position of soliciting the cooperation of global allies to apprehend international drug dealers that transact with the domestic US population.[17] Given the enforcement efficacy and prosecutorial reach of the US FBI, non-US vendors on SR2 may perceive an overwhelming amount of risk should they continue to transact on the policed site. We note that this extended scope of deterrence may not be observed in scenarios where the focal enforcement agency is not the US FBI.

Finally, the study makes a unique contribution to the literature on online platforms by taking the novel approach of examining whether online transactions might be disrupted with external regulations. Insights to this question differs starkly from that from the existing literature on platforms which has taken the opposite approach of addressing how transactions can be facilitated or enhanced on online marketplaces (e.g., Dellarocas, 2005; Dimoka et al. 2012, Gu and Zhu forthcoming, Overby and Forman 2015). In terms of conceptual insights, our findings reveal that when an external signal of risk is introduced to a well-functioning online platform, it can effectively upend users' willingness to make subsequent transactions on the site. This holds true even when the platform has protective features to shield its users from such risks, as seen in the case of the SR2 market. Interestingly, the immediate response of reducing transaction levels on the site (based on the coefficients of the leads-lags model) revealed that users are rather sensitive towards these risk signals. While past literature has shown the role of trust and how it can be built in online marketplaces (e.g., Lim et al. 2007; Pavlou and Gefen 2004), our work adds a new theoretical insight to this literature by showing that trust can diminish fairly quickly on online markets upon the receipt of

[17] See https://www.fbi.gov/about/leadership-and-structure/international-operations.

external risk signals, even in the face of established online measures and institutions that have been effective in protecting the users' interests in the past.

Limitations and Future Work

This study is not without limitations, some of which may pave the direction for future work on the study of enforcement effects of darknet sites. First, our work is based on the analysis of the policing effort on one darknet site, SR2. While the evidence provided in our work pertains to a large darknet platform, it is unclear if results would generalize to other darknet sites. It is possible that different darknet sites may have different security properties and that future darknet sites might come up with stronger security and anonymization innovations based on learnings of the failures met by the predecessor sites. Should such technological innovations improve substantially over time, deterrence effects as a result of greater perceived risk of apprehension might not apply to future sites. Thus, it would be worthwhile for future research to assess the impact of enforcement on newer darknet sites to ascertain if our uncovered results continue to hold.

Second, related to the first point, the policing effort in our empirical assessment is based off the US FBI, which is known to bear unique international presence in terms enforcement authority. As reasoned earlier, deterrence effects may not be similar if a different enforcement agency was leading the policing effort. Subsequent studies on the topic may wish to investigate this issue further. Finally, we have chosen Agora and Evolution as candidate darknet sites to which SR2 participants would migrate to, given that these are the largest and most popular darknet sites that co-existed with SR2 during the study period. One might argue that while there are no evidence indicating migratory patterns to these two alternative sites, SR2 participants might have gone to lesser known and smaller darknet sites to transact following the enforcement incident. While this is a possibility, it is extremely hard to evaluate empirically, given that data for these less known and obscure sites are not readily available given the existence of these platforms are unknown to researchers in the first place.[18]

[18] Even if the data on these lesser known sites are available, the data quality on their site activities are less trustworthy, as there are fewer concurrent academic verification of the data source.

That said, our work represents an initial effort of assessing and causally measuring the short-term impact of enforcement efforts on darknet activity and demonstrating whether affected darknet participants would migrate to alternative "well-known" darknet sites, under the assumption that darknet users are less willing to transact at smaller sites that do not have an established reputation and a sufficient pool of vendors and buyers to transact with. With the availability of better data, future studies could embark on an investigation to causally determine whether users from policed sites might move to smaller, lesser known darknet sites over longer periods of time.

REFERENCES

Abadie, A., 2005 Semiparametric difference-in-differences estimators. *Review of economic studies*, 72(1), pp. 1-19.

Apel, R., and D.S. Nagin. 2010. Deterrence. In crime, 4th edition, eds. James Q. Wilson and Joan Petersilia. Oxford, U.K.: Oxford University Press.

Autor, D.H., 2003. Outsourcing at will: The contribution of unjust dismissal doctrine to the growth of employment outsourcing. *Journal of labor economics*, 21(1), pp.1-42.

Babcock, Q. and Byrne, T., 2000. Student perceptions of methylphenidate abuse at a public liberal arts college. *Journal of American college health*, 49(3), pp.143-145.

Beccaria, C. 1986. *On crimes and punishment*. Indianapolis, IN: Hackett.

Benjamin, V., Valacich, J.S. and Chen, H., 2019. DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly*, 43(1).

Bentham, J. 1988. *The principles of morals and legislation*. Amherst, NY: Prometheus books.

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R., StExo, El Presidente, Anonymous, Lau, D., Sohhlz, Kratunov, D., Cakic, V., Van Buskirk, Whom, McKenna, M., Goode, S. "Dark Net Market archives, 2011–2015", 12 July 2015. Web.

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L. and Rossy, Q., 2017. A geographical analysis of trafficking on a popular darknet market. *Forensic science international*, 277, pp.88-102.

Brynjolfsson, E., Hu, Y. and Smith, M.D., 2003. Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers. *Management science*, 49(11), pp.1580-1596.

Burtch, G. and Chan, J., 2019. Investigating the relationship between medical crowdfunding and personal bankruptcy in the United States: Evidence of a digital divide. *MIS Quarterly,* 43(1), pp. 237-262.

Chan, J., and Ghose, A. 2014. Internet's Dirty Secret: Assessing the Impact of Online Intermediaries on HIV Transmission. *MIS Quarterly*, 38(4), pp. 955-976.

Chan, J., Ghose, A., and Seamans, R. 2016. The internet and racial hate crime: offline spillovers from online access, *MIS Quarterly*, 40(2), pp. 381-403.

Chan, J., Mojumder, P. and Ghose, A., 2019. The digital sin city: an empirical study of Craigslist's impact on prostitution trends. *Information systems research*, 30(1), pp.219-238.

Christin, N., and May. 2013. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In proceedings of the 22nd international conference on world wide web, pp. 213-224.

Cover, J.P. and Thistle, P.D., 1988. Time series, homicide, and the deterrent effect of capital punishment. *Southern economic journal*, pp.615-622.

Corbitt, B., Thanasankit, T., Yi, H., (2003). Trust and e-commerce: a study of consumer perceptions, *Electronic Commerce Research and Applications*, 2(3), pp. 203-215.

Cyr, D. (2008). Modeling Web Site Design across Cultures: Relationships to Trust, Satisfaction, and E-Loyalty. *Journal of Management Information Systems, 24*(4), 47-72.

Dellarocas, C. 2005. "Reputation Mechanism Design in Online Trading Environments with Pure Moral Hazard," *Information Systems Research*, 16(2), pp. 209-230.

Demant, J., Munksgaard, R. and Houborg, E., 2018. Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime*, 21(1), pp.42-61.

Dimoka, A., Hong, Y., and Pavlou, P. 2012. On Product Uncertainty in Online Markets. Theory and Evidence. *MIS Quarterly*, 36(2), pp. 395-426.

Dingledine, R., Mathewson, N., and Syverson, P. 2004. Tor: The second-generation onion router. In proceedings of the 13th USENIX security symposium, august 2004.

Dittus, Martin, Joss Wright, and Mark Graham., 2018. Platform criminalism: The last-mile geography of the darknet market supply chain. Proceedings of the 2018 World Wide Web conference on World Wide Web. International World Wide Web conferences steering committee.

Dolliver, D.S. and Kenney, J.L., 2016. Characteristics of drug vendors on the tor network: a cryptomarket comparison. *Victims & offenders*, 11(4), pp.600-620.

Durlauf, Steven N., and Daniel S. Nagin. 2011. Imprisonment and crime: Can both be reduced? *Criminology & Public Policy*, 10:13–54.

Ehrlich, I., 1975. The Deterrent Effect of Capital Punishment: A question of life and death. *American Economic Review*, 65(3), pp.397-417.

Eisenmann, T.R., Parker, G., and Van Alstyne, M. 2006. "Strategies for Two-Sided Markets," *Harvard Business Review*, 84(10), pp. 92–101.

Gefen, D. E-commerce: The role of familiarity and trust. *Omega*, 28(6), pp. 725-737.

Ghosh, S., Das, A., Porras, P., Yegneswaran, V. and Gehani, A., 2017, August. Automated categorization of onion sites for analyzing the darkweb ecosystem. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1793-1802).

Greenberg, A.2014. 'Silk road 2.0' launches, promising a resurrected black market for the dark web. https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/#46e6b6595714

Gu, G. and Zhu, F. (forthcoming). "Trust and Disintermediation: Evidence from an Online Freelance Marketplace." *Management Science*.

Hardy, R.A. and Norgaard, J.R., 2016. Reputation in the internet black market: an empirical and theoretical analysis of the deep web. *Journal of institutional economics*, 12(3), pp.515-539.

Hoenack, S.A. and Weiler, W.C., 1980. A structural model of murder behavior and the criminal justice system. *American Economic Review*, 70(3), pp.327-341.

Irrerra, A. 2019. Daily bitcoin transactions on darknet markets doubled throughout 2018: report. https://www.reuters.com/article/us-crypto-currencies/daily-bitcoin-transactions-on-darknet-markets-doubled-throughout-2018-report-idUSKCN1PC1OE

Kessler, D. and Levitt, S.D., 1999. Using sentence enhancements to distinguish between deterrence and incapacitation. *Journal of Law and Economics*, 42(S1), pp.343-364.

Kilmer, J.R., Hunt, S.B., Lee, C.M. and Neighbors, C., 2007. Marijuana use, risk perception, and consequences: Is perceived risk congruent with reality? *Addictive behaviors*, 32(12), pp.3026-3033.

Krijestorac, H., Garg, R., Mahajan, V., and Hofstede, F. (forthoming). Cross-Platform Spillover Effects in Consumption of Viral Content: A Quasi-Experimental Analysis Using Synthetic Controls. *Information Systems Research*.

Layson, S.K., 1985. Homicide and deterrence: A reexamination of the United States time-series evidence. *Southern Economic Journal*, pp.68-89.

Landsman, V., and Stremersch, S. 2011. Multihoming in two-sided markets: an empirical inquiry in the video game console industry, *Journal of Marketing*, 75(6), pp. 39-54.

Li, Z., Agarwal, A. 2017. Platform Integration and Demand Spillovers in Complementary Markets: Evidence from Facebook's Integration of Instagram. *Management Science*, 63(10):3438-3458.

Lim, K., Sia, C., Lee, M., and Benbasat, I. (2006). How Do I Trust You Online, and If So, Will I Buy?: An Empirical Study on Designing Web Contents to Develop Online Trust. *Journal of Management Information Systems*, 23(2), pp. 233-266.

Lin, M., Liu, Y., and Viswanathan, S. "Effectiveness of Reputation in Contracting for Customized Production: Evidence from Online Labor Markets". *Management Science*, 64 (1), pp. 345-359.

Lloyd, T. (2019). Exit Scam: Suspicion Grows Over Dark-Web Market's $30 Million Crypto Theft. Cryto-Currency News, April 23, 2019, https://www.ccn.com/exit-scam-ark-web-market-30-million-theft/, retrieved on Feb 29, 2020.

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

Nagin, D. S., Solow, R. M., & Lum, C. 2015. Deterrence, criminal opportunities, and police. https://onlinelibrary.wiley.com/doi/full/10.1111/1745-9125.12057#crim12057-bib-0004

Nagin, D.S., 1998. Criminal deterrence research at the outset of the twenty-first century. *Crime and justice*, 23, pp.1-42.

Nakamoto, S. 2008. Bitcoin: a peer-to-peer electronic cash system.

Norgaard, J.R., Walbert, H.J. and Hardy, R.A., 2018. Shadow markets and hierarchies: comparing and modeling networks in the Dark Net. *Journal of Institutional Economics*, 14(5), pp.877-899.

Overby, E. and Forman, C., 2014. The effect of electronic commerce on geographic purchasing patterns and price dispersion. *Management Science*, 61(2), pp.431-453.

Parker, G., and van Alstyne, M., 2005. Two-sided network effects: a theory of information product design. *Management Science*, 51(10), pp.1494-1504.

Pavlou, P. and Gefen, D. 2004. Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, 15(1), pp. 37-59.

Patton, M.A. and Jøsang, A., 2004. Technologies for trust in electronic commerce. *Electronic Commerce Research*, 4(1-2), pp.9-21.

Popper, N. June 11 2019. Dark web drug sellers dodge police crackdowns. New York Times.

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q. and Esseiva, P., 2016. Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic science international*, 267, pp.173-182.

Rysman, Marc. 2009. The economics of two-sided markets. *Journal of economic perspectives*, 23 (3), pp.125-43.

Seamans, R., and Zhu, F. 2014. Responses to entry in multi-sided markets: the impact of Craigslist on local newspapers, *Management Science*, 60(2), 476-493.

Silberman, M., 1976. Toward a theory of criminal deterrence. American Sociological Review, pp.442-461.

Song, P., Xue, L., Rai, R., and Zhang, C. 2018. The ecosystem of software platform: A study of asymmetric cross-side network effects and platform governance. *MIS Quarterly*, 42(1), pp. 121-142.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S. and Roxburgh, A., 2017. The recovery of online drug markets following law enforcement and other disruptions. *Drug and alcohol dependence*, 173, pp.159-162.

Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E., Sindicich, N., Matthews, A., Butler, K. and Burns, L., 2016. Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. *International Journal of Drug Policy*, 35, pp.32-37.

Weber, B.S., 2019. Uber and urban crime. Transportation research part A: policy and practice. Available at: https://www.sciencedirect.com/science/article/pii/S0965856418311418 [Accessed December 6, 2019].

Wen, W. and Zhu, F. 2019. Threat of Platform-Owner Entry and Complementor Responses: Evidence from the Mobile App Market. *Strategic Management Journal* 40(9), 1336-1367.

Woolf, N. 2015, March 18. Bitcoin 'exit scam': deep-web market operators disappear with $12m. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars

Xu, Y., 2017. Generalized synthetic control method: Causal inference with interactive fixed effects models. *Political Analysis*, 25(1), pp.57-76.

Zervas, G., Proserpio, D., and Byers, J. 2017. The rise of the sharing economy: estimating the impact of Airbnb on the hotel industry. *Journal of marketing research*, 54(5), pp. 687-705.

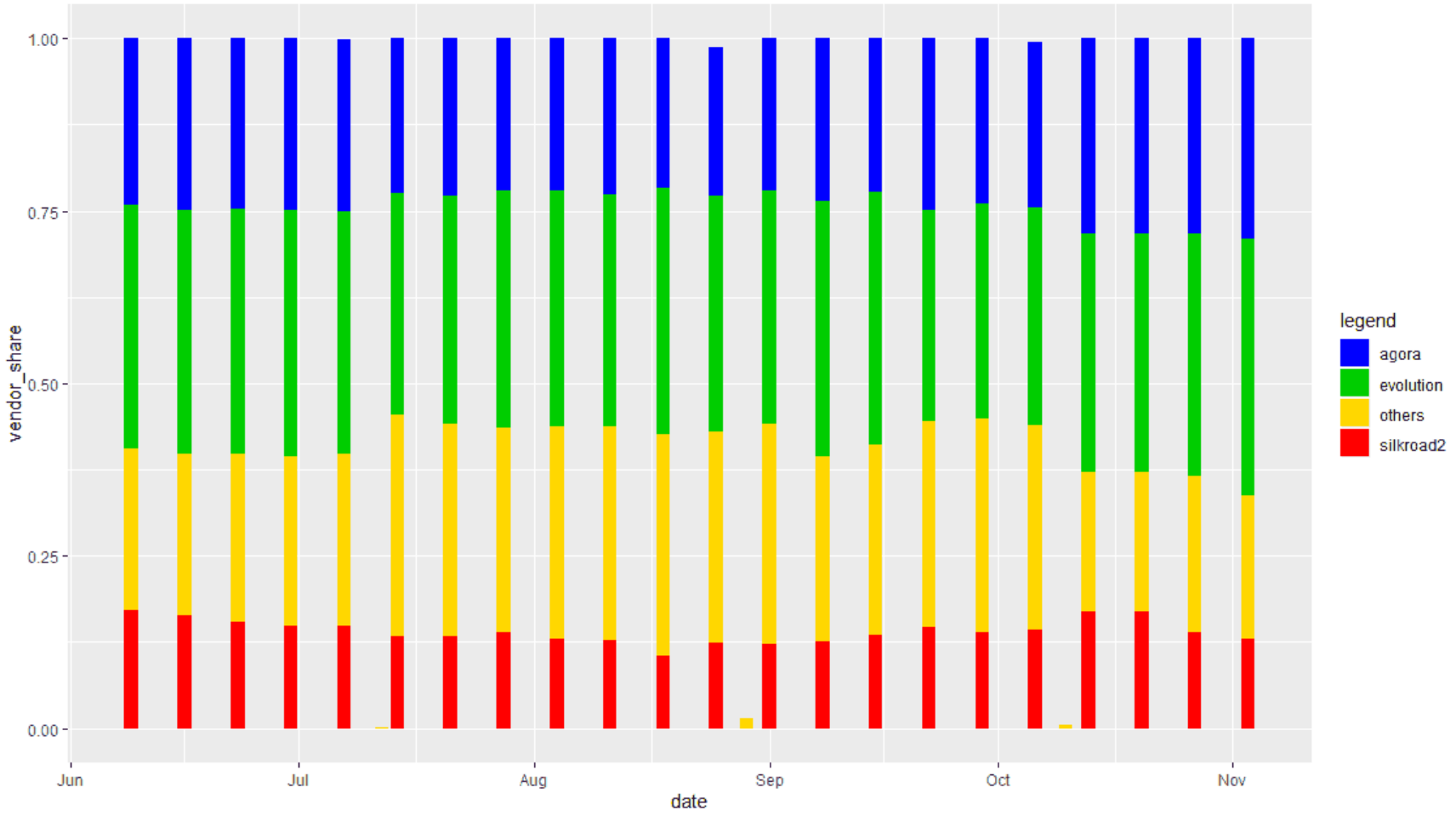
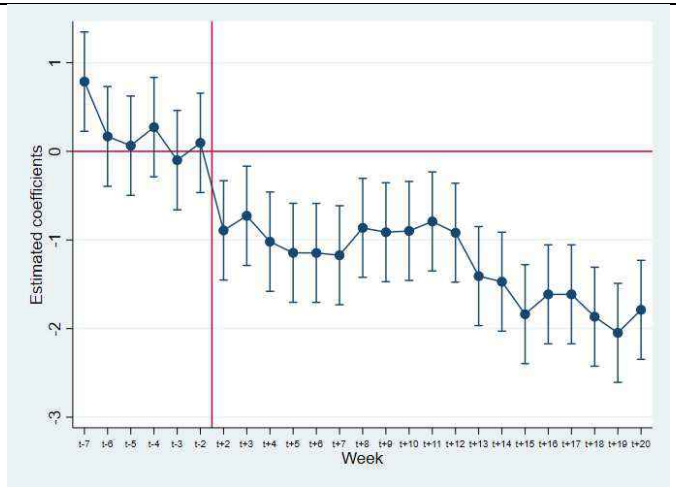
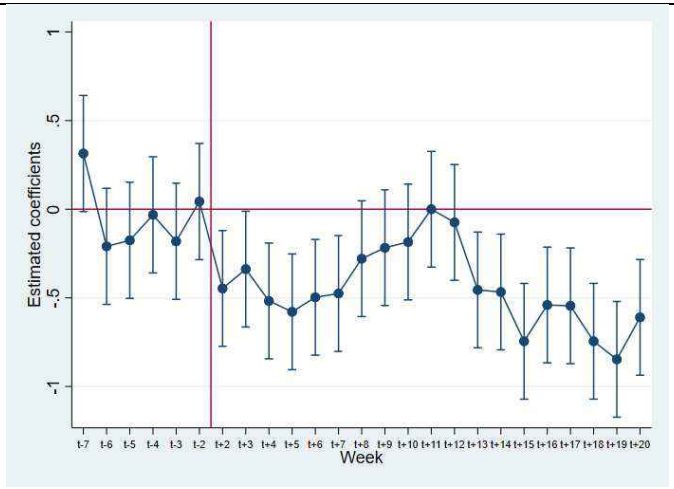


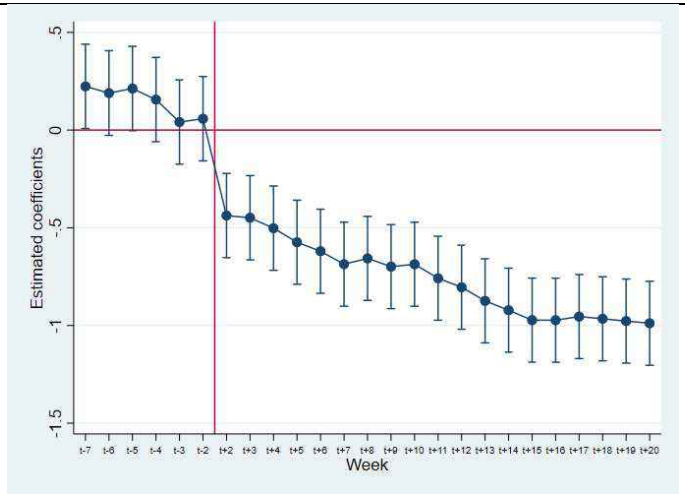
Figure 1: Vendor Share of Darknet Market



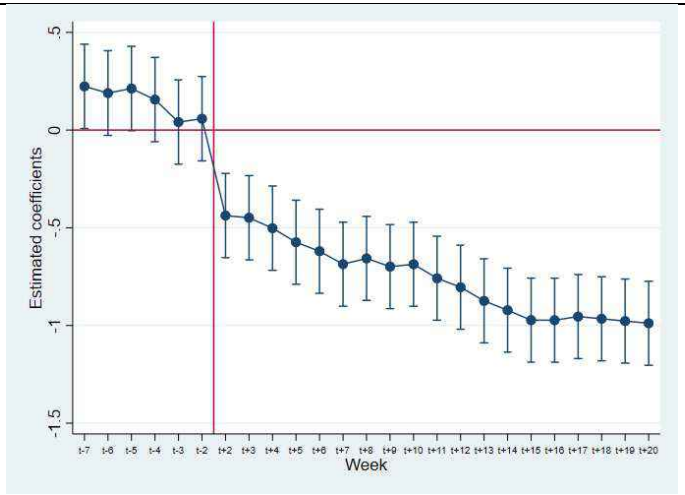
(a) Total review



(b) Avg review per vendor



(c) Number of vendors with active transaction each week



(d) Number of Remaining vendors

Figure 2 Parallel trend test of treatment effects on Silkroad2

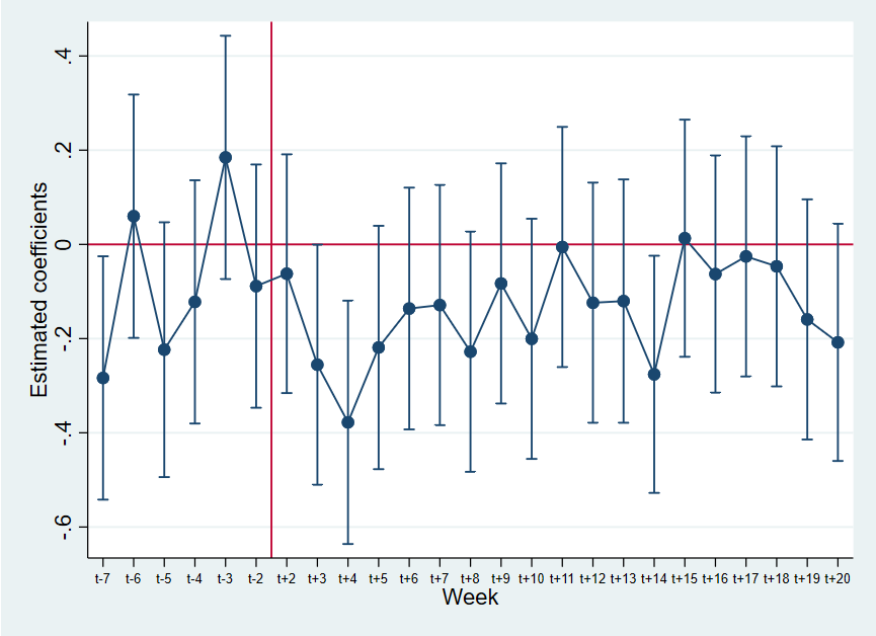


Figure 3 Number of new vendors on Agora and Evolution over time

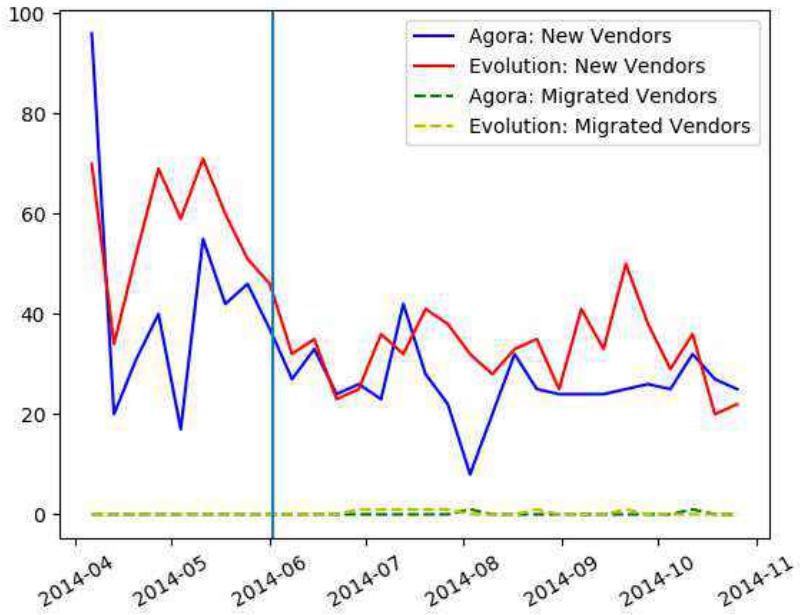
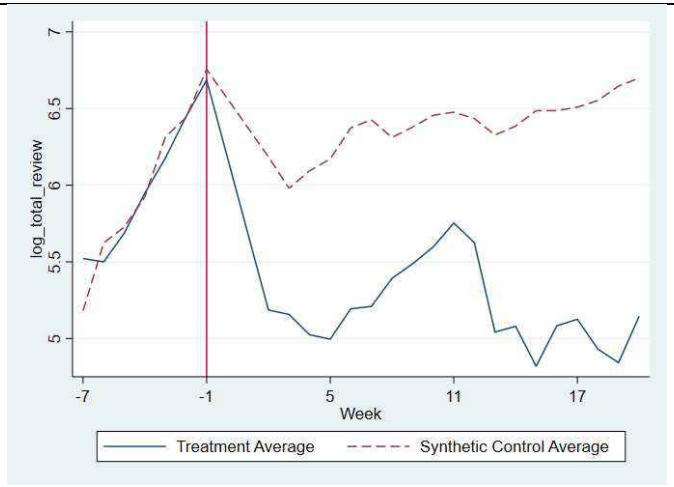
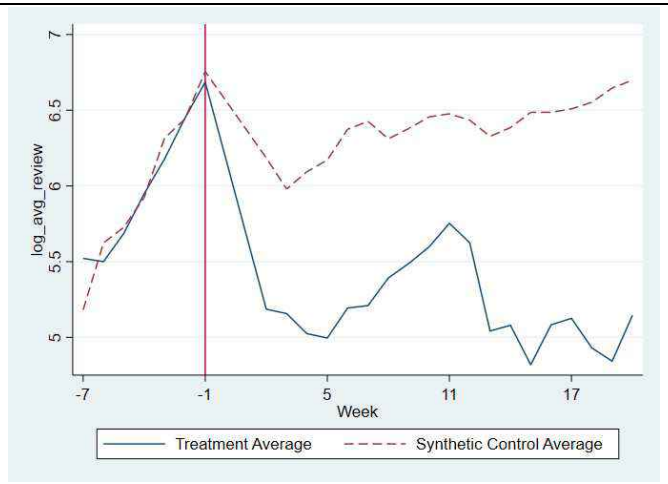


Figure 4: Number of new vendors on Agora and Evolution with the same username as Silkroad2 vendors, before and after the policing event

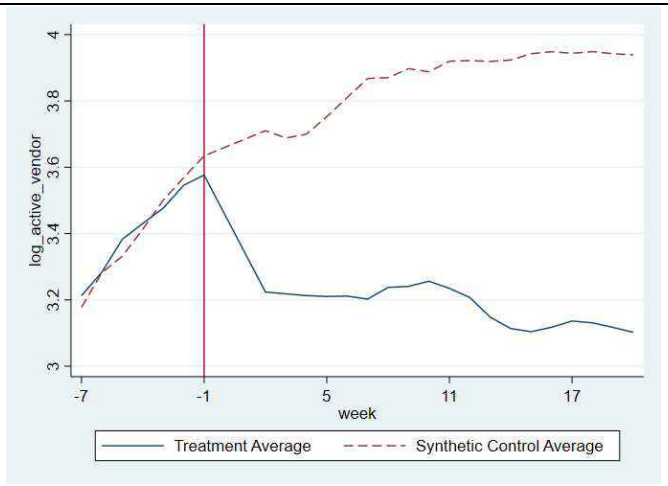
Note: The dotted lines indicate the number of new vendors with same username as that on SR2, the solid lines indicate the number of new vendors joining the two control sites.



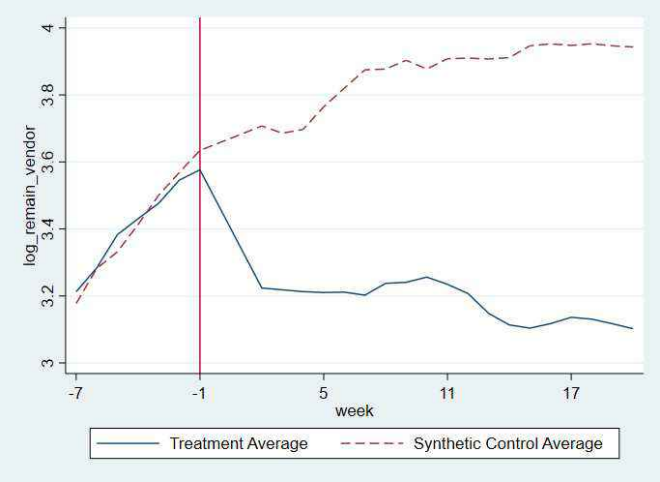
(A) Total review



(B) Avg review per vendor



(C) Number of vendors with active transactions each week



(D) Number of remaining vendors

Figure 5: Treatment effects on US vendors on Silkroad2 using the Synthetic Control Method

Table 1 Summary statistics

Variable	Obs	Mean	Std. Dev.	Min	Max
US vendors on Silkroad2					
Total review	338	415.216	468.616	2	3850
Avg review	338	12.990	13.974	0.667	141.429
Vendor level review	6,494	21.611	43.241	0	854
Unique vendor	338	35.683	28.336	2	109
After	338	0.731	0.444	0	1
Week	338	81.962	8.214	68	95
Drug type	338	7	3.747	1	13
Non-US vendors on Silkroad2					
Total review	338	1206.787	1117.216	44	8376
Avg review	338	14.587	7.296	2.664	43.853
Vendor level review	10,965	37.200	82.704	0	1,329
Unique vendor	338	77.944	44.324	16	191
After	338	0.731	0.444	0	1
Week	338	81.962	8.214	68	95
Drug type	338	7	3.747	1	13
Non-US vendors on Agora and Evolution					
Total review	613	207.620	284.217	0	1954
Avg review	613	3.997	3.006	0	19.677
Vendor level review	20,245	8.840	19.879	0	643
Unique vendor	613	40.662	36.103	1	179
After	613	0.739	0.440	0	1
Week	613	82.127	8.172	68	95
Drug type	613	7.130	3.874	1	14

Table 2: The Impacts of Policing on US vendors' Transactions on Silkroad2

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.454***	-0.449**	-0.889***	-0.889***	-0.859***
	(0.292)	(0.181)	(0.115)	(0.115)	(0.096)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	951	951	951	951	26,739
R-squared	0.433	0.373	0.352	0.571	0.122

Table 3: Robustness check with randomly selected treated vendors

	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count
Number of iterations	10000	10000	10000	10000
Mean	0.000921	0.000483	0.000435	0.0000447
S.D.	0.095	0.066	0.051	0.008
H0: Mean = 0	0.966	0.729	0.854	0.578
P value	0.334	0.466	0.393	0.563

Table 4: Comparisons between treated and control vendors using T-test and Kolmogorov–Smirnov test

VARIABLES	Difference	t-test	Kolmogorov–Smirnov test
No. of reviews	-0.002	-0.011	1.000
Dollar sales amount	-0.041	-0.177	0.867
Unique drugs transacted	0.146	1.281	0.486
Drug categories transacted	0	1.000	1.000
Vendor's tenure on site	-1.050	-0.182	0.253
No. weeks with active transactions	0.014	0.020	1.000
No. of matched pairs	140	140	140

Table 5: Robustness check using CEM matched vendors

	Site level				**Vendor level**
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-0.897***	-0.596*	-0.472***	-0.196**	-0.643***
	(0.315)	(0.311)	(0.0990)	(0.0905)	(0.203)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug type FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	896	896	896	896	4,606
R-squared	0.254	0.154	0.399	0.469	0.146

Table 6: Robustness Check Using Synthetic Control

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.454***	-0.449**	-0.889***	-0.889***	-0.935***
	(0.206)	(0.102)	(0.086)	(0.086)	(0.041)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	951	951	951	951	1,803

Table 7: The impacts of arrest news disclosures on Silkroad2 using Negative Binomial Model

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.192***	-0.356*	-0.860***	-0.748***	-0.777***
	(0.262)	(0.207)	(0.101)	(0.0905)	(0.102)
Week FE	Yes	Yes	Yes	Yes	Yes
Website FE	Yes	Yes	Yes	Yes	
Drug type FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	951	951	951	951	26,486
Number of vendors					1,737

Table 8: The Impacts of Policing on US vendors' Transactions on Silkroad2 based on Two Characters

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.424***	-0.437**	-0.877***	-0.673***	-0.872***
	(0.294)	(0.177)	(0.125)	(0.090)	(0.098)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	951	951	951	951	23,726
R-squared	0.422	0.363	0.356	0.514	0.125

Table 9 The impacts of arrest news disclosures without "worldwide" control vendors

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.525***	-0.465**	-0.920***	-0.920***	-0.806***
	(0.318)	(0.188)	(0.127)	(0.127)	(0.0969)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug type FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	937	937	937	937	24,531
R-squared	0.353	0.278	0.533	0.533	0.133
Number of website and drug	37	37	37	37	
Number of vendors					1,688

Table 10 The impacts of arrest news disclosures on non-US vendors' transactions on Silkroad2

	Site level				Vendor level
	(1) Total review count	(2) Avg review per vendor	(3) Count of vendors w active transactions	(4) Remaining vendor count	(5) Total review count
Policing Effort	-1.187***	-0.291*	-0.816***	-0.816***	-0.655***
	(0.277)	(0.149)	(0.113)	(0.113)	(0.0825)
Week FE	Yes	Yes	Yes	Yes	Yes
Drug type FE	Yes	Yes	Yes	Yes	
Website FE	Yes	Yes	Yes	Yes	
Vendor FE					Yes
Observations	951	951	951	951	31,210
R-squared	0.379	0.304	0.591	0.591	0.120
Number of website and drug	37	37	37	37	
Number of vendors					2,167

Table 11 The heterogeneous treatment effects on large and small vendors

	US vendors			Non-US vendors		
	Small vendors	Large vendors	All	Small vendors	Large vendors	All
Policing Effort	-1.098***	-0.366***	-0.351***	-1.069***	-0.303***	-0.289***
	(0.130)	(0.0784)	(0.0755)	(0.147)	(0.0721)	(0.0691)
Policing Effort *Small Vendor			-0.881***			-0.882***
			(0.106)			(0.106)
Weekly FE	Yes	Yes	Yes	Yes	Yes	Yes
Drug type FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	853	922	1,775	882	922	1,804
R-squared	0.570	0.305	0.617	0.567	0.272	0.625
Number of drug types	36	36	36	36	36	36

Table 12 The heterogeneous treatment effects on old and new vendors

	US vendors			Non-US vendors		
	New vendors	Old vendors	All	New vendors	Old vendors	All
Policing Effort	-1.230***	-0.212***	-0.284***	-1.095***	-0.213***	-0.203***
	(0.113)	(0.0756)	(0.127)	(0.119)	(0.0702)	(0.121)
Policing Effort *New Vendor			-0.883***			-0.878***
			(0.0904)			(0.0906)
Weekly FE	Yes	Yes	Yes	Yes	Yes	Yes
Drug type FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	854	920	1,774	882	922	1,788
R-squared	0.593	0.219	0.527	0.567	0.272	0.578
Number of drug types	36	36	36	36	36	36

APPENDIX

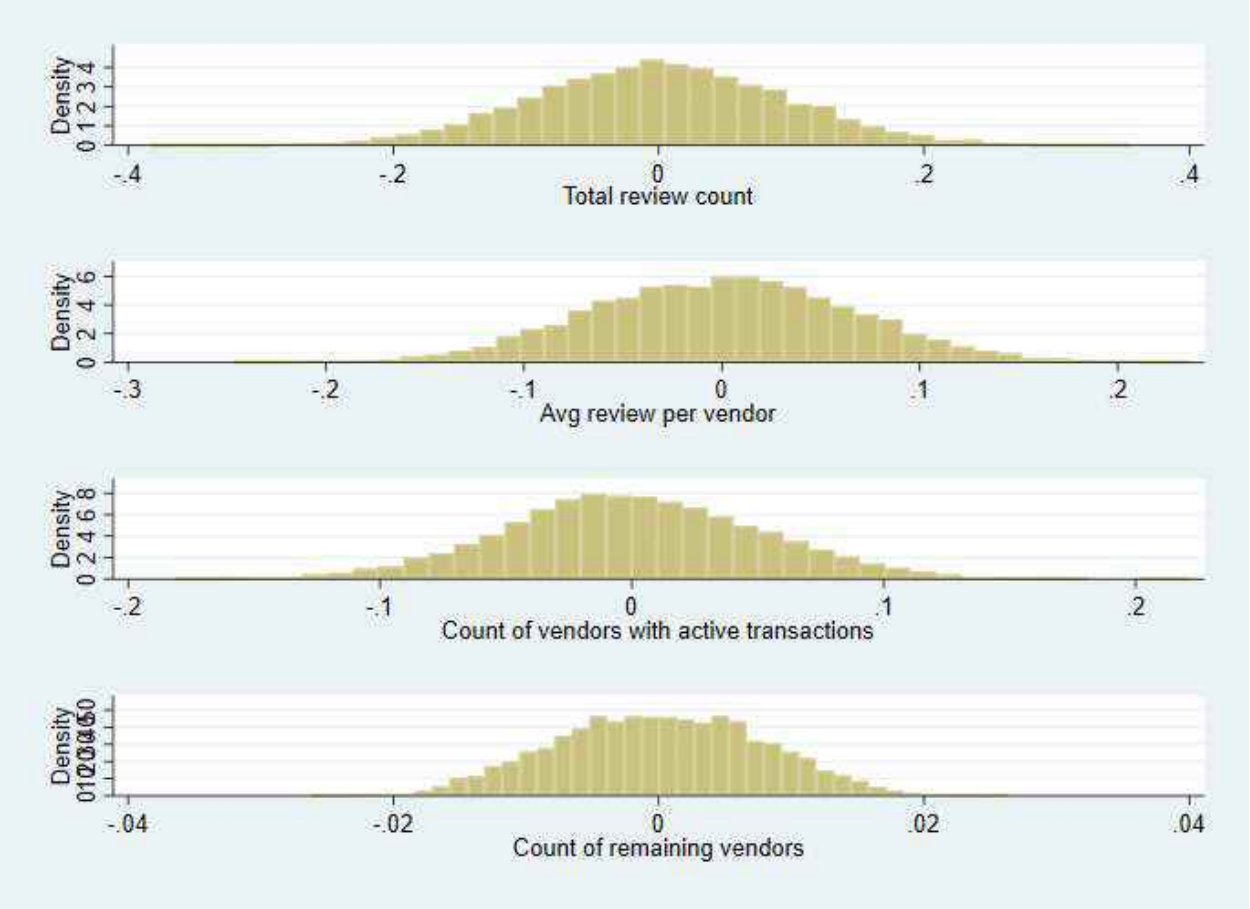


Figure A1: Estimated treatment effects based on 10,000 simulations