THE INFORMATION SOCIETY
2017, VOL. 33, NO. 1, 23–34
http://dx.doi.org/10.1080/01972243.2016.1248612

Routledge
Taylor & Francis Group

Silk Road: The market beyond the reach of the state

Rita Zajácz

Department of Communication Studies, University of Iowa, Iowa City, Iowa, USA

ABSTRACT

Between February 2011 and October 2013, Silk Road operated the largest and most sophisticated anonymous online marketplace for illegal drugs. More than a business venture, it was designed for anarcho-capitalist resistance to state power. The primary research question of this inquiry is: Can a stable market, defying the state, emerge under conditions of online anonymity? The article shows that Silk Road was built on a contradiction. On the one hand, strong cryptographic anonymity was embraced because it facilitated hiding from the state. On the other hand, the very same cryptographic anonymity made it difficult to impose rules and create a stable market. Silk Road sought to cultivate subcultural norms to ensure proper behavior in face of anonymity but they were not strong enough to control the behavior enabled by its architecture.

ARTICLE HISTORY
Received 3 June 2015
Accepted 17 April 2016

KEYWORDS
Data market; cryptomarket; anonymity; private regulation; libertarian activism; opportunism; enforcement; working anarchy

Between February 2011 and October 2013, Silk Road operated the largest and most sophisticated anonymous online marketplace for illegal drugs. This "eBay for drugs" adopted the best practices from the world of legitimate e-commerce alongside cutting-edge advances in peer-to-peer technologies. Site administrator Dread Pirate Roberts (DPR) expressly sought to provide order while hiding from the state. In his efforts to protect buyers and sellers from each other (and both from the state), DPR took on some of the internal and external security functions of the state, including fighting internal crime[1] on Silk Road and protecting site participants from external threats. Yet Silk Road functioned as a complex environment with minimal surveillance and identification. In the following, I examine what actually transpired when DPR implemented his ideas, asking whether a stable market, in direct defiance of the state, can emerge under conditions of online anonymity.

In the 1990s government agencies (Freeh 1997), researchers (Froomkin 1999; Kling, Lee, Teich, and Frankel 1999), and activists (May 1992; Levy 1996) anticipated that online anonymity would pose a challenge to the traditional control mechanisms of states. This preoccupation with the challenge to state power, however, obscured the challenge that anonymity would pose for radical resistance. As DPR took on some of the functions of the state, the challenges the state faces when dealing with anonymous activities became his challenges. The lack of enforcement options on Silk Road, resulting from the site's anonymity protections, resulted in a chasm between DPR's promise to ensure honest transactions and his inability to do so.

This article reviews scholarship on the governance mechanisms of markets, followed by a discussion of the libertarian underpinnings of DPR's vision. The next two sections analyze DPR's attempts at dealing with the internal and the external security threats: protecting market participants from each other and the entire community from the state. Finally, I examine the problem of opportunism that Silk Road could not solve: How would the dark market protect site administrators from extortion?

On markets, anonymity, and governance

The emergence of privacy-enhancing technologies (PETs) has intensified hopes of a techno-libertarian resistance to state power. In the early 1990s, the Crypto-Anarchist Manifesto predicted fundamental changes in the nature of regulation and the state's ability to tax and control economic interactions in the wake of new technologies (May 1992). Benkler (2013, 247) characterizes the ensuing challenges to state power in the networked environment—some facilitated by a marriage of encryption technology and peer-to-peer networking—as mutualistic or "practical anarchic."

According to Benkler, practical anarchism is the systematic effort to expand the domains of application of peer mutualism in order to work around the imperfections of states and markets, rather than replace them.

CONTACT Rita Zajácz rita-zajacz@uiowa.edu Department of Communication Studies, University of Iowa, 129 BCSB, Iowa City, IA 52242, USA.

Benkler identifies three types of practical anarchism—commons-based peer production, pervasive illegality, and radical resistance—but focuses on commons-based peer production and leaves the other two types unelaborated. Commons-based peer production of information is manifest, for example, in the self-governing, distributed decision-making processes of the Internet Engineering Task Force or Wikipedia. These are "working anarchies" because they successfully avoid dependence on "direct or delegated power from the state" (2013, 217). Pervasive illegality, on the other hand, refers to people disobeying restrictive laws, as in alcohol consumption during the Prohibition era or outlawed personal relationships in the face of sodomy laws. Finally, radical resistance can be either legal as in the case of WikiLeaks (an example of a peer model for delivering public accountability for Benkler) or marginally legal, like the activities of the Anonymous hacking collective.

Benkler takes pains to exclude markets from the definition of working anarchies, as they rely on state enforcement of the system of property relationships that provide the institutional foundations for their functioning. Though markets display voluntary behavior, they are inherently coercive. What, then, of crypto or dark markets, like Silk Road, where goods and services are exchanged "between parties who use digital encryption to conceal their identities" (Martin 2014, 356)? DPR himself championed voluntarism as the backbone of the site's operation. "Order and civility," without the coercive power of the state, were his stated goals (Mullin 2015b). In effect, Silk Road blended Benkler's second and third types of practical anarchy—pervasive illegality and radical resistance. Like a Prohibition-era speakeasy, the site made available illegal substances, but it also foregrounded radical resistance as the raison d'être of its existence. Here harnessing of the power of the state to enforce property relations was out of the question. The scope of libertarian activism is, therefore, broader than Benkler's conception of working anarchies.

Resistance to state power via a market immediately raises the Hobbesian problem of order: Is the pursuit of self-interest compatible with social stability? The literature on Silk Road itself provides little guidance, as researchers have used it as a case to inform their discussions on cybercrime and drug policy, not to understand the complex decisions that transformed lines of source code into a vibrant market (Aldridge and Décary-Hétu 2014; Christin 2012; Martin 2014; Van Hout and Bingham 2013a, 2013b, 2014). Various strands of economics and sociology, however, have a lot to offer. Unlike neoclassical economists and libertarian theorists, who imagine a stable order built on self-interest, economic sociologists and scholars of new institutional economics follow sociologist Max Weber and philosopher Thomas Hobbes in positing a conflict between self-interest and the interest of society. In the latter perspective, *opportunism*—the pursuit of self-interest via fraud and force—is integral to the free market. Rather than a venue for orderly transactions, the free market is in fact a war of all against all where norms play no role and crime runs rampant (Block 1990; Doherty 2007; Granovetter 1985; Trubek 1972).

Certain strands of economic sociology and new institutional economics agree that market participants are unable to provide rules for themselves and instead require institutions "whether they are aware of them or not" (Fligstein 2001, 33; Williamson 1975, cited in Fligstein 2001; Granovetter 1985). New institutional economists distinguish between "adherent" and "contractual" organizations, where the former coordinate their members' actions via self-enforcing, "incentive-compatible" agreements (i.e., informal institutions), while the latter combine these agreements with formal rules that require third-party enforcement (North, Wallis and Weingast 2009, 16). The size of "the enforcement entity" increases with the size of the society until we arrive at the modern state, which, in Max Weber's classical formulation, is distinguished by the legitimate use of force (Weber 1968, cited in Trubek 1972).

A central insight of new institutional economics concerns the role of technology in facilitating the enforcement of rights. Private property rights in land were not possible until technological change—the invention of the barbed wire—made enforcement easier (Anderson and Hill 1975, cited in Kruse 2005). Lessig (2006) has highlighted technology as one of four main ways of regulating behavior online: the market, the law, norms, and "code," which is best understood as the architecture of social life in cyberspace. Since Silk Road was a black market, DPR and his team were left with two governance mechanisms: norms (libertarian ideas and Silk Road's organizational rules) and code (the architecture of the site) to ensure accountability.

Behavioral norms prevent crime, whereas a site's architecture can be used for both prevention and enforcement, except that using code for prevention often means surveillance, while using code for enforcement requires identification (Katyal 2004). For example, eBay, run by libertarians but desirous of integrating into the consumer economy, started employing both surveillance and identification and turned to the state for enforcement actions, as it shed its original identity and character as an anonymous,[2] self-governing community (Goldsmith and Wu 2008). I follow DPR's attempts to create a stable market in an online environment, which, in the absence of social relations or institutions, was as close to Hobbes's state of nature as it gets.

As revelations about the surveillance practices of the U.S. government are transforming online anonymity into "a key policy issue of the twenty-first century" (Kozinski 2015, 17), we are reminded of an earlier debate about the impact of anonymizing technologies. In 1999 *The Information Society* published a special issue on "Anonymous Communication on the Internet" based on an American Association for the Advancement of Science (AAAS) conference held in November 1997. Here Kling et al. (1999), in an article that "distills and elaborates on the discussions at the AAAS Conference" (80), noted that such technologies would "challenge the efficacy of traditional control mechanisms available to states" (84) and identified the potential rise of online drug markets as one of the possible harms of anonymity. But they did not delve into the mechanics of how online drug markets would operate, as these were not the primary focus of the discussion. Yet, as Marx (1999) in an article in this special issue noted, no commentary about online anonymity fails to point out its dual nature: Anonymizing technologies facilitate free speech and individual autonomy, but they may also serve as the breeding ground for opportunism, enhancing the conflict between self-interest and the interests of the community. A market for illegal and dangerous goods can exist, a federal judge recently commented, "only because it is possible to use the Internet to render transactions anonymous and thus, drastically reduce the risks of engaging in antisocial behavior" (Kozinski 2015, 5). Could an organization defying the state enjoy the advantages of online anonymity without suffering its pitfalls?

I have reconstructed the social and material underpinnings of Silk Road based on court documents, other researchers' accounts, newspaper articles, and pseudonymous comments on such articles. Court documents describe the technological features of the site, and include extensive information from DPR's chat logs, as well as screen captures of the site. These are primary sources for analyzing the operation of the site; though pre-selected by the state, the amount information available is large enough to facilitate "thick description," that is, the study of actions in context, which is a form of "within-case analysis" in social scientific terms (Geertz 1973; Eisenhardt 1989). Such case studies provide intimate familiarity with each case as a stand-alone entity, laying the groundwork for cross-case comparisons concerning, for example, the possibilities of technolibertarian resistance provided by anonymizing technologies. Historical analysis does not, however, permit the collection of information in real time. As a result, it is ill-equipped to analyze how norms emerge and operate to constrain opportunism. Field notes, incorporating a running commentary around my sources, formed the basis of the analysis: I identified key topics, and grouped together information pertaining to these topics from multiple sources. In cases of inconsistent accounts that mattered for the analysis, I gave preference to the more complete and authoritative source, unless the other source had firsthand knowledge of the developments.

Libertarian underpinnings

By fall 2013, Silk Road comprised more than 100,000 users who completed $182.9 million in sales, earning DPR $13.17 million in commissions—a fraction of the more than $300 billion global drug trade, to be sure, but a good start for a market only available on the Dark Web (Martin 2014; Mullin 2015d). The site was not a retail operation, but a platform for illegal consumer-to-consumer transactions. Much like Airbnb, which connects owners of residential property with travelers interested in renting them, Silk Road simplified the process of posting descriptions and photographs of sellers' products, offered a system for taking payment, and tackled the broader marketing challenge of attracting customers (Guttentag 2015). Sellers appreciated direct distribution, which eliminated the risk of nonpayment and theft of product, and buyers were attracted by Silk Road's similarity to mainstream e-commerce sites and the convenience it offered (Martin 2014). By contrast, earlier sites established for selling drugs online, such as the Farmers' Market, were less widely used, and many of Silk Road's successors went down in flames as site administrators made off with tens of millions of dollars (Segal 2014; *The Economist* 2016). At least part of Silk Road's success can be attributed to the community-building efforts of the site's creator, which centered on an exchange of libertarian ideas and functioned as a means of creating social discipline.

When finishing his master's program in materials science, site administrator Ross Ulbricht became interested in the Internet "as a venue for perfecting free markets" (Grossman and Newton-Small 2013, 30). The five sections of Silk Road's Community Forum—Philosophy, Security, Shipping, Drug Safety, and Off Topic—served as the primary place of interaction for participants, much like a single grand entrance to a real space building where members would get to know each other and look out for one another (Katyal 2004; Mullin 2015a). The Philosophy section housed DPR's Book Club, which was devoted to the Austrian school of economics—represented by Ludwig von Mises and Murray Rothbard, who most recently theorized the self-correcting market—as well as to the countereconomics of a libertarian activist, Samuel E. Konkin. Participants got to know DPR through his ideas and actions, shared their experiences

with various drugs on the "harm reduction forum," and got acquainted with the vendors on the site via information about prior transactions posted by others. A good experience would lead to repeat purchases. In effect, DPR's Silk Road provided a good illustration of the importance of social relations for the functioning of any market—even the so-called free market.

DPR's ideas about the state closely mirrored those of Rothbard, who linked a refusal of coercive forms of authority to a reverence for the free market in a mixture called "anarcho-capitalism." According to Rothbard, the state, legitimized by a hopelessly inconsistent liberal tradition, has abused its war-making and taxation powers to such an extent that it was nothing more than a "criminal band" (1978). The "tax eating, life sucking, violent, sadistic, war mongering, oppressive machine," DPR declared on March 20, 2012, on the Silk Road website, did not deserve people's loyalties (quoted in Greenberg 2013, 6). Voluntarism was the ideal foundation for human civilization and the free market could supply everything that human beings needed (Silk Road Charter 2013; Doherty 2007). Government worked best when it competed with private providers of transportation, law, and security/defense, DPR declared on September 29, 2012, on the Silk Road website (cited in Greenberg 2013). Thus, the state did not have a monopoly on the use of force: Individuals were justified to use force to prevent crime or recover their property (Rothbard 1982).

In a clear reversal of the liberal standpoint, DPR understood the market as the solution to the problem of the illegitimate state. Silk Road was to provide an experience of a world "without the systemic use of force," where market forces, rather than a central power, regulated conduct (DPR, quoted in Ulbricht criminal complaint 2013, 24). The site embodied a practical application of countereconomics, that is, the use of the market to "evade, avoid and defy" the state (Konkin 1983, 7). If countereconomics was the strategy, agorism was the goal: a new society based on the Greek agora, an open marketplace—libertarian in ethos and free-market in practice (Konkin 1983).

DPR's libertarian ideas sought to give a higher meaning to drug deals, articulating the ideological core of the virtual community he had developed. He worked to create an adherent organization—a working anarchy—with shared goals and a common interest in a stable market. "Regardless of your motivations, you are a revolutionary," he wrote, as participants on Silk Road debated whether they were there "for the drugs or the revolution" (quoted in Grossman and Newton-Small 2013, 31). As one Silk Road customer expressed, many participants "came for the drugs, stayed for the revolution," indicating that they were on board with DPR's challenge to state power (quoted in Grossman and Newton-Small 2013, 31). Thus, when DPR announced policy changes in a State of the Road address, modeled after U.S. presidents' State of the Union address, few thought that anything was amiss (Ulbricht criminal complaint 2013, 18). A participant in a research study on DPR's Silk Road stated the obvious: "We are a community, and Dread Pirate Roberts is our president in a sense" (quoted in Van Hout and Bingham 2013b, 527).

Protecting buyers and sellers from each other

If participants thought of DPR as akin to their president, then was Silk Road a state? By attempting to bring order and civility into the black market, DPR took on a key function of the state: protecting citizens from harming each other through force, fraud, or theft (Goldsmith and Wu 2008). His approach to Silk Road reflected the recognition that buying drugs online was risky, and there was more to a successful market than the possibility of a bargain. Markets are best understood on a continuum of "marketness" based on the primacy of price considerations (Block 1990). Buyers often favor security over price and are willing to pay more to a supplier they trust, thereby reducing the "marketness" of transactions (1990). The four pillars of Silk Road's organizational framework—limiting the items for sale, the commission structure, the escrow system, and the reputation mechanism—anticipated market participants' desire to be assured of payment, product safety, product quality, and so forth even when they avoided personal relationships.

Silk Road sought to reduce the "marketness" of the anonymous market by balancing the protections offered to buyers and sellers and by creating an environment that promised a sense of accountability while retaining the anonymity of all participants. "Consumer rights" associated with legitimate marketplaces were in the air and the site administrators did not dispel such hopes, even though they lacked the ability to protect them. DPR did anticipate opportunism among site participants, but his efforts to prevent internal crime relied too much on norms and too selectively on code. He understood the importance of identification, even asking his staff to send him their drivers' licenses so that he would know who to look for if they did something wrong, but the site's architecture eschewed surveillance (Government exhibit 256 in Mullin 2015e). If cyberspace seems "dark" to advocates of government surveillance, Silk Road was darker still: No one could see what others were doing on the site, including DPR (Katyal 2004). Before long he was fighting internal crime with one hand tied behind his back.

Limiting what could be sold

In the state of nature, there is no crime. Protecting people from harming each other, on the other hand, requires a clear distinction between lawful and criminal acts. Despite listing items that are illegal in most jurisdictions, DPR pointed out, Silk Road is not "lawless" (Dread Pirate Roberts 2013, para. 2). Counterfeit currency, child pornography, assassinations, and stolen personal information were off limits throughout the duration of the site, but DPR allowed forgeries of government-issued documents such as fake identifications (IDs) and passports (Sellers' guide 2013; Ulbricht criminal complaint 2013).[3] This was a human-made market, not a spontaneous gathering, and there was more to Silk Road than community building. While professing a view of the market as a self-regulating economic mechanism, DPR nevertheless became its lawmaker.

For a site administrator who disavowed any attempt to control people's behavior, these restrictions could not go unexplained. DPR's justifications included such practical concerns as acquiring a critical mass alongside such moral objectives as the protection of innocent people (Sellers' guide 2013). These restrictions are best understood as a form of "signaling." Much like niche cable networks communicating their identities to target audiences, DPR's policies emphasized principled resistance, not a greedy free-for-all (Turow 1997). This site, the ground rules made clear, was for reasonable users who simply objected to government restrictions on their attempts to realize their inner "psychonauts." A large vendor would later identify his clientele as professionals in their 30s and 40s who paid extra for "peace of mind and quality" (O'Neill 2014, para. 9).

The prohibition on the sale of personal information, in particular, counteracted a problem familiar in legitimate e-commerce: Buyers parted with sensitive information without any hope of control over how that information would be used (Connolly 2013). While most vendors would have sold personal information acquired via hacking, they could also turn around, just like in real space, to sell their buyers' personal information as well. As a result, Silk Road's system would delete the buyer's shipping address as soon as the seller clicked on "confirm shipment." DPR also requested that sellers never ask their clients for personal information and that they destroy their clients' shipping addresses after the transaction was complete (Sellers' guide 2013). Whether vendors complied, however, DPR could not tell. In fact, the FBI's case against Ulbricht shows listings for "Firearms + Ammunition," "Stolen Info (CC, [credit card] Paypal)," and "Hitmen (10+ countries)"—all in clear violation of Silk Road's policies (Ulbricht criminal complaint 2013, 10). Potential disclosure of personal information would turn out to be a major threat to the integrity of the site.

Silk Road's escrow system and its commission structure

For a site ostensibly regulated by market forces, Silk Road was remarkably centralized. DPR set up an internal "bank" in Bitcoin, a virtual currency far less traceable than credit card payments. Users who wanted to conduct transactions had to hold an account. When buyers made purchases, they deposited their Bitcoin payment into a "wallet" maintained by Silk Road, which meant that the site held the currency in escrow. When buyers received the goods, they finalized the transaction and the Bitcoins were released to the seller's account, and DPR took the commission (Ulbricht criminal complaint 2013). The combination of Bitcoins and the escrow system safeguarded DPR's short- and long-term interests by ensuring that he always got the commission and that transactions were hidden from the state. But the escrow system also anticipated fraud and served as a means of buyer protection. It prevented internal crime by addressing the risk that had plagued electronic market transactions from the very beginning, namely, that the consumer and the vendor were separated in place and time and the former often paid well before the receipt of goods (Connolly 2013). With the escrow system in place, each order consisted of two parts: the request for the item and the confirmation that it arrived. Money was to be transferred only after receipt of the purchase, and a problem unique to online transactions—that buyers would not get anything for their money—nearly disappeared. Libertarian ideas thus went hand in hand with the use of code to reduce opportunism via centralization.

Risk, however, never truly disappears on the dark market. Certainly in 2013, before a peer-to-peer version of the escrow system was implemented on a dark market, any arrangement that protected buyers from site administrators exposed them to seller fraud (via fake vendor accounts, for example) and vice versa. Protection from vendors via a centralized system simply meant that buyers were asked to trust the site administrator, who could abscond with the money they had placed in escrow. Moreover, some vendors refused to use the system, which shifted the risk back to the buyer (Comments on Threatlevel blog 2013; for successful uses of the escrow system see Van Hout and Bingham 2013b).[4] In sociological terms, however, the imbalance between

buyers and sellers led to the organic emergence of a mainstay of a stable market—a "status hierarchy" (Fligstein 2001). Recognizing that buyer protections alone did not guarantee stability, DPR's policy changes facilitated the emergence of a status hierarchy.

Almost a year after the site went online, DPR replaced the original flat rate commission with a tiered commission structure and introduced "Stealth Mode" to meet the needs of the site's "superstar vendor(s)" who felt they were "at particular risk of becoming a target for law enforcement" (Ulbricht criminal complaint 2013, 18). Under the new arrangement, sellers paid a 10% commission on the first 50 dollars and only 1.5% on sales over 1000 dollars (Christin 2012). Stealth mode, in turn, meant that buyers could only access a vendor's listings if they had received a specific URL from that vendor. Both changes facilitated volume transactions and, taken together, anticipated interest by nonparticipating drug vendors who might consider moving some of their operations online. Even though Silk Road was in the Dark Web, the new policy revealed, it had been a public market all along where risks were distributed evenly among sellers. Now small vendors and new entrants were exposed to law enforcement browsing anonymously.

When a user complained about the hike in Silk Road commission after the introduction of Stealth Mode, DPR's authoritarian tone stood in stark contrast to his model customer service persona. "Whether you like it or not, I am the captain of this ship," DPR wrote. "You are here voluntarily, and if you don't like the rules of the game, or you don't trust your captain, you can get off the boat" (Ulbricht criminal complaint 2013, 18). Voluntarism, then, simply meant that buyers had the option not to participate in a website whose basic framework they were not to influence. Silk Road was becoming as hierarchical and authoritarian as a version of the real world where those who do not like the direction of their countries are encouraged to leave. If, however, the test of the radical libertarian challenge was a stable market, the site appeared to be on its way.

The reputation mechanism

If the escrow system diminished the risk of buyers not getting anything for their money, the reputation mechanism regulated the relationship between market participants by addressing buyer concerns about product safety and product quality. Buying drugs from strangers was risky, a common concern, because they could be selling poison. On the other hand, when buyers are able to leave feedback, vendors acquire a reputation, which makes them "accountable" (Van Hout and Bingham 2013a). Pioneered by eBay as a form of "community enforcement," the possibility of feedback promised accountability even under conditions of anonymity (Goldsmith and Wu 2008).

Feedback on Silk Road consisted of three fields—a rating, a textual description of the feedback, and the age of the feedback (Christin 2012). The reputation mechanism did its job when information-empowered buyers and sellers were sensitive to consumer expectations, offering, for example, Halloween and Christmas specials (Martin 2014). It failed when vendors—aided by the site's robust anonymity protections—made purchases from themselves and left themselves positive feedback (O'Neill 2014). Reputation mechanisms are weak governance structures, precisely because they are easily gamed (Goldman 2011).

Although the site's anonymity protections undermined every aspect of DPR's rules, the first important change to Silk Road's policies concerned the inadequacy of the reputation system as a source of social control. Just 5 months into the operation of the site, DPR realized that he was unable to deter a vendor who threatened to send carcinogenic and poisonous substances. Neither the feedback mechanism nor pulling down his account made a difference; the vendor would just "create a new account as soon as they got bad feedback" (DPR 2011). "This was shocking and horrifying to us," DPR wrote, revealing a true romance with free markets and reasonable users, despite his shrewd attempts at institution building (DPR 2011). When he reopened new seller registration, he found a suitably agorist solution: He made new accounts scarce by auctioning them off, hoping that this would deter recalcitrant users from opening one new account after another. Yet the question arose of whether Silk Road was the adherent organization that DPR had imagined, where the rules were indeed self-enforcing.

Regardless of the gradual erosion of the original institutional arrangements, buyers compared Silk Road favorably to the street trade. At the center of the comparison lay the matter of consumer rights. In contrast to the multiple vendors and product reviews present on Amazon or eBay, a participant explained, the street market is "based on a 'take it or leave it'" approach which "gives no rights to a buyer" (quoted in Van Hout and Bingham 2013b, 526). Participants regularly compared Silk Road to mainstream e-commerce sites or physical stores, rewarding vendors when they behaved like mainstream sellers, and cutting them slack when they did not. "[V]endor did not even address the fact that i was unhappy with my order but w.e. this isnt Walmart i guess," a user commented with resignation as he posted a 5/5 rating (Ulbricht criminal complaint 2013, Exhibit B). Site participants forgave the shortcomings of the market because they understood that they were getting something remarkable: the experience of a legitimate market on the Dark Web.

Protecting the market from the state

As the site's logo—"Silk Road anonymous market"—indicates, Silk Road promised to put market participants beyond the reach of the state. Significantly, the challenge was not simply to operate a market without relying on the state, but to do so while actively hiding from it. Anonymity on Silk Road was understood purely as a solution against government intrusion into the market and was enshrined in the site's architecture. "Now it is profitable to throw off one's chains," DPR gushed on an internal forum on March 20, 2012, "with amazing crypto technology reducing the risk of doing so dramatically" (quoted in Greenberg 2013, 6). Yet if anonymizing the one-way process of information submission, à la WikiLeaks, was an arduous task, anonymizing market transactions among thousands of users was a task of mind-boggling complexity whose contours can only be outlined here (Zajácz 2013). The three focal points of the discussion that follows—access, transaction, and shipment—direct our attention to the intersections between virtual and real space, the least secure spots of the operation of a website. For all of its efforts to displace the state, we show in the following that Silk Road remained dependent on the infrastructure maintained by the liberal state.

Access refers to the connection between users sitting at computers and servers in the physical world hosting a website. If a site operates anonymously, neither the location of the servers nor the identity and location of any user should be available to interested parties. With user competence about Internet security out of his hands, DPR focused his efforts instead on (1) blurring the link between the sender and receiver by directing users to rely on the Tor network and (2) hiding the location of Silk Road's servers.

Tor is an anonymizing computer relay that fragments the link between computers accessing or hosting websites by routing the information exchange through several Tor nodes. In effect, Tor severs the connection between the computer and its Internet protocol, or IP address, which can be used to determine its physical location (Ulbricht criminal complaint 2013). When a site operates within the Dark Web as "a Tor hidden service," its URL does not map to a known IP address, but uses a pseudo top-level domain, onion, that only the Tor browser can reach (Christin 2012). The origin, destination, and date of transmission of messages are hidden behind layers of encryption that Tor relays peel off like layers of an onion. To the destination computer, the last node of the relay network appears as the source of the message. According to the FBI, using Tor in connection with a Virtual Private Network (VPN) makes it "practically impossible" to locate computers requesting information from websites or those hosting the sites (Ulbricht criminal complaint 2013).

The importance of Silk Road's servers cannot be overstated. Once the FBI found a server in Iceland, it was able to obtain vendor postings, records of Silk Road sales, and private messages between users, not to mention the computer code used to operate the website (Declaration of Christopher Tarbell 2014). Moreover, since the source code used on the original Silk Road had not been distributed to multiple servers, any attempt to revive the site had to start from the ground up.

Not surprisingly, therefore, one of the most discussed aspects of the Silk Road prosecution was how the FBI located the site's servers. Investigators explained their access with DPR's security lapses, citing evidence for recurring problems with "IP address leaks" at Silk Road. Tor can only hide an IP address if the applications running on the computer are properly configured for that purpose. The FBI noticed a single IP address that was not associated with any publicly listed Tor node (Declaration of Christopher Tarbell 2014). DPR did access the server via a virtual private network, but the FBI obtained a subpoena for the records of the server-hosting company that DPR rented the VPN from (Ulbricht criminal complaint 2013). Ulbricht's defense was not able to question the FBI at trial about this matter, nor could it advance its suspicion that the organization received help from the National Security Agency. As a result, journalists are still in doubt about how the server was found (Jeong 2015).

Since Silk Road was a market, security of access was hardly the end of DPR's challenges. A transaction must also take place that involves offering and accepting payment. A site operates anonymously if it severs the link between the buyer who parts with a state-backed currency and the seller who takes home payment in a state-backed currency. Unlike its predecessors, Silk Road did not need to rely on credit cards or PayPal. Instead, it required Bitcoin, a peer-to-peer financial instrument not backed by a central authority, which the FBI calls "as anonymous as cash" (Ulbricht criminal complaint 2013, 6). Its hitherto anonymous creator had designed the "blockchain," the equivalent of a virtual public ledger, to prevent people from using the same Bitcoin more than once. At once anonymous and transparent, the blockchain reveals all transactions, but none can be linked to an individual (Pathe 2014). Because it cannot be traced, blocked, or confiscated, it appears to be beyond the reach of the state.

If this sounds too good to be true, it is because transparency does work against anonymity. Since the history of all transactions is publicly available, law enforcement

employs network analysis techniques to map sets of public encryption keys to individual Bitcoin users (Christin 2012). To counter this vulnerability, Bitcoin.org warns that addresses should only be used once. Rather than burdening users with more security measures, DPR used a Bitcoin tumbler instead, which sent individual transactions through a series of dummy transactions to disguise the link between buyers and sellers. As a result, no one could use the blockchain to follow the money trail even if the buyer's and the vendor's Bitcoin addresses were both known (Ulbricht criminal complaint 2013).

After a user completed the transaction, the drugs purchased online needed to arrive via some type of transportation, a process identified here as shipment. As much as DPR thought that he created a truly free market hidden from the state apparatus, Silk Road was dependent on the infrastructure of the liberal state. Thus, the site offered advice on how to avoid attracting the attention of postal and customs authorities. Silk Road's Sellers' Guide and discussion forums were awash in counter-interdiction strategies, from vacuum-sealing packages to business-style printed envelopes (Martin 2014). Skills in concealment were essential to the reputation of a vendor—"Excellent stealth!" "Packaging/stealth was dead on 5/5 A+++"—and those who possessed the necessary stealth were rewarded with increased business (cited in Martin 2014, 360, Figure 1). Such comments empowered the online community against the state: While stealth did not come naturally, these forums made clear, it could be mastered.

Yet no aspect of the site's operation was less secure than shipment. Technologies based on a relay logic were essential for the security of access and transactions alike (law enforcement agencies received information about the use of Bitcoins only after they had leads on the identities of Silk Road participants), and their strength masked DPR's relative lack of familiarity with security protocols (Bolles criminal complaint 2013). Shipment, however, did not benefit from relay technologies and required a more wide-ranging technical background than was initially apparent, even as the size of the market magnified the dangers of lax security procedures.

Silk Road disrupted traditional models of the drug trade: simplifying both access to stock and the process of selling widened the seller base. On the street, dealers generally acquire stock on credit, which necessitates on-the-ground connections and relationships of trust with middle-level drug dealers and/or importers. By contrast, Silk Road operated like "a virtual cash-and-carry business," where almost anyone could access stock (Aldridge and Décary-Hétu 2014, 17). For newly minted vendors, however, DPR's Sellers' Guide was not detailed enough to prevent all slip-ups, nor could it be enforced. Sooner or later, someone was going to put a return address on a package, as a medical student eventually did, leading law enforcement to a commercial post office box she had rented using her driver's license and vehicle registration for identification (Bolles complaint 2013). Every account seized like this resulted in information for law enforcement and the possibility of turning account owners into informants. Users, who referred to Silk Road as "a safer way of sourcing," seemed to be unaware of these dangers (Van Hout and Bingham 2013a, 387). As law enforcement worked to bring down the site, problems with the security of personal information opened Silk Road to internal threats as well.

Protecting site administration from extortion?

Silk Road's inability to deliver on its promise of hiding its users from the state was the most immediate cause of its downfall. For the purpose of examining market-based resistance, however, the immediate cause is less important than DPR's failure to stem the tide of opportunism. DPR anticipated problems like fraud between users, but seemed hard-pressed to imagine that users would endanger the operation of the site itself. When theft and blackmail emerged as threats, anonymity brought DPR face-to-face with the problem of enforcement, which, at minimum, will haunt any libertarian electronic market in a nonlibertarian political economy and, perhaps, any electronic market with any rules.

While hapless vendors simply forgot to delete their clients' contact information, the opportunists went straight to blackmail, threatening to reveal that Silk Road's promises of user protection were hollow. A user by the screen name of "Friendly Chemist," for example, threatened to disclose the personal information of site participants he had obtained by hacking into the account of a vendor. Friendly Chemist showed DPR a sample of the 5000 user names and addresses and demanded $500,000 in return for his silence (Ulbricht criminal complaint 2013). "[W]hat do u … think will happen if thousands of user names, ordr [sic] amounts, addresses get leaked?" Friendly Chemist asked DPR. "All those people will leave sr [Silk Road] and be scared to use it again," he answered his own question (21). Personal information was even more sensitive on Silk Road than in legitimate e-commerce, and the information imbalance tempted opportunism. Site administration was an obvious target, since it had the most incentive to keep the vulnerability of the site secret. Instances of sellers blackmailing buyers whose personal information they held have also been documented (*The Economist* 2016).

This was not the first attempt at extortion, nor would it be the last. "I've been busting my ass every god damn day for over two years to make this place what it is," a

frustrated DPR complained to a federal agent in the guise of a user threatening him. "Somehow psychotic people still turn up at my doorstep. I've been scammed, I've been stolen from, I've been hacked, I've had threats made against the site, I've had threats made against the community, and now, thanks to you, I've had threats made against my life" (Department of Justice to Judge Katherine B. Forrest 2015, 2). Silk Road appeared to be less and less of an adherent organization, where internal norms and rules are so widely accepted that members' cooperation is assured.

Extortion was a problem identified by technolibertarian activists themselves in the 1990s. In debating a hypothetical case, where encryption allowed a blackmailer to commit the perfect crime, activists involved with the Cypherpunk mailing list made five recommendations: Do not read unsolicited mail, never pay, assume that the threat will be carried out ("If it is blackmail, tell everything before the blackmailer can"), make your life so secretive that you do not become a target of extortion, and finally, rely on police competence in finding other kinds of clues (Brin 1999, 228–29).

How the libertarian framework would address the two instances of malfeasance that blackmail on Silk Road has revealed deserves a more extended treatment. The Cypherpunks' advice clearly does not contemplate a dark market operator who has the integrity of his enterprise to look after. DPR could not very well publish the information of the 5000 victims before Friendly Chemist, nor could he even warn the community that such disclosure was coming without leading to the collapse of his site. And what about the users whose personal information was on the line? The recommendations just listed presuppose a minor infraction, which can be revealed publicly, and a functioning state where it is safe to reveal personal information and one can turn to the police. But should a person disclose his or her information on the dark market in order to beat a blackmailer to it? Once this information was made available, the common libertarian advice with regard to property (returning it to its owner) falls short. Information is a unique type of property, if it is property at all: The victim never truly loses it, but law enforcement may also secure it.

DPR now reached the point that led eBay's founder, Pierre Omidyar, to the conviction that the philosophy of a self-governing community "didn't really scale up" (Goldsmith and Wu 2008, 134). DPR had tried to prevent opportunism by employing a staff of 10 to monitor user activity on the site, a type of limited surveillance, and to resolve disputes. He gave them authority to remove user postings and reset passwords, but inadvertently also entrusted federal agents with admin privileges (Greenberg 2015; Mullin 2015a, Ulbricht criminal complaint 2013). The most serious tool of enforcement at Silk Road was the removal of user accounts. In physical markets, where personal relations and community norms are most likely to work, market organizers may successfully deny people the ability to participate, captured by the medieval concept of "banishment" (Johnson and Post 1996, 1390). But what recourse did a site with anonymous participants have against theft or extortion?

Involving the court system or law enforcement was, of course, both infeasible and philosophically abhorrent to DPR. One could always pay, as DPR did, when he agreed to a weekly ransom of $50,000 to hackers who discovered a vulnerability of the site (Government exhibit 241 in Mullin 2015e). A large theft of Bitcoins, committed by a federal agent, and Friendly Chemist's attempt at blackmail, on the other hand, prompted discussions inside Silk Road about what constituted a serious enough offense for executing someone. DPR hoped to recover the money by beating up the thief, but the idea was quickly dismissed in favor of the more violent norms of the drug trade (Memorandum of law in opposition to the defendant's motions in limine 2013).

Speaking like a system builder, DPR explained the need for violence for protecting the integrity of Silk Road. "Necessities like this do happen from time to time to a person in my position," he commented (Ulbricht criminal complaint 2013, 22). No longer did his actions seem voluntary to him. When presented with the images of a hit victim, which later turned out to be fabricated, DPR replied that he did not have any other choice (Segal 2014). "We are all players in something that has grown way beyond any one of us," he noted on July 31, 2012, on the Silk Road website, in awe of his own creation (quoted in Greenberg 2013, 2).

DPR's use of commissioned killings, however, was hardly justified under a libertarian framework. Rothbard has sketched the contours of a libertarian legal order, which recognized only two parties to a dispute—the victim and the alleged criminal—and warned against crimes against an ill-defined "society" (1982). He would have recognized Friendly Chemist's attempt at extortion as a crime and DPR as its victim, since, for him, the overt and immediate threat of property invasion was equivalent to the invasion itself. But DPR's intended punishment was not proportional to the crime. If DPR lost money, he was entitled to money, but had no claim on the life of the perpetrator.

DPR's decision to use violence was only the beginning of his problems. "I need [Friendly Chemist's] real world identity, so I can threaten him with violence," he wrote to an associate (Mullin 2015c, para. 2). However, Silk Road's anonymity protections thwarted his attempts to identify his targets and to tell whether his orders were

carried out. In one case, DPR ordered a hit from an undercover agent without being aware that he was talking to the FBI. After the "hit," he was presented with a staged picture of a murder that he had no way to verify. He also received pictures of the hit on Friendly Chemist, but the FBI was unable to find any evidence of a homicide in the Canadian town at the time of the hit (Ulbricht criminal complaint 2013). Just why Friendly Chemist chose not to disclose the information he had obtained remains to be discovered. It is apparent, however, that a crime boss who cannot tell whether anybody complies with his orders cannot deter opportunism.

Conclusion

My interest here lies in the deployment of anonymizing technologies for challenging state power. Silk Road was a credible challenge to state power in spite of—rather than because of—DPR's brand of libertarianism. DPR's instinctual override of the libertarian vision led to a replication of state functions: making law and attempts to use force to give effect to his rules (Strange 1996). At any given point in time, therefore, Silk Road was engaged both in community building and in something akin to state building. While the community forum and the reputation mechanism facilitated the norms essential for social relations, centralization, backed by code, also worked to prevent opportunism on the site. The stability of Silk Road can be traced to the balance DPR achieved between buyer protection and policies fostering the emergence of a status hierarchy, which benefited the largest sellers. But this was an online marketplace, and DPR's faith in anonymizing technologies ignored their risks: The site's anonymity protections favored sellers over buyers, and market participants over site administration.

Judged by DPR's goals, however, Silk Road was far from a sustainable challenge to state power. While anonymous nonmarket activities would be less likely to engender opportunism, physical—by definition, not anonymous—markets would not produce an inability to enforce market rules. Yet Silk Road was far from an adherent organization that could do without enforcement. Due to DPR's one-sided understanding of online anonymity, both internal and external security suffered. On the one hand, strong anonymity protections coupled with a heightened fear of privacy violations made the site a breeding ground for blackmail, while Silk Road's subcultural norms were not strong enough to keep this behavior in check. Even if all blackmailers and thieves were federal agents (a fact we cannot ascertain), the very threat of blackmail proved to be corrosive. Not only did thoughts of coercion taint Silk Road's ideals, DPR's attempts at enforcement also foundered on the site's anonymity protections. On the other hand, DPR's libertarian commitments fostered a patchy deployment of code, resulting in a site that eschewed automated surveillance. As a result, DPR could not even tell whether any of his associates worked for law enforcement. That such a clear effort at introducing order into the black market failed demonstrates that the opportunism facilitated by anonymity threatens crypto-anarchist markets as much as it does the state.

Strikingly, the state figured prominently in the market, which was defined in opposition to it. In addition to providing the physical infrastructure for shipment, the state served as a model for both site administration and users. Participants' experience of "consumer rights" provides a fruitful avenue for researchers interested in the role of the state in the 21st-century networked world. Just how expansive did site participants image this "right" to be? If market participants see being fleeced as the price of convenient access to a variety of illegal products, is blackmail also compatible with consumer satisfaction? Should blackmail prove unacceptable, what, if any, level of surveillance are participants willing to accept in return for minimizing the dangers of internal crime? The dark market, it should be apparent by now, is a mirror image of real space, where debates about surveillance parallel those present in academic journals and in the halls of Congress.

For activists sketching the contours of a networked world that excludes the state, the problem of anonymity is worth a second look. If technological solutions to prevent malfeasance prove insufficient, do the current imperfect enforcement mechanisms available online facilitate stability? Could the technolibertarian utopia replace the power of the state with "Internet justice," that is, the power of a technical elite who "command the authority to enforce norms by appeal to technical power" (Coleman 2014, 190)? Dark markets face not only the problem of enforcement, but also the problem of legitimating whatever enforcement mechanism seems to be working. And if enforcement does improve, what else would be required to make this world livable?

For academics, the case of a site that took on state functions represents an extreme position of limited, manual surveillance against which all other alternatives could be evaluated. What is the relationship between surveillance and security? What role, in particular, does the surveillance capability of the state play in its legitimacy? It is only by considering the development of policy debates alongside debates in the Dark Web and other types of activist communities, going back to the 1990s Cypherpunk mailing list, that we can map the conceptual landscape surrounding government surveillance online. These debates, in turn, hold the key to the intertwined histories of government policies and the deployment of

privacy-enhancing technologies that characterize the present moment.

Evaluating the developing mixture of security and anonymity protections will be a complex task. After all, as Benkler advises, the purpose of anarchistic projects is to build a degree of freedom into the world defined by powerful states and markets. Morally ambiguous though they may be, pervasive illegality and radical resistance "nonetheless grab, and sometimes genuinely facilitate, degrees of freedom" (Benkler 2013, 247). Silk Road did not rely on state power for enforcement and was not otherwise coercive. Do dark markets, where site operators desire coercive power but cannot use it, facilitate freedom? Are they preferable to dark markets where the objective is purely to fleece participants? DPR, of course, also believed that Silk Road was about freedom—freedom from government power and the freedom of market forces—even as he restricted the freedom of site participants. How do competing conceptions of freedom figure into the evaluation of state actions and activist resistance? And what other values need attention along with the freedom that dark markets grab? If a complex online environment without surveillance or identification is a world of opportunism, then the case could serve as a reference point for addressing the balance between freedom and competing values when debating acceptable levels of government surveillance online.

Notes

1. Silk Road itself was a criminal enterprise. Thus, the use of the term "crime" within the world of Silk Road—crime from DPR's perspective——should be seen in that light.
2. eBay did not rely on cryptographic anonymity to hide from the state. Rather, its anonymity was the default mode of the early public Internet. Market participants interacted with strangers and site administration had no idea who the participants were, either. Omidyar preferred to let the market run itself until he realized that they had to move toward identification and surveillance.
3. A copy of the Seller's Guide is in the author's possession; it is no longer available online.
4. The comments, along with the user's screen name, are in the author's possession; they are no longer available online.

Acknowledgments

I thank John Durham Peters, Tim Havens, and the three anonymous reviewers at this journal for their helpful comments and suggestions.

References

Aldridge, J., and D. Décary-Hétu. 2014. Not an "eBay for drugs:" The cryptomarket "Silk Road" as a paradigm shifting criminal innovation. http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2436643 (accessed July 2016).

Anderson, T. J. L., and P. J. Hill. 1975. The evolution of property rights: A study of the American West. *Journal of Law and Economics* 18 (1):163–79.

Benkler, Y. 2013. Practical anarchism: Peer mutualism, market power, and the fallible state. *Politics & Society* 41 (2):213–251.

Block, F. 1990. *Postindustrial possibilities*. Berkeley, CA: University of California Press.

Bolles criminal complaint. 2013. Complaint, *United States of America v. Olivia Louise Bolles*. 6:13-mj-1614. (M.D. Fla., 2013).

Brin, D. 1999. *The transparent society*. Reading, MA: Perseus Books.

Christin, N. 2012. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *WWW'13: Proceedings of the 22nd International conference on the World Wide Web*, 213–23. New York, NY: ACM. http://dl.acm.org/citation.cfm?id=2488408 (accessed May 2015).

Coleman, G. 2014. *Anonymous*. New York, NY: Verso.

Connolly, R. 2013. Trust in commercial and personal transactions in the digital age. In *Oxford handbook of Internet studies*, ed. W., Dutton, 262–78. New York, NY: Oxford.

Declaration of Christopher Tarbell. 2014. Declaration of Christopher Tarbell, *United States of America v. Ross William Ulbricht*. S1 14 Cr. 68 (KBF) (S.D.N.Y., 2014).

Department of Justice to Judge Katherine B. Forrest. 2015, February 1. Re: *United States v. Ross William Ulbricht*, S1 14 Cr. 68 (KBF) 260628594-Ulbricht-post-trial-unsealed-filings.pdf (accessed May 2015).

Dread Pirate Roberts. 2011, July 1. New seller accounts. http://antilop.cc/sr/users/dpr/html/dpr_posts_page_44_start_645.html (accessed October 3, 2016).

Dread Pirate Roberts. 2013. A few words from the Dread Pirate Roberts. http://mainstreamlos.tumblr.com/post/29329382663/a-few-words-from-the-dread-pirate-roberts (accessed July 2016).

Doherty, B. 2007. *Radicals for capitalism*. New York, NY: Public Affairs.

Eisenhardt, K. M. 1989. Building theories from case study research. *Academy of Management Review* 14 (4):532–50.

Fligstein, N. 2001. *The architecture of markets*. Princeton, NJ: Princeton University Press.

Freeh, L. 1997. Statement of Louis J. Freeh, Director, Federal Bureau of Investigation before the Senate Judiciary Committee, July 9. https://epic.org/crypto/legislation/freeh_797.html (accessed October 3, 2016).

Froomkin, A. M. 1999. Legal issues in anonymity and pseudonymity. *The Information Society* 15 (2):113–27.

Geertz, C. 1973. *The interpretation of cultures*. New York, NY: Basic Books.

Goldman, E. 2011. Regulating reputation. In *The reputation society*, ed. H. Masum and M. Tovey, 51–73. Cambridge, MA: MIT Press.

Goldsmith, J., and T. Wu. 2008. *Who controls the Internet?* New York, NY: Oxford University Press.

Granovetter, M. 1985. Economic action and social structure: The problem of embeddedness. *American Journal of Sociology* 91 (3):481–510.

Greenberg, A. 2013. Collected quotations of the Dread Pirate Roberts, founder of underground drug site. *Forbes*, April 29. http://

www.forbes.com/sites/andygreenberg/2013/04/29/collected-quotations-of-the-dread-pirate-roberts-founder-of-the-drug-site-silk-road-and-radical-libertarian (accessed December 2015).
Greenberg, A. 2015. Silk Road defense says Ulbricht was framed by the "real" Dread Pirate Roberts *Wired*, January 13. http://www.wired.com/2015/01/isilk-road-trial-opening-statements (accessed July 2016).
Grossman, L., and J. Newton-Small. 2013. The Deep Web. *Time*, 182 (20):26–34. Available at EBSCO Business Source Complete. Accessed November 10, 2016.
Guttentag, D. 2015. Airbnb: Disruptive innovation and the rise of an informal tourism accommodation sector. *Current Issues in Tourism* 18:1192–217.
Jeong, S. 2015. How Ross Ulbricht's defense was derailed. *Forbes*, February 3. http://www.forbes.com/sites/sarahjeong/2015/02/03/the-silk-road-trial-that-wasnt (accessed, May 2015).
Johnson, D. R., and D. Post. 1996. Law and borders: The rise of law in cyberspace. *Stanford Law Review* 48:1367–402.
Katyal, K. K. 2004. Digital architecture as crime control. *Yale Law Journal* 112:2261–89.
Kling, R., Y. Lee, A. Teich, and M. S. Frankel. 1999. Assessing anonymous communication on the Internet: policy deliberations. *The Information Society* 15 (2):79–90.
Konkin, S. E. 1983. New libertarian manifesto. http://docs.evancarroll.com/politics/theory/agorism/nlm.pdf (accessed September 30, 2016).
Kozinski, A. 2015. The two faces of anonymity. *Capital University Law Review* 43:1–17.
Kruse, E. 2005. Endogenous property rights in economics and the case of the radio spectrum. In *Law and economics*, ed. M. Oppenheimer and N. Mercuro, 161–98. Armonk, NY: M. E. Sharpe.
Lessig, L. 2006. *Code 2.0*. New York, NY: Basic Books.
Levy, S. 1996. Crypto rebels. In *High noon on the electronic frontier*, ed. P. Ludlow, 185–205. Cambridge, MA: MIT Press.
Martin, J. 2014. Lost on the Silk Road: Online drug distribution and the "cryptomarket." *Criminology and Criminal Justice* 14 (3):351–67.
Marx, G. T. 1999. What's in a name? Some reflections on the sociology of anonymity. *The Information Society* 15 (2):99–112.
May, T. 1992. The crypto-anarchist manifesto. http://www.activism.net/cypherpunk/crypto-anarchy.html (accessed September 30, 2016).
Memorandum of law in opposition to the defendant's motions in limine. 2013. Exhibit A. *United States of America v. Ross Ulbricht*. S1 14 Cr. 68 (KBF) (S.D.N.Y., 2013).
Mullin, J. 2015a. At Silk Road trial federal agent explains how he trapped Ulbricht. *Ars Technica*, January 15. http://arstechnica.com/tech-policy/2015/01/silk-road-trial-federal-agent-explains-how-he-trapped-ulbricht/ (accessed May 2015).
Mullin, J. 2015b. "I have secrets": Ross Ulbricht's private journal shows Silk Road's birth. *Ars Technica*, January 21. http://arstechnica.com/tech-policy/2015/01/silk-road-trial-fbi-reveals-whats-on-ross-ulbrichts-computer-in-open-court (accessed May 2015).
Mullin, J. 2015c. Silk Road trial: How the Dread Pirate Roberts embraced violence. *Ars Technica*, January 29. http://arstechnica.com/tech-policy/2015/01/silk-road-trial-how-the-dread-pirate-roberts-embraced-violence (accessed July 2016).
Mullin, J. 2015d. Silk Road prosecutors complete the bizarre DPR murder-for-hire story. *Ars Technica*, February 2. http://arstechnica.com/tech-policy/2015/02/silk-road-prosecutors-complete-their-bizarre-murder-for-hire-story (accessed May 2015).
Mullin, J. 2015e. Drugs, chatlogs, and fake IDs: Images from the Silk Road trial. *Ars Technica*, February 5. http://arstechnica.com/tech-policy/2015/02/how-to-build-a-clandestine-drug-lab-images-from-the-silk-road-trial (accessed May 2015).
North, D. C., J. J. Wallis, and B. R. Weingast. 2009. *Violence and social orders*. Cambridge. UK: Cambridge University Press.
O'Neill, P. H. 2014. The final confessions of a Silk Road kingpin. *The Daily Dot*, January 22. http://www.dailydot.com/crime/silk-road-confession-steven-sadler-nod (accessed May 2015).
Pathe, S. 2014. Gamblers wage millions on unregulated Bitcoin betting sites. *PBS.org*, March 2. http://www.pbs.org/newshour/updates/bitcoin-gambling-sites-fly-regulatory-radar (accessed December 2014).
Rothbard, M. N. 1978. *For a new liberty* (2nd rev. ed.). San Francisco, CA: Fox and Wilkins.
Rothbard, M. N. 1982. *The ethics of liberty*. Atlantic Highlands, NJ: Humanities Press.
Segal, D. 2014. Eagle Scout. Idealist. Drug trafficker? *The New York Times*, January 18. http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html (accessed July 2016).
Silk Road Charter. 2013. Available at https://www.reddit.com/r/SilkRoad/comments/1d5f0q/silk_road_charter/ (accessed November 10, 2016).
Strange, S. 1996. *The retreat of the state*. Cambridge, UK: Cambridge University Press.
The Economist. 2016. Shedding light on the Dark Web. July 15, 50–52.
Trubek, D. M. 1972. Max Weber on law and the rise of capitalism. *Wisconsin Law Review* 1972 (3):720–53.
Turow, J. 1997. *Breaking up America*. Chicago, IL: University of Chicago Press.
Ulbricht criminal complaint. 2013. Complaint, United States of America v. Ross William Ulbricht. S1 14 Cr. 68 (KBF) (S.D. N.Y., 2013). https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf (accessed July 2016).
Van Hout, M. C., and T. Bingham. 2013a. Silk Road, the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy* 24 (5):385–91.
Van Hout, M. C., and T. Bingham. 2013b. Surfing the Silk Road: A study of users' experiences. *International Journal of Drug Policy* 24 (6):524–29.
Van Hout, M. C., and T. Bingham. 2014. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy* 25 (2):183–89.
Weber, M. 1968. *Economy and society*. New York, NY: Bedminster Press.
Williamson, O. E. 1975. *Markets and hierarchies, analysis and antitrust implications: a study in the economics of internal organization*. New York, NY: Free Press.
Zajácz, R. 2013. WikiLeaks and the problem of anonymity: A network control perspective. *Media, Culture and Society* 35 (4):487–503.