

THE 21st CENTURY'S SILK ROAD

Introduction

While political revolution has been largely responsible for the tearing down of physical barriers to trade, the technological revolution has done even more to connect buyers and sellers. The Internet has broadened the horizons of buyers and sellers across the world: a one-time international transaction that once seemed unprofitable, impossible, and inefficient can now be completed with a click of the mouse. The Internet puts consumers in control of purchasing with an unprecedented ability to “shop around” and compare costs. The Internet also empowers smaller entrepreneurs and providers with an ability to expose and promote their goods and services to wider audiences. However, just as trade liberalization has benefited both licit and illicit sales across the globe, so too has the Internet facilitated unseemly and nefarious activities. For example, one only need open his or her email “spam” folder to see countless offers for prescription drugs or search “legitimate” online marketplaces such as eBay to find counterfeit goods or stolen items.¹ But, beyond the traditional Internet user’s encounter with illicit sales of legal or illegal goods, there is another online world altogether: the “Dark.” It is within this “dark” world that some of the seediest transactions take place.²

The anonymity offered by the Darknet is attractive to buyers and sellers of illicit goods, which is why several online marketplaces take advantage of it. Among these sites is “Silk Road,”

¹ eBay has terms of service banning the sale of counterfeit and stolen products (eBay 2013).

² There are three levels of the “Dark.” First is the “dark internet,” which is hosted on the “conventional internet,” but it “appears to be unreachable using conventional online means”; second is the “dark web,” also known as the “deep web,” wherein servers cannot be located “using any regular search engines such as Google”; and the third is “darknet,” perhaps the deepest level of the Internet, and it is used “to covertly communicate, swap information and undertake commerce online” (Everett 2009). Information on the “darknet” is sent through peer-to-peer networks and is encrypted and broken up so that the original sender is completely anonymous to the end-user (Everett 2009).

which was created in February 2011 and has received considerable attention the past couple of years because of its reliance on Bitcoins, a virtual currency (Christin 2012). While “licit” goods are for sale, the site has gained notoriety for its services offered to drug users and dealers. Silk Road is not a drug vendor in and of itself, but provides a “bazaar” like eBay or Craigslist in order to connect those who wish to sell and those who wish to buy. And, like eBay’s PayPal service, but unlike craigslist, it facilitates the exchange of funds. This paper will explore the history of Silk Road, the technological tools it utilizes, its size, and the challenges and opportunities associated with policing Silk Road.

Silk Road: How It Works

Before understanding the Silk Road, it is important to understand the platforms on which it relies – the network and software known as “Tor” and the currency known as “Bitcoin.”

Tor: Silk Road’s website is inaccessible to those not operating with Tor, an anonymising software and network that was created and ultimately released by the U.S. and Swedish governments in 2001 (Koul 2012). As its website explains, Tor, created at the U.S. Naval Research Laboratory, has a number of legitimate uses, including, but not limited to: providing Internet browsing privacy; offering journalists a platform through which to talk with whistleblowers and non-government organizations ways to communicate with on-the-ground workers; and, providing secrecy for governments’ communication (Tor 2013). Tor works by providing multiple levels of encryption through a “distributed, anonymous network” utilizing indirect and random methods of data transmission. Individuals volunteer to be a “node” on the network, and traffic routes through at least three different nodes before reaching the recipient (Tor 2013). As of December 2012, there were 3,200 volunteer nodes, but the uptick in interest –

especially in the U.S. and Europe due to growing concerns about Internet privacy – to about 600,000 users means Tor needs about 7,000 more volunteer nodes (Fowler 2012).

Bitcoins: All Silk Road transactions occur exclusively utilizing a digital currency known as “Bitcoin.” Sellers must purchase goods only in Bitcoins, and all buyers must accept the currency. The virtual currency was developed in 2009 by Satoshi Nakamoto³ who professed frustration with the financial meltdown of the early 2000s and a desire to utilize a currency immune from the “predations of bankers and politicians” (Davis 2011). As a means of controlling the currency and of providing users with some stability and expectations as to inflation, Bitcoins are released in a regular, predictable pattern: “50 every 10 minutes, with the pace halving in increments until around 2140” (Wallace 2011).

People who wish to purchase goods or obtain services with Bitcoins can obtain the virtual currency by “mining” which means to “[lend] their computers’ resources to service the needs of the Bitcoin network” (Surowiecki 2011). In the Bitcoin world, a coin symbolizes a “chain of digital signatures” (Nakamoto 2008). Fraud is supposed to be avoided through the maintenance of a public ledger, and Bitcoins are stored in digital “wallets.” A number of exchanges and services to protect currencies from hacking have been established by third parties; as a result, concerns have been raised because of the creation of a “primitive and unregulated financial services industry...to safeguard clients’ digital assets” (Wallace 2011).

Despite the predictable pattern of Bitcoin release, public interest in Bitcoin has led to wild speculation of the currency. Since the currency’s inception, there have been a handful of spikes in the value of Bitcoin, each associated with media attention, as explained in a September 2012 article in *The Economist*:

³ Many sources read for this paper suggest this is not a real person. See Wallace (2011).

“Shortly after the currency launched, articles spread around the internet arguing that Bitcoins would protect wealth from hyperinflation and that early adopters would make a fortune. The dollar price of a Bitcoin currency unit climbed from a few cents in 2010 to a peak of nearly \$30 in June 2011...according to data compiled by Mt Gox, a popular online Bitcoin exchange. Inevitably, the currency then crashed back down, bottoming out at \$2 in November 2011. But in the nine months since, Bitcoin has recovered.”

More recently, a banking crisis in Cyprus caused the value of Bitcoin to skyrocket over a matter of days. On March 16, 2013, the currency closed at \$47.00 on the Mt Gox exchange; a month later, on April 6, 2013, it closed at \$63.36, but, in the meantime, it reached a peak of \$230.00 on April 9, 2013 (Bitcoin Charts n.d.).

Although the legality of Bitcoin has not been tested (Bitcoin 2011), lawmakers – including New York Senator Chuck Schumer, who called for Silk Road to be shut down (Slattery 2011) and subsequently criticized the currency by deeming it “money laundering” (Wallace 2011). His accusation is likely grounded in a user’s ability to convert to and from Bitcoins without leaving any record and conduct untraceable transactions.⁴ In other words, it abridges the abilities of regulators and law enforcement to track and trace the currency. There is no way for the eyes and ears of government to perform the “due diligence” typically expected of central and commercial banks when facilitating currency exchanges and transactions. Furthermore, many legal experts say that Bitcoin operates in a “gray area” because transactions happen beyond the scopes of domestic and international law (Sanati 2012).

Silk Road: Once a user is equipped with Tor and a stash of Bitcoins, he is ready to engage in a transaction. As explained by Nicolas Christin of Carnegie Mellon University, who has done the most extensive research on the site, a user creates an account to access the lists of

⁴ This may not be the only reason Senator Schumer criticized Bitcoin. He represents the State of New York, home to Wall Street, and since 1989, has received nearly \$10 million in campaign contributions from the securities and investment industry and more than \$1 million from commercial banks; these entities are threatened by the existence of a virtual currency (see later in this paper for a discussion about the European Central Bank branding virtual currencies as “schemes”). (OpenSecrets.org)

items for sale. Once the user is ready to purchase, the seller is notified, and the buyer starts the transaction by providing his Bitcoins to Silk Road. Silk Road then holds the funds in escrow so that commission fees can be determined and the transaction can be finalized. If the transaction circumvents this escrow system, users can be banished from the marketplace. The seller ships the item (it is recommended that the products be shipped to a third-party address – or at least one untraceable to the buyer), and upon the buyer receiving it and informing Silk Road, the funds are released to the seller. The system stores no information about addresses. Users are expected to rate the transaction. (Christin 2012)

How Big is the Silk Road?

Christin's study gathered and analyzed data over the course of eight months in 2011 and 2012. His key findings indicate that Silk Road is made up of many small-time buyers who purchase from small-time sellers. His research during this limited time frame led to insights that:

- Buyers and sellers engage in roughly \$1.2 million in transactions every month; this equates to about \$15 million every year;
- There are relatively few sellers (1,239 in six months) and each enjoys relatively small market share (no more than 1.5% of the products are sold by any one user), and they sell their goods to an estimated 30,000-150,000 customers;
- There are 220 distinct categories with marijuana, other drugs, and prescriptions rounding out the top slots (13.7%, 9%, and 7.3% of all listings, respectively).
- The majority of goods are sold within three weeks, and a quarter of goods are gone in three days;

- The website operators make money through a tiered commission scale: 10% on the first \$50; 8.0% on \$50.01-\$150; 6% on \$150.01 to \$300; 3.0% on \$300.01-\$500; 2% on \$500.01-\$1000 and 1.5% on \$1000+;
- According to Christin’s screenshots of the Silk Road website, the top product categories sold on Silk Road are weed (13.7%), drugs (9%), prescriptions (7.3%), benzos (4.9%), books (3.9%), cannibas (3.6%), hash (3.4%), and cocaine (2.6%). All other goods account for less than 2 percent of total sales. In other words, there is no concentration of products dominating the site’s offerings.

The aforementioned data demonstrate that the Silk Road represents just a fraction of the overall global drug trade (which is estimated to be approximately \$330 billion annually (Count the Costs 2012)). Further, the sellers and buyers represent just another small fraction of the overall estimated 230 million individuals who use an illegal drug at least once per year (United Nations Office on Drugs and Crime 2012, 59). Those who support legalization of some or all types of drugs (or even those who believe government should maximize its “bang for the buck” when it comes to law enforcement) would likely argue that, given Silk Road’s minimal influence and size, it is not worth dumping large sums of money into investigating and prosecuting this small operation; the costs would likely exceed the sales (although with such calculations it would be important to take into account any externality costs as well).

Despite the volatility of Bitcoin over the past few months, traffic on Silk Road has not suffered. According to the site’s founder, the “Dread Pirate Roberts” (DPR), who sent a public statement to *Forbes* writer Andy Greenberg, “a rapidly changing price does have some effect, but it’s not as big as you might think” (Greenberg, Founder Of Drug Site Silk Road Says Bitcoin

Booms And Busts Won't Kill His Black Market 2013). Silk Road may not have felt the effects because, as it was been pointed out by Greenberg, there are two types of people who use Bitcoins: those who purchase goods with them (as Silk Road users do) and those who speculate, seeing the virtual currency as an investment opportunity (and “hoard” them until there is money to be made). Therefore, the currency is always moving. There is an incentive for drug users to spend the Bitcoins quickly because when the value goes up, the amount of drugs they can purchase goes down. Greenberg explained:

“Silk Road has built-in protections against Bitcoin’s spikes and crashes. Although purchases on Silk Road can only be made with Bitcoin, sellers on the site have the option to peg their prices to the dollar, automatically adjusting them based on Bitcoin’s current exchange rate as defined by the central Bitcoin exchange Mt. Gox. To insulate those sellers against Bitcoin fluctuations, the eBay-like drug site also offers a hedging service. Sales are held in escrow until buyers receive their orders via mail, and vendors are given the choice to turn on a setting that pegs the escrow’s value to the dollar, with Silk Road itself covering any losses or taking any gains from Bitcoin’s swings in value that occur while the drugs are in transit. So while Bitcoin’s crash last week from \$237 to less than \$100 means that the Dread Pirate Roberts was likely forced to pay out much of the extra gains Silk Road made from Bitcoin’s rise, most of his sellers were protected from those price changes and continued to trade their drugs for Bitcoins despite the currency’s plummeting value.” (Ibid.)

What about the Online Drug Market?

As mentioned earlier, the drug market yields approximately \$320-\$330 billion per year in profits (General Assembly of the United Nations 2012), and only a fraction of it happens online (and an even smaller fraction on Silk Road). However, as with the trade in licit goods, the Internet has opened additional opportunities for traders and traffickers to offer competitive pricing (by being able to research the costs in other markets) and to obtain and share knowledge about new products (United Nations Office on Drugs and Crime 2012, 85). Nevertheless, just as the Internet has provided new avenues for those in the drug business, it has also empowered law

enforcement to “monitor the illicit drug market and the criminals’ planning and operations... [and] to cooperate closely across borders” (United Nations Office on Drugs and Crime 2012, 85).

What Are Possible Intervention Points for the Silk Road?

To date, only one person, an Australian, is believed to have been convicted for using Silk Road (Solon 2013). How should domestic and international lawmakers cope with Silk Road, if at all? Nicholas Cristin outlined a number of “potential intervention strategies” to tackle Silk Road. Among them are “disrupting the network, disrupting the financial infrastructure, disrupting the delivery model, and laissez-faire” (Christin 2012).

In terms of **dismantling the network**, regulators would have to intervene to disrupt Tor – which, somewhat ironically, is a product created by the U.S. government. Certainly (or at least hopefully) the U.S. government would possess the knowledge of how to dismantle Tor, but there would be far-reaching ramifications for doing so. Not only are there legitimate uses for Tor – as mentioned earlier, regular users utilize Tor for privacy, and governments also rely on it to communicate with covert workers and foreign dissidents and to communicate within – but given the pushback by Internet privacy advocates in recent policy fights⁵, there is likely to be political ramifications for lawmakers who allow bureaucrats to take Internet control to a new level.

Although Silk Road is perhaps the most prominent of sites for illicit transactions, it is not alone. In April 2012, the U.S. Drug Enforcement Administration (DEA) broke up “The Farmer’s Market,” an online site similar to – but not exactly like – Silk Road. According to a release from DEA after the arrest of six Americans in the U.S., one American in Buenos Aires, and one Dutch

⁵ Villasenor, Monk and Bronk (2011) argue “As the recent struggle to pass a House of Representatives bill that would have required Internet service providers to store certain types of information 18 months shows, there are highly divergent views in the legislative and broader community on how to achieve the proper balance between preserving privacy and preventing criminal activity.”

citizen in the Netherlands, the site provided goods to more than 3,000 customers in every single U.S. state as well as in 34 countries (States News Service 2012). The investigation took two years, and two of the accused handled more than 5,000 transactions of approximately \$1.04 million (ibid.). Like Silk Road, The Farmer's Market operated on the Tor network. Unlike Silk Road, however, sellers and buyers on The Farmer's Market utilized traditional money exchanges (including Western Union) to process and accept payments. This likely facilitated the ability to develop a case against the site's users and actually find them as well.

In May 2013, it was reported that "Silk Road has reportedly come under repeated denial-of-service attacks, which involve overloading a site with web traffic" (Munroe 2013). While some believed these to be the work of governments attempting to dismantle and disrupt the network, there are others who believe that these attacks offer the "possibility of a virtual turf war in the growing online market for illicit drugs" (ibid.).

It is often suggested that "following the money" is the best way to disrupt illicit trade. Certainly the indictments against The Farmer's Market could not have been issued without tracking the money that flowed through Western Union and other "above-ground" channels. Christin has suggested **tackling the financial infrastructure**, which would mean taking on the elements that allow buyers and sellers to exchange compensation for the goods sold and acquired; this would include the currency or the infrastructure.

First, taking a step back and addressing the financial infrastructure of Internet transactions, fellows and researchers at the Center for Technology Innovation at Brookings and the James A. Baker III Institute for Public Policy at Rice University published a paper in August 2011 in which they outline possible ways to detect, monitor, and ultimately limit and prosecute online illicit financial transactions. Their basket of "solutions" include "self-regulation,

government-industry collaboration, and change in both technology and culture within government agencies” (Villasenor, Monk and Bronk 2011, 4). Specifically, they recommend that private sector entities – including both mobile money transfer platforms and internet service providers alongside banks and governments – establish collaborative efforts to track the flow of money. Additionally, they offer the age-old suggestion that agencies within government work together to “focus specifically on emerging financial threats” and that they “maintain an understanding of the novel methods being used to move money” (2011, 17). In terms of technology, these authors also suggest the adoption of “information processing methods that can appropriately detect and trace illicit financial transactions...[relying on] methods for anonymising customer data to allow analysis while simultaneously preserving privacy in more traditional consumer Internet applications” (2011, 19). The problem with these solutions is that these private sector entities operate in the licit realm; certainly the tactics may be applicable to catching and deterring illicit transactions, but they have no incentive to combat the illicit product trade when it does not compete with their own goods and services.

The only accepted currency on Silk Road is Bitcoin; so, either Bitcoin specifically has to disappear, or the law has to catch up with the existence of virtual currency. In sum, it operates and exists in a vacuum. And, as is often the case, a vacuum is seen as an opportunity by lawmakers as a void to fill. The legality of Bitcoin remains largely untested (Cohn 2011).

Beyond the use of Bitcoins to finance the purchase of illicit goods, there is some concern about Bitcoins being used to facilitate money laundering or to finance criminal activity. The European Central Bank issued a report in October 2012 – “Virtual Currency Schemes” – in which the lack of regulation was presented as an opportunity for enterprising criminals, particularly when the virtual currency scheme enabled “bidirectional flows” (European Central

Bank 2012, 44).⁶ Although the report did provide this brief mention of criminal and illicit activity, it was more focused on the threats to normal finance – including determining the role for central banks to regulate and the impacts on price and financial stability. Notably, this report argued that these virtual currencies “could have a negative impact on the reputation of central banks, assuming the use of such systems grows considerably...since the public may perceive the incident being caused, in part, by a central bank doing its job properly” (ibid., 6). Positioning Bitcoin as a threat to financial stability (or special interests with tremendous political clout) may be a better selling or talking point to convince lawmakers to get on board with regulation of the currency. After all, U.S. lawmakers took a more active role in addressing counterfeits when pharmaceutical industry heavyweights put it on the agenda because their bottom lines were threatened by the creation and sale of fake or illegally-duplicated drugs (Efrat, *Governing Guns, Preventing Plunder: International Cooperation against Illicit Trade* 2012, 264).

In the U.S., the Federal Bureau of Investigation (FBI) has also explored the use of Bitcoin for money laundering. The FBI argues that a number of factors make the currency attractive for such nefarious purposes, including:

“no anti-money laundering software or monitoring capabilities to identify suspicious monetary patterns; no identification of account owners or their actual location; no historical records of transactions associated with real world identity; more difficult to identify the original source of funds compared to other online currencies; [and] law enforcement cannot target one central location or company for investigative purposes or to shut down the system” (2012, 6).

⁶ In addition to bidirectional flows, this European Central Bank identified two other types of “virtual currency schemes” – including “closed” which “are basically used in an online game” and “unidirectional flows” for purchasing online currency that is then used for “virtual goods and services, but exceptionally also to buy real goods and services.” Essentially with a bidirectional flow, a consumer can convert their currency to the virtual currency and then cash out to their currency as well.

In other words, it is ripe for individuals and organizations looking to maintain low profiles or go undetected.

The aforementioned Brookings Institution and Baker Institute report touched on the possibility of money laundering with Bitcoin (specifically with the FBI's reference to the challenges of identifying the original source of funds):

“Scale enables vanishingly low transaction costs, which are an essential element in the ability to hide larger movements of money by conducting many smaller transactions. A movement of \$900,000 conducted using 100 different electronic transfers of \$9,000 might be easy to spot. If, however the power of a large, distributed online network were used to move money using 100,000 transactions with randomized amounts generally in the \$6 to \$15 range, detection would be much more difficult.” (Villasenor, Monk and Bronk 2011, 6-7)

Notably, both the 2012 FBI report and the Brookings Institution/Baker Institute paper lack any actual cases of Bitcoin money laundering. The FBI report does offer other examples of virtual currencies being used for such purposes, but nothing specific to Bitcoin.

As a potential remedy for bringing virtual currency under the watchful eye of government, the 2012 FBI report suggested “any third-party service that qualifies as a money transmitter must register as a money services business with the Financial Crimes Enforcement Network (FinCEN) and implement an anti-money laundering program” (2). This places the burden on those that facilitate the exchange of Bitcoin, rather than on individuals who utilize the currency. As a follow up, in March 2013, FinCEN issued language attempting to codify that third parties, like the exchanges that work alongside Bitcoin, must register (and therefore be bound by anti-money laundering laws). The regulations are explicit in that they exclude individual users of the currency from registration but include anyone who “creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in

transmission to another location and is a money transmitter” and explain “a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency” (Financial Crimes Enforcement Network 2013). Under these terms, “if you're a lone Bitcoin miner who uses all of your proceeds to buy drugs on the Silk Road, FinCEN will not expect you to register as an MSB [money services business]” (Lee 2013).

Christin also suggested that one intervention point is “**attacking the delivery model,**” noting specifically that “a large number of sellers seem not to worry about seizures. Most items are marked as shipping internationally, which means that the risk of package loss or destruction is viewed as minimal by the sellers... Very often, seized packages are simply destroyed, or returned to the sender” (Christin 2012, 22). While a good point, research indicates that sellers and buyers typically involve a third-party address when sending and receiving goods. So, the effort to investigate based on addresses may be moot. Furthermore, it is common knowledge that many of the shipments coming into the U.S. – either by mail, air, or boat – go uninspected. While U.S. Customs and Border Patrol’s website boasts of a 100 percent inspection rate of “all cargo transported on passenger aircraft departing U.S. airports,” (U.S. Department of Homeland Security 2013), roughly only four percent of cargo arriving through maritime ports is inspected (Bliss 2012). Given that there is little appetite among the American people to increase government spending and/or little political will in Washington to cut wasteful spending that could be redirected toward these efforts, the dedication of additional resources to searches and seizures seems like a remote possibility. Finally, most of the sales made through the Silk Road are minimal, so the odds of law enforcement being able to put copious amounts of “dope on the

table” for a press conference are slim; the lack of optics eliminate the incentives – especially when the costs are high.

Christin’s fourth suggestion for Silk Road intervention is **laissez-faire**: nothing. Christin is unspecific as to whether he means allowing Silk Road to persist (while buying, selling, and using drugs remains illegal) or if he means lifting all limits on the purchase, sale, and use of illicit drugs (drug legalization). His mention of the lower costs associated with preventing drug abuse rather than law enforcement seems to indicate his inclination toward lifting prohibition altogether (Christin 2012, 22). Christin is not the first to suggest this approach, and in fact many places throughout the United States are moving toward legalization of marijuana.⁷

In a review critical of Moisés Naím’s book, *Illicit*, Harvard Professor Jeffrey Miron explores several issues surrounding drug prohibition, including the emergence of black markets. Miron argues that black markets create the undesirable effects of drug usage, including violence and corruption because “participants in illegal markets cannot address grievances with the government using standard means,” a whole host of negative externalities and higher costs (that ultimately result in “bang-for-the-buck” uses that spread disease) (Miron 2006). Although it is not a cure-all (especially as it relates to uninvolved third parties who suffer consequences of drug abuse, such as the children of users), the online marketplace may help to alleviate some of the negative consequences of black markets, particularly the violence associated with the drug trade and usage. A seller is insulated with anonymity; with Silk Road, an unsatisfied buyer has no way to find out exactly who the seller is and where he or she is located, therefore limiting violent recourse. To that end, however, there is also the possibility that Silk Road may implode on its own or may never amount to much in terms of volume and market share precisely because of the

⁷Voters in Colorado and Washington State both legalized the recreational use of marijuana in 2012 (National Council of State Legislatures 2012).

anonymity it offers. Certainly a buyer can receive negative feedback – and those who do not follow the terms of service can be kicked off the site – but a successful enterprise relies on brand identity, and that is hard to achieve without names and faces.

Nations face a number of challenges trying to combat international drug trade when products are exchanged “traditionally,” but the challenges are even more complicated when the trade involves online buying, trading, and selling. So while one solution for coping with Silk Road might be more **international coordination and regulation**, the prospects for developing a single stance – let alone a single approach – seem daunting, if not impossible. According to John Lyons, CEO of the International Cyber Security Protection Alliance, who talked about the possibilities for the United Kingdom to regulate the dark web, “The Government could work with regimes around the world who might be capable of taking these sites down without infringing their own laws...[b]ut, at the moment, there’s no cohesive strategy” (Franklin 2012).

Not only are there capacity issues (the abilities of governments to develop and dedicate resources to Internet-related investigations) but there are altogether differing opinions about the role of government and Internet surveillance. Consider the overview Watson (2012) provided when he explored the differences in how nations approach Tor:

- **United States:** While the U.S. does not restrict Tor (after all, the U.S. government created it and relies on it), there is no clarity as to whether anyone who serves as a node on the network could be liable for the illegal transmission of intellectual goods (Watson 2012, 725). This and other Internet privacy issues have been the subject of debate in Congress and in the White House in recent years, but no major resolutions have been reached. Watson mentions that President Obama backs legislation that would “inhibit Internet privacy” by “requir[ing] all services that enable communications...to be

technically capable of complying if served with a wiretap order” (ibid., 726). Since 2010, the FBI has sought additional authority and power to “wiretap” Internet communication. As reported in *The New York Times* in May 2013, the FBI has issued a big-stick proposal that will empower the FBI to fine companies up to \$25,000 per day for failing to comply with wiretap orders. Furthermore, there is no longer “wobble room” for technology companies to say that they attempted to help comply with a judge’s wiretap order; there is no choice but to comply with the order. However, the proposed rule would not force “companies that facilitate the encryption of users’ messages to always have a key to unscramble them if presented with a court order...[t]he current proposal would allow services that fully encrypt messages between users to keep operating” (Savage 2013).

- **China:** The “Great Firewall of China” has made Tor illegal, by “blocking access to entrance node IP addresses, but...users continue to circumvent this bulwark by linking with the Tor network through bridge nodes” (Watson 2012, 729).
- **Saudi Arabia:** “Like China, [Saudi Arabia] routes all Internet traffic through its national network” (ibid., 729) and “the Tor site is blocked...however, circumvention of the network appears to be relatively common in the country” (ibid., 731). According to Watson’s analysis, Saudi Arabia “focuses its Internet regulation on heavily quashing dissent, prohibiting the publication or accessing of ‘anything contrary to the state or its system’” (ibid., 730); this would include drugs (sold on Silk Road via Tor) or pornography or even just discussion (facilitated on Tor).
- **United Arab Emirates:** Not only is Tor banned in UAE, but so too is any proxy site. Such steps are taken to keep out “blocked content, such as pornography and sites

detailing how to conduct criminal activity...[and to prevent] Internet users to evade government monitoring” (ibid., 732).

Governments tend to engage in international trade regulation (of legitimate industries) when a key constituency is threatened or activated, as the U.S. pharmaceutical industry was in the 1980s when concern over counterfeit drugs grew. Asif Efrat argued that nations tend to come to the international negotiation table when there are “increases with [the] magnitude of the trade’s negative externalities and with their perceived severity” (Efrat, *Governing Guns, Preventing Plunder: International Cooperation against Illicit Trade* 2012, 264). In a separate article, Efrat had explained that there are primary and secondary externalities associated with illicit trade, the former being those that have monetary and security impacts (the latter being about the larger cause, such as humanitarian concerns) (Efrat, *Toward Internationally Regulated Goods: Controlling the Trade in Small Arms and Light Weapons* 2010, 105-106). Knowing this, international regulation will not develop unless and until the threat becomes large enough to a nation’s economy; at that point, it might be too late.

As it relates to Silk Road, the **opportunities for international trade regulation** exist with regulating the goods themselves (defining the legality of the products), the financial transactions (Bitcoin and other anonymous virtual currencies), and the technology. Although some of the goods sold on Silk Road are licit drugs (and therefore might draw the interest of pharmaceutical companies), the volume is so minimal compared to the overall size of the counterfeit drug market -- an estimated \$75 billion annually (Bate 2012). Most of the transactions involve illicit goods, and there is no organized industry group for illicit drugs (although some of the networks carry tremendous political influence and clout, as Moisés Naím

has detailed in *Illicit*). Therefore, industry is not likely to call for regulation because of the goods themselves.

Where industry might get involved, however, is with the desire to regulate financial transactions and the technology. Although Bitcoin has experienced tremendous volatility and hacks, some might suggest that central banking authorities could view Bitcoin as a legitimate threat to fiat currency (and related products, including credit cards and traditional bank accounts used for online purchases) (Freeman 2013). In addition to its use on Silk Road, consumers are embracing Bitcoins out of political reasons (dissatisfaction with currency manipulation by central banking authorities) and for economic reasons (stability and possible investment) (Lew 2013). In fact, the European Central Bank's analysis of virtual currency "schemes" suggest that currencies like Bitcoin "could represent a challenge for public authorities, given the legal uncertainty surrounding these schemes...[and] could have a negative impact on the reputation of central banks" (European Central Bank 2012, 47). If consumers – purchasing illicit or licit goods – decide Bitcoin is a better tool with which to purchase goods and services online or even in-person, then that keeps money out of the traditional fiat circulation and out of the hands of banks and credit card companies.

As it relates to regulating the technology, Internet service providers (ISPs) have been relatively silent, including on the use of Tor by computers utilizing their networks⁸, but if liability is reassigned to them, then ISPs (and the major telecommunications companies by which they are owned) may take steps to insulate themselves from civil or criminal penalties. As Watson noted, "there has not yet been a case dealing with the legality of running a Tor exit node. However, some Tor exit node facilitators have received DMCA [Digital Millennium Copyright

⁸ The Electronic Frontier Foundation maintains a list of "Tor-friendly" ISPs: <https://trac.torproject.org/projects/tor/wiki/doc/GoodBadISPs>

Act, a U.S. law] notices from their ISPs, universities, and similar organizations” (Watson 2012, 733). In Australia, a man whose computer served as a node on the Tor network was charged with transmitting child pornography, although he says he never accessed it – he argued that the content just filtered through his node (Pauli 2012).

One other source of industry intervention is from the delivery industry. UPS recently agreed to pay \$40 million to “settle a federal probe into shipments for illegal online pharmacies, admitting the company had information it was helping distribute controlled substances” (Schoenberg 2013). Under this agreement, UPS committed to establish a “compliance program to prevent illegal Internet pharmacies from using its shipping services” following the discovery that the shipping company’s employees were aware of the products being delivered through its global delivery service (Schoenberg 2013). When governments cannot seem to get the job done, it is often suggested that the private sector either engage in self-regulation or seek collaboration with the government; Villasenor, et. al. offered such suggestions for dealing with illicit financial transactions, and ,perhaps, similar alternatives exist for online drug sales.

Conclusion

Dismantling and disrupting Silk Road would likely have little to no effect on the overall drug trade. In the same way that scene after scene of “dope on the table” has not reduced drug usage or scaled back the global trade of drugs, shutting down one website – from founders to sellers to buyers – would be an expensive operation. As the example of “Operation Adam Bomb” showed, in which two years of investigation by several U.S. and international agencies yielded less than a dozen arrests of individuals barely transacting more than \$1 million on “The Farmer’s Market, the problem is deeper than finding out who runs websites and who sells drugs on those sites. As with the “traditional” drug problems, illicit trade in drugs happens for economic reasons (as a source of income), political reasons (governments lack capacity to enforce laws, corruption, etc.), and because of the plain and simple demand for the product.

Realistically, ending the drug trade is likely to never happen because of the aforementioned multitude of reasons that drive it; eliminating those is next to impossible. That said, a number of possible intervention points exist for policymakers who wish to curtail and limit the drug trade and its harmful consequences on society. First, electronic commerce is never going away; in fact, it will only expand as more people obtain Internet access and as incomes continue to rise. Therefore, governments (through the mandates of the people) must determine the extents to which such transactions will be regulated (if at all). Will virtual currencies be allowed? And, if so, to what extent will they be bound by the rules and regulations of traditional currencies and banking authorities? Will anonymous purchases be allowed? Second, and on a related front, to what extent do the technologies that facilitate these transactions maintain liabilities for licit and illicit transactions? Are the cables and cords that enable someone to sell a good any more responsible than the street corners and alleyways in which marijuana used to

change hands? Third, where are resources going to be invested? Is it worth the time and money to make an example out of one website and small-scale dealers and buyers – especially when there is no chilling effect because of the multitude of alternatives?

This is an extremely good paper and I think you should submit it to the school's journal. The only change I would add is to the say about the limitations on regulation especially in the transnational situation in which this illicit trade occurs. You have done a truly impressive amount of research that is up to the last moment. You have shown real breath in your reading. It present fine insights. It is clearly written and organized. I would like to put it up on the TraCCC website if you give us permission.

Grade A plus

Bibliography

Adweek. "Not so funny money." May 30, 2011: 22.

Ahmed, Murad. "Drugs, guns and passports for sale on 'Dark Web'." *The Times*, April 3, 2012.

—. "'It's like Amazon, but for criminals'; A 'Snooper's Bill' may affect your privacy, but it won't prevent those who use the internet as a digital black market, finds Murad Ahmed." *The Times*, April 3, 2012.

Allnutt, Luke. "Show Me the Money." *Sunday Times*, July 3, 2011.

Bate, Roger. *PHAKE: The Deadly World of Falsified and Substandard Medicines*. Washington: American Enterprise Institute Press, 2012.

Bitcoin Charts. *Bitcoin Charts: Mt. Gox (USD)*. <http://bitcoincharts.com/markets/mtgoxUSD.html> (accessed May 11, 2013).

Bitcoin. *What is the current legal status of Bitcoin around the world?* August 30, 2011. <http://bitcoin.stackexchange.com/questions/131/what-is-the-current-legal-status-of-bitcoin-around-the-world> (accessed March 17, 2013).

Bliss, Jeff. "U.S. Backs Off All-Cargo Scanning Goal With Inspections at 4%." *Bloomberg*. August 13, 2012. <http://www.bloomberg.com/news/2012-08-13/u-s-backs-off-all-cargo-scanning-goal-with-inspections-at-4-.html> (accessed April 27, 2013).

Butcher, Steve. "Secret website harboured drugs smorgasbord, court hears." *The Age*. January 31, 2013. <http://www.theage.com.au/victoria/secret-website-harboured-drugs-smorgasbord-court-hears-20130131-2dlw3.html> (accessed March 16, 2013).

Chen, Adrian. "Are Authorities Closing In On the Online Drug Market Silk Road?" *Gawker*. June 16, 2012. <http://gawker.com/5926440/are-authorities-closing-in-on-the-online-drug-market-silk-road> (accessed March 16, 2013).

—. "The Underground Website Where You Can Buy Any Drug Imaginable." *Gawker*. June 1, 2011. <http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable> (accessed February 18, 2013).

Christin, Nicholas. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace." November 28, 2012. <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1106&context=cylab> (accessed March 17, 2013).

Cohn, Cindy. "EFF and Bitcoin." *Electronic Frontier Foundation*. June 20, 2011. <https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin> (accessed May 11, 2013).

Count the Costs. "Alternative World Drug Report." *Count the Costs*. June 26, 2012. <http://www.countthecosts.org/sites/default/files/AWDR.pdf> (accessed April 13, 2013).

Davis, Joshua. "The Crypto-Currency." *The New Yorker*, October 10, 2011.

eBay. *Replicas, counterfeit items, and unauthorized copies policy*. 2013. <http://pages.ebay.com/help/policies/replica-counterfeit.html> (accessed March 16, 2013).

—. *Stolen property and property with removed serial numbers policy*. 2013. <http://pages.ebay.com/help/policies/stolen.html> (accessed March 16, 2013).

Efrat, Asif. *Governing guns, preventing plunder: international cooperation against illicit trade*. New York: Oxford University Press, 2012.

Efrat, Asif. "Toward Internationally Regulated Goods: Controlling the Trade in Small Arms and Light Weapons." *International Organization* 64, no. 01 (2010): 97-131.

European Central Bank. *Virtual Currency Schemes*. October 2012. <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (accessed March 16, 2013).

Everett, Cath. "Moving across to the dark side." *Network Security*, no. 9 (September 2009): 10-12.

Federal Bureau of Investigation. "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Detering Illicit Activity." *Wired Magazine*. April 24, 2012. http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (accessed May 5, 2013).

Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies ." *Financial Crimes Enforcement Network*. March 18, 2013. http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html (accessed May 5, 2013).

- Fowler, Geoffrey. "Tor: An Anonymous, And Controversial, Way to Web-Surf ." *Wall Street Journal*. December 17, 2012. <http://online.wsj.com/article/SB10001424127887324677204578185382377144280.html> (accessed March 16, 2013).
- Franklin, Oliver. "Unravelling the dark web." *GQ*. November 7, 2012. <http://www.gq-magazine.co.uk/comment/articles/2013-02/07/silk-road-online-drugs-guns-black-market/viewall> (accessed March 16, 2013).
- Freeman, James. "The Weekend Interview: Bitcoin vs. Ben Bernanke ." *Wall Street Journal*. May 3, 2013. <http://online.wsj.com/article/SB10001424127887323809304578429142650304564.html> (accessed May 11, 2013).
- Gayathri, Amrutha. "From marijuana to LSD, now illegal drugs delivered on your doorstep." *International Business Times*. June 11, 2011. <http://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021> (accessed March 13, 2013).
- Geere, Duncan. "Peer-to-peer currency Bitcoin sidesteps financial institutions." *Wired.co.uk*. May 16, 2011. <http://www.wired.co.uk/news/archive/2011-05/16/bitcoin-p2p-currency?page=all> (accessed March 16, 2013).
- General Assembly of the United Nations. "Thematic Debate of the 66th session of the United Nations General Assembly on Drugs and Crime as a Threat to Development." *United Nations*. June 26, 2012. <http://www.un.org/en/ga/president/66/Issues/drugs/drugs-crime.shtml> (accessed April 27, 2013).
- Gibbs, Mark. "vCash, Crypto, and Anonymization Equals Drugs to Your Door." *Network World (Online)*, June 6, 11.
- Greenberg, Andy. "Black Market Drug Site 'Silk Road' Booming: \$22 Million In Annual Sales." *Forbes*. August 6, 2012. <http://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales/> (accessed March 16, 2013).
- . "Founder Of Drug Site Silk Road Says Bitcoin Booms And Busts Won't Kill His Black Market." *Forbes*. April 16, 2013. <http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/> (accessed May 5, 2013).
- Greenwell, Daisy. "The Currency of the Dark Side." *The Times*, April 3, 2012.
- Keene, Shima D. "Emerging threats: financial crime in the virtual world." *Journal of Money Laundering Control*, 2012: 25-37.
- Koul, Scaachi. "The dark side of the Internet." *Maclean's*, October 22, 2012.
- Lee, Timothy B. "US regulator: Bitcoin exchanges must comply with money-laundering laws." *Ars Technia*. March 19, 2013. <http://arstechnica.com/tech-policy/2013/03/us-regulator-bitcoin-exchanges-must-comply-with-money-laundering-laws/> (accessed May 5, 2013).
- Lew, Jeremy. "Why I Take Bitcoin Seriously as a Venture Capitalist." *American Banker*. April 5, 2013. <http://www.americanbanker.com/bankthink/why-i-take-bitcoin-seriously-as-a-venture-capitalist-1058079-1.html> (accessed April 13, 2013).

Matonis, Jon. "ECB: "Roots Of Bitcoin Can Be Found In The Austrian School Of Economics"." *Forbes*. November 3, 2012. <http://www.forbes.com/sites/jonmatonis/2012/11/03/ecb-roots-of-bitcoin-can-be-found-in-the-austrian-school-of-economics/> (accessed March 16, 2013).

Miron, Jeffrey. "Opening Pandora's Box: A Radical Look at Controlling Illicit Trade." *Georgetown Journal of International Affairs* 7, no. 2 (Summer 2006): 155-159.

Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. "An Analysis of Underground Forums." *ACM Internet Measurement Conference*. Berlin, 2011.

Munroe, Ian. "Welcome to the 'dark web,' a haven for illegal trafficking." *CBC*. May 3, 2013. <http://www.cbc.ca/news/technology/story/2013/05/02/dark-web-illegal-goods-global.html> (accessed May 5, 2013).

Naím, Moisés. *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*. New York: Anchor Books, a Division of Random House, 2005.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." November 1, 2008. <http://bitcoin.org/bitcoin.pdf> (accessed March 13, 2013).

National Council of State Legislatures. "Legalizing and Decriminalizing the Recreational Use of Marijuana." *NCSL - Drug Policy on the Ballot*. November 7, 2012. <http://www.ncsl.org/legislatures-elections/elections/drug-policy-on-the-ballot.aspx?stateid=wa#rec> (accessed May 11, 2013).

NPR . "Silk Road: Not Your Father's Amazon.com." *NPR: All Things Considered*. June 12, 2011. <http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com> (accessed March 16, 2013).

Office of U.S. Senator Joe Manchin. *Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs*. June 6, 2011. <http://manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3> (accessed March 16, 2013).

OpenSecrets.org. *Senator Charles E. Schumer - Career Profile - Top Industries*. <http://www.opensecrets.org/politicians/industries.php?cycle=Career&cid=N00001093&type=I> (accessed May 11, 2013).

Pauli, Darren. "Tor exit node operator raided by police." *SC Magazine*. November 30, 2012. <http://www.scmagazine.com.au/News/324804,tor-exit-node-operator-raided-by-police.aspx> (accessed May 5, 2013).

"Peer-to-peer currency Bitcoin sidesteps financial institutions." *Wired.co.uk*. May 16, 2011. <http://www.wired.co.uk/news/archive/2011-05/16/bitcoin-p2p-currency?page=all> (accessed March 16, 2013).

Quittner, Jeremy. "For Banks, Digital Currency Poses Threat - and Opportunity." *American Banker*, January 17, 2012.

Rolling Stone. "Hot Black Market: 21st Century Drug Bazaar." November 10, 2011: 74.

Sanati, Cyrus. "Bitcoin looks primed for money laundering." *CNN Money*. December 18, 2012. <http://finance.fortune.cnn.com/2012/12/18/bitcoin-money-laundering/> (accessed March 16, 2013).

Savage, Charles. "U.S. Weighs Wide Overhaul of Wiretap Laws." *The New York Times*. May 7, 2013. <http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html> (accessed May 8, 2013).

Schoenberg, Tom. "UPS Pays \$40 Million to End Illegal Drug Shipment Probe." *Bloomberg*. March 29, 2013. <http://www.bloomberg.com/news/2013-03-29/ups-settles-probe-of-illegal-online-drug-shipments-u-s-says.html> (accessed May 5, 2013).

Sederstrom, Jotham. "Not so funny money." *Adweek*, May 30, 2011: 22.

Slattery, Brennon. "U.S. Senators Want to Shut Down Bitcoins, Currency of Internet Drug Trade." *PC World*. June 11, 2011. http://www.pcworld.com/article/230084/u_s_senators_want_to_shut_down_bitcoins.html (accessed March 16, 2013).

Solon, Olivia. "Police crack down on Silk Road following first drug dealer conviction." *Wired.co.uk*. February 1, 2013. <http://www.wired.co.uk/news/archive/2013-02/01/silk-road-crackdown> (accessed March 18, 2013).

States News Service. "Operation Adam Bomb: Arrest of Creators, Operators of Online Secret Narcotics Marketplace -- First Federal Indictment of Its Kind; Operated in All 50 States, 34 Countries." *States News Service (via Lexis Nexis)*. April 16, 2012. www.lexisnexis.com/hottopics/Inacademic (accessed May 5, 2013).

Surowiecki, James. "Cryptocurrency." *Technology Review*, September 1, 2011: 106-107.

The Economist. "Monetarists Anonymous; Bitcoin." September 29, 2012: 80.

The Economist. "The bursting of the Bitcoin bubble ." *The Economist*. October 21, 2011. <http://www.economist.com/blogs/babbage/2011/10/virtual-currencies> (accessed April 14, 2013).

Tor. *How is Tor different from other proxies?* March 15, 2013. <https://www.torproject.org/docs/faq.html.en#Torisdifferent> (accessed March 16, 2013).

—. *Tor: Overview*. March 15, 2013. <https://www.torproject.org/about/overview.html.en> (accessed March 16, 2013).

U.S. Department of Homeland Security. "A Multi-layered Approach to Cargo Security." *Department of Homeland Security*. 2013. <http://www.dhs.gov/cargo-screening> (accessed April 27, 2013).

United Nations Office on Drugs and Crime. "2012 World Drug Report." *United Nations Office on Drugs and Crime*. June 2012. http://www.unodc.org/documents/data-and-analysis/WDR2012/WDR_2012_web_small.pdf (accessed April 13, 2013).

Villasenor, John, Cody Monk, and Christopher Bronk. "Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments." *Baker Institute*. August 29, 2011. <http://www.bakerinstitute.org/publications/ITP-pub-FinancialTransactions-082911.pdf> (accessed April 13, 2013).

Wallace, Benjamin. "The Rise and Fall of Bitcoin." *Wired*. December 2011. http://www.wired.com/magazine/2011/11/mf_bitcoin/all/ (accessed March 16, 2013).

Watson, Keith D. "The Tor Network: A Global Inquiry." *Washington University Global Studies Law Review* 11 (2012): 715-737.