UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	14 Cr. 68 (KBF)
- against -	:	(Electronically Filed)
ROSS ULBRICHT,	:	
Defendant.	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT ROSS ULBRICHT'S PRE-TRIAL MOTIONS CHALLENGING THE FACE OF THE INDICTMENT

JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Whitney Schlimbach

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER

Introduction

This Memorandum of Law is submitted on behalf of defendant Ross Ulbricht in support of his pretrial motions addressing the face of the Indictment, which charges Mr. Ulbricht with Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances, in violation of 21 U.S.C. §846 (Count One), Continuing Criminal Enterprise, in violation of 21 U.S.C. §848(a) (Count Two), Conspiracy to Commit Fraud and Related Activity in Connection with Computers, in violation of 18 U.S.C. §1030(b) (Count Three), and Money Laundering, in violation of 18 U.S.C. §1956(h) (Count Four). For the reasons set forth below, it is respectfully submitted that all of the charges against Mr. Ulbricht should be dismissed.

As detailed below, the Indictment advances an unprecedented and extraordinarily expansive theory of vicarious liability under certain statutes – particularly 21 U.S.C. §§846 & 848, and 18 U.S.C. §1030(a)(2), that would impose criminal responsibility upon Mr. Ulbricht based on the conduct, knowledge, and intent of others.

There are several fatal flaws in that approach:

(1) as review of the case law establishes, the statutes do not cover the conduct alleged against Mr. Ulbricht. Nor were those statutes intended to cover such conduct, and, indeed, they have never been applied to it before. Analogously, no landlord has been prosecuted under the federal controlled substances statutes for renting an apartment to a know drug seller. Nor has any internet service provider been prosecuted because users of the service engage in illegal transactions using the provider's internet service;

(2) to the extent Mr. Ulbricht's alleged conduct is even arguably covered by the

statutes, two rules of statutory construction – the rule of lenity, and the doctrine of constitutional avoidance – restrict the ambit of the statutes, and render them inapplicable here;

(3) 47 U.S.C. §230, provides absolute civil immunity to a "provider or user of an interactive computer service" by declaring that such provider or user shall not "be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. §230(c)(1). While that immunity is expressly not intended to "impair the enforcement of . . . any [] Federal criminal statute[,], *see* 47 U.S.C. §230(e)(1), it nevertheless informs the discussion with respect to not only internet policy regarding liability for the conduct of others, but also the application of the rule of lenity and the doctrine of constitutional avoidance; and

(4) if, assuming *arguendo* the statutes apply to Mr. Ulbricht's alleged conduct, they fail to provide adequate notice of what conduct is proscribed and/or subject to arbitrary and discriminatory enforcement, and therefore is unconstitutionally vague as applied to Mr. Ulbricht in this case. Moreover, to the extent the alleged conduct involves protected speech, the statutes are unconstitutionally overbroad, and invalid in this case.

Also, §1030 suffers from a specific additional vagueness because the pivotal term "access without authorization" in §1030(a)(2)(C) is undefined, thereby potentially encompassing conduct by others for which Mr. Ulbricht lacks any notice of criminality, much less knowledge and intent. That vagueness is amplified by the attenuation of Mr. Ulbricht from any conduct that a

purchaser or user of software might perform that could arguably violate §1030.

In addition, Count Four, which alleges money laundering, is defective because it fails to allege sufficiently an essential element of the offense – that Mr. Ulbricht engaged in, or conspired to engage in, "financial transactions" under §§1956(a)(1)(A)(i) or (B)(i) – as Bitcoin, the alleged "payment system that served to facilitate the illegal commerce conducted on the site," *see* Indictment, at ¶ 18 (p. 7), does not constitute either "funds" [in §1956(c)(4)(A)(i)] or a "monetary instrument[]" [defined in §1956(c)(5)], either of which is a necessary component of "financial transaction" [defined in §1956(c)(4)].

Accordingly, for all the reasons set forth above and detailed below, it is respectfully submitted that the Indictment should be dismissed.

Statement of the Facts

As noted **ante**, the Indictment charges Mr. Ulbricht with devising and operating Silk Road, an "underground website" allegedly "designed to enable users across the world to buy and sell illegal drugs and other illicit goods and services anonymously and outside the reach of law enforcement." Indictment at ¶ 1. Mr. Ulbricht is alleged to have owned and operated the site "with the assistance of various paid employees who he managed and supervised" from in or about January 2011 through in or about October 2013, when Silk Road was shut down by law enforcement. *Id*., at ¶¶ 2, 3.

According to the Indictment, during the period that the Silk Road website was operational it "emerged as the most sophisticated and extensive criminal marketplace on the Internet" and was "used by several thousand drug dealers and unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to well over a hundred

thousand buyers worldwide." *Id*., at ¶ 2.

The website is also alleged to have been used "to launder hundreds of millions of dollars from these illegal transactions." *Id*. The Indictment further alleges that Mr. Ulbricht "reaped commissions worth tens of millions of dollars" from the many sales conducted on his website, and that he "solicit[ed] the murder-for-hire of several individuals he believed posed a threat" to Silk Road in order to "protect his criminal enterprise and the illegal proceeds it generated." *Id.*, at ¶¶ 3, 4.

The Indictment includes four counts:

- Count One charges Mr. Ulbricht with a narcotics trafficking conspiracy, in violation of 21 U.S.C. §846, for his alleged role in providing a platform for drug dealers to buy and sell drugs, including heroin, cocaine, lysergic acid diethyamide ("LSD"), and methanthetamine via the Internet. Count One alleges that as a part and object of that conspiracy Mr. Ulbricht and others (1) distributed and possessed with the intent to distribute controlled substances in violation of 21 U.S.C. §841(a)(1); (2) delivered, distributed, and dispensed controlled substances "by means of the Internet" and aided and abetted that activity, in violation of 21 U.S.C. §841(h); and (3) knowingly and intentionally "used a communication facility in committing and in causing and facilitating the commission" of felonies pursuant to 21 U.S.C. §§841, 846, 952, 960, and 963, and in violation of 21 U.S.C. §843(b) (*see* Indictment at ¶¶ 6-9);
- Count Two charges Mr. Ulbricht with engaging in a Continuing Criminal Enterprise by knowingly and intentionally violating 21 U.S.C. §§841, 843 & 846,

which violations were part of a continuing series of violations, in violation of 21 U.S.C. §848(a). Count Two alleges that these violations were committed by Mr. Ulbricht "in concert with at least five other person with respect to whom Ulbricht occupied a position of organizer, a supervisory position, and a position of management" and that Mr. Ulbricht "obtained substantial income and resources" from the continuing series of violations (*see* Indictment at ¶ 12);

- Count Three charges Mr. Ulbricht with a computer hacking conspiracy, in violation of 18 U.S.C. §1030 (b), asserting that the Silk Road website allegedly "provided a platform for the purchase and sale of malicious software designed for computer hacking, such as password stealers, keyloggers, and remote access tools" and that Mr. Ulbricht and others "intentionally access[ed] computers without authorization" and thus "obtain[ed] information from protected computers, for purposes of commercial and financial gain" (*see* Indictment at ¶¶ 14, 16); and
- Count Four charges a money laundering conspiracy, in violation of 18 U.S.C. §1956(h), contending that Mr. Ulbricht allegedly "designed Silk Road to include a Bitcoin-based payment system that served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of the users transmitting and receiving funds on the site" (*see* Indictment at ¶ 18). The Indictment further alleges that it was "part and an object of the [money laundering] conspiracy" that he and others "conduct[ed] and attempt[ed] to conduct financial transactions, which in fact involved the proceeds of specified

unlawful activity, to wit, narcotics trafficking and computer hacking" and that they did so "knowing that the property involved in certain financial transactions represented proceeds from some form of unlawful activity"(*see* Indictment at ¶ 20).

The Indictment also includes forfeiture allegations pursuant to 18 U.S.C. §§981 & 982, 21 U.S.C. § 853, and 28 U.S.C. §2461. S*ee* Indictment at ¶ 22-24.

Mr. Ulbricht has pleaded not guilty to all charges. These motions follow.

ARGUMENT

POINT I

COUNTS ONE, TWO, AND THREE SHOULD BE DISMISSED BECAUSE THE CONDUCT CHARGED THEREIN AGAINST MR. ULBRICHT DOES NOT STATE AN OFFENSE UNDER THE ENUMERATED STATUTES AND BECAUSE EVEN IF THE CONDUCT DID STATE AN OFFENSE, THOSE STATUTES WOULD BE UNCONSTITUTIONALLY VAGUE AS APPLIED IN THIS CASE

As detailed below, Counts One, Two, and Three suffer from similar, and fatal, defects: the allegations therein do not state an offense under the specific statutes underlying each count. Regarding Counts One and Two, alleging a narcotics trafficking conspiracy and a Continuing Criminal Enterprise, neither statute was intended, or has ever been used, to prosecute the conduct alleged against Mr. Ulbricht – that he operated a web site through which other persons – sellers and purchasers – committed illegal activity.[1]

[1] For purposes of these motions, and because challenges to an Indictment on its face do not involve disputing the facts alleged therein, the conduct of the Silk Road and Dread Pirate Roberts will be attributed nominally to Mr. Ulbricht. However, of course, that does not in any way constitute an admission by him with respect to any allegation in the Indictment.

Regarding Count Three, it utterly fails to connect Mr. Ulbricht to any illegal conduct – the unauthorized access to any computer. Merely offering for sale software that the purchaser and/or ultimate user might utilize to commit a crime cannot transfer that person's intent – unknown to Mr. Ulbricht, not communicated to him, and perhaps not even manifested by the purchaser or seller at the time of the transaction on Silk Road – to Mr. Ulbricht for purposes of establishing the necessary *mens rea* to constitute a violation of 18 U.S.C. §1030(a)(2).

Also, with respect to Counts One, Two, and Three, two important rules of statutory construction – the rule of lenity, and the doctrine of constitutional avoidance – operate convincingly to compel dismissal of those counts. In addition, a civil statute, 47 U.S.C. §230, which provides immunity for internet providers for content posted by others, further informs the analysis and confirms that the statutes charged in Counts One, Two, and Three do not cover the conduct alleged against Mr. Ulbricht.

Moreover, should the statutes at issue be deemed to proscribe Mr. Ulbricht's conduct, they would be unconstitutionally vague as applied to him because they present the twin deficiencies of inadequate notice of what is prohibited as well as the danger, realized herein, of arbitrary and discriminatory enforcement.

A. *The Applicable Law Regarding Challenges to the Sufficiency of an Indictment*

As the Second Circuit has declared, "[a]n indictment that fails to allege the essential elements of the crime charged offends both the Fifth and Sixth Amendments." *United States v. Pirro*, 212 F.3d 86, 92 (2d Cir. 2000) (*citing Russell v. United States*, 369 U.S. 749, 760-61 (1962)). As the Court in *Pirro* explained, "'[t]he Indictment Clause of the Fifth Amendment requires that an indictment contain some amount of factual particularity to ensure that the

prosecution will not fill in elements of its case with facts other than those considered by the grand jury.'" *Id*. (quoting *United States v. Walsh*, 194 F.3d 37, 44 (2d Cir. 1999)). *See also United States v. Gonzalez*, 686 F.3d 122, 128-30 (2d Cir. 2012).

In *Pirro* the Court added that the Sixth Amendment "guaranty of the defendant's right 'to be informed of the nature and cause of the accusation' against him is also offended by an indictment that does not state the essential elements of the crime." 212 F.3d at 93, *quoting Russell*, 369 U.S. at 761, *and citing Walsh*, 194 F.3d at 44. As a result, "the indictment must state some fact specific enough to describe a particular criminal act, rather than a type of crime." 212 F.3d at 93; *see also United States v. Hashmi*, not reported in ___ F.Supp.2d ___, 2009 WL 404281, *3 (S.D.N.Y. 2009).[2]

Rule 12(b), Fed.R.Crim.P., provides in relevant part that "[a]ny defense, objection, or request that the court can determine without a trial of the general issue" may be raised before trial by motion. Courts have routinely held that "[f]or purposes of Rule 12(b)(2), a charging document fails to state an offense if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation." *United States v. Panarella*, 227 F.3d 678, 685 (3d Cir. 2000). *See also United States v. Aleynikov*, 676 F.3d 71, 75-76 (2d Cir. 2012); *United States v. Alsugair*, 2003 WL 1799003 (D.N.J. April 3, 2003).

Thus, if the facts alleged in the charging document do not establish the crime charged,

---

[2] In *Pirro*, an interlocutory appeal by the government, the Second Circuit upheld the district court's order striking a portion of one of the counts of the indictment which failed to allege an essential element of a tax fraud charge, *i.e.*, a material false representation. 212 F.3d at 93.

the charge must be dismissed. *Panarella*, 227 F.3d at 685. The indictment here does not satisfy these constitutional and statutory standards with respect to Counts One, Two, or Three.[3]

In addition, the requirements enunciated in *Pirro* and *Russell* are all the more important in the context of complex inchoate crimes (as opposed to simple, single-event offenses) that require knowledge and specific intent, as well as additional unusual or peculiar elements that are present in this case. *See e.g. United States v. LaSpina*, 299 F.3d 165, 177-78 (2d Cir. 2002).

Accordingly, the Indictment must be scrutinized to determine whether it meets these constitutional and statutory standards, and such scrutiny reveals that the Indictment is fatally deficient.

B. *The Statutes Cited In Counts One, Two, and Three Do Not Cover the Conduct Alleged Against Mr. Ulbricht*

Examination of the statutes underlying the allegations in Counts One, Two, and Three demonstrates that they do not cover the conduct alleged against Mr. Ulbricht.

1. *Count One: The Controlled Substances Trafficking Conspiracy*

Count One charges Mr. Ulbricht with conspiracy to possess and possess with intent to distribute controlled substances. Yet Mr. Ulbricht is not alleged to be either the seller or purchaser of controlled substances (or the possessor at any point during such transactions). Rather, he is alleged to have operated a website, Silk Road, that enabled such transactions to occur.

The Silk Road website is described in the Indictment, at ¶1, as "an underground website . . . designed to enable users across the world to buy and sell illegal drugs and other illicit goods

[3] Of course, "it is a settled rule that a bill of particulars cannot save an invalid indictment." *Russell*, 369 U.S. at 770. *See also Pirro*, 212 F.3d at 95 n. 10 (same).

and services[.]" Yet that does not describe a co-conspirator in the controlled substances transactions because a landlord – in this instance, with Silk Road acting as the digital landlord for its tenants (the alleged "drug dealers," "unlawful vendors" and other "users" of the Silk Road website) – is a *not* a co-conspirator of, and/or liable for, the criminal conduct of his tenants, under §846 regardless whether the landlord possesses knowledge that the premises are being used for illegal purposes.

Indeed, federal law specifically covers the question of liability for those whose property is used for purposes of illegal drug activity. For example, pursuant to 21 U.S.C. §881(a)(7), when a landlord *knows* his property is being "used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of a violation of [the United States Code] punishable by more than one year's imprisonment" the penalty is civil forfeiture of the property, *not* criminal liability. *See also, e.g., United States v. All Right , Title and Interest in Real Property And Appurtenances Thereto Known As 143-147 East 23rd Street*, 888 F.Supp. 580, 583 (S.D.N.Y. 1995) (imposing fine in the form of forfeiture of landlord's property when "landlord does not dispute that [the property] was used for drug trafficking and that the claimant knew about the trafficking").

In fact, civil forfeiture, and *not* criminal liability, is the default cause of action even if a landlord creates conditions on his property that nurture or foster illegal activity. *See, e.g., 143-147 East 23rd Street*, 888 F.Supp., at 586-87 ("a colorable criminal case may exist" against the management, but imposing a fine even when the property, under its management, "provided seclusion and privacy for the consummation of drug transactions . . . in excess of the seclusion that one could obtain from an ordinary hotel").

In addition, in October 1986, decades after §§841 and 846 were effective, and a full 16 years after the enactment of 21 U.S.C. §881, which prescribes civil forfeiture penalties, Congress enacted 21 U.S.C. §856 to address a particular scourge – "crack houses." The text of and legislative history for §856 make it clear that it imposes criminal liability only on persons whose premises are operated for the purpose of manufacturing, storing, distributing or using a controlled substance. *See* H 5484, 99th Cong, 2d Sess (Sept 8, 1986), in 132 Cong Rec S 26473, 26474 (Sept 26, 1986) (purpose of §856 was to "[o]utlaw operation of houses or buildings, so-called 'crack-houses,' where 'crack,' cocaine and other drugs are manufactured or used"); *see also* Historical and Statutory Notes to 21 U.S.C. §856. Hence, §856's colloquial name: the "Crack House Statute."

Plainly, §856 was intended to cover a gap in the criminal code: conduct that was *not* covered by pre-existing law (*i.e.*, §§841, *et seq*.). Just as clearly, Congress, no doubt advised by the Department of Justice, sought to create a vehicle for holding criminally liable those whose premises were used, with their knowledge and intent, for the particular criminal activity described in §856. If either §841 or §846 were available to punish such conduct, §856 would have been unnecessary and superfluous.

Indeed, §856 might be viewed as counterproductive because the range of penalties for violating §856 – "a term of imprisonment of not more than 20 years or a fine not more than $500,000, or both[,]" *see* 21 U.S.C. §856 (b); *see also* §856(a)(1) & (2) – are far less severe than those available under either §841(b)(1)(A) [or (b)(1)(B)] or §846.[4]

[4] Consistent with Congress's express purpose in enacting §856, it has been primarily applied to punish those individuals involved in operating drug manufacturing or distributing operations out of crackhouses, warehouses, or large drug manufacturing and storage facilities.

Thus, neither §841 nor §846 cover the conduct alleged against Mr. Ulbricht. Also, under the government's theory a whole array of web hosts, internet service providers, and web sites could be liable for the criminal conduct (and not just narcotics trafficking) of those who avail themselves of the particular services offered or enabled by those internet entities.

For example, search engines and internet service providers are fully aware that the internet contains illegal web site content accessible to their consumers – whether it is child pornography, pirated copyrighted works (video or otherwise), *jihadist* recruitment or radicalizing materials that constitute "material support" for terrorism, or instructions on how to construct explosive devices – as well as a whole range of predatory activity, from chat rooms to ordinary or sophisticated fraudulent schemes, without being prosecuted for that conduct either as a principal or aider and abettor.[5]

See United States v. Wicker, 848 F.2d 1059 (10th Cir.1988) (methamphetamine lab); *United States v. Martinez–Zyas*, 857 F.2d 122 (3rd Cir.1988) (cocaine warehouse and packaging facility); *United States v. Bethancurt*, 692 F.Supp. 1427 (D.C. Dist.Ct.1988) (crack house); *United States v. Restrepo*, 698 F.Supp. 563 (E.D.Pa.1988) (cocaine warehouse). *But see United States v. Tamez*, 941 F.2d 770, 773-74 (9th Cir. 1991) (owner of used car dealership who was aware of large-scale drug distribution activities emanating from his dealership, and allowed them to continue, was guilty of violating §856(a)(2)); *United States v. Chen*, 913 F.2d 183, 185, 191 (5th Cir. 1990) (same re: motel owner who was aware of and/or willfully blind to the fact that her motel was occupied by drug dealers who sold drugs in the rooms and on the premises, and who also stored drugs at her motel).

[5] In the copyright context, it is doubtful that operating a site that provides hyperlinks to streaming versions of pirated material is even a civil, much less criminal, violation. *See, e.g., Perfect 10, Inc., v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir.2007) (linking not a copyright violation); *Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012) (viewing a "stream" does not constitute a copyright violation); *United States v. Rojadirecta.org*, 11 Civ. 4139 (PAC) (S.D.N.Y.) Notice of Voluntary Dismissal, Document 55, August 29, 2012 (government moved to vacate seizure warrants in light of "recent judicial authority involving issues germane to the . . . action"); *WPIX, Inc. v. ivi, Inc.*, 691 F.3d 275 (2d Cir. 2012) ("streaming" implicates only a public performance right of a copyright holder, and not the right of reproduction in copies or public distribution of copies by sale or other transfer of ownership, or by rental, lease or

Also, the conduct alleged against Mr. Ulbricht is analogous to a "steerer" in a drug transaction, which is *not* equivalent to a co-conspirator. In fact, it is well-settled under Second Circuit case law that "evidence adduced by the government merely show[ing] that [an individual] helped a willing buyer locate a willing seller . . . , standing alone, is insufficient to establish the existence of an agreement between the facilitator and the seller." *United States v. Tyler*, 758 F.2d 66, 69 (2d Cir. 1985) (evidence of facilitator's role insufficient to establish the existence of a conspiracy between facilitator and seller), *citing United States v. Hysohion*, 448 F.2d 343, 347 (2d Cir. 1971) ("fact that Rimbaud told Everett, a willing buyer, how to make contact with a willing seller does not necessarily imply that there was an agreement between that seller . . . and Rimbaud"); *United States v. Torres*, 519 F.2d 723, 726 (2d Cir. 1975) ("membership in a conspiracy is not established . . . by the fact that a defendant told a willing buyer how to make contact with a willing seller").

Consequently, for all these reasons, it is respectfully submitted that Count One fails to state an offense under 21 U.S.C. §846, and must therefore be dismissed.

2. *Count Two: The Continuing Criminal Enterprise*

Count Two, charging the Continuing Criminal Enterprise (hereinafter "CCE") violation, suffers from two fatal flaws: (a) it fails to allege satisfactorily that Mr. Ulbricht occupied the requisite management authority – not surprising considering the unique nature of the allegations against Mr. Ulbricht under §848(a), heretofore reserved for "kingpins" of drug-trafficking organizations, or their upper management; and (b) it fails to identify the "continuing series" of predicate violations with sufficient specificity.

---

lending).

a. ***Count Two Fails to Allege Sufficiently That Mr. Ulbricht Occupied a "Position of Organizer, a Supervisory Position, and a Position of Management" Necessary to a CCE Violation***

Pursuant to the standards set forth **ante**, at 7-9, Count Two is deficient because it fails to allege any conduct that could establish Mr. Ulbricht as occupying a "position of organizer, a supervisory position, and a position of management" required to for a violation of §848(a). Essentially, §848 has been directed – in its passage as well as implementation – at "kingpins" and upper supervisory personnel *directly* involved in the sale of controlled substances. No one in Mr. Ulbricht's position – allegedly operating a web site serving as a "platform" for illegal activity – has ever been prosecuted under §848(a).

As a result, citing only Mr. Ulbricht's alleged role as owner and operator of the Silk Road website, the Indictment fails to allege any conduct rising to the level of organizer, supervisor or manager, as that element has been defined and interpreted by the courts. Although CCE prosecutions pursuant to §848 traditionally encompass straightforward narcotics conspiracies, with a visible structure or hierarchy, the government still must demonstrate that the relationship between the defendant and at least five individuals with whom he undertook the series of violations, satisfies the definition of supervisory. *See also United States v. Casamento*, 887 F.2d 1141 (2d Cir. 1989); *United States v. Cruz*, 785 F.2d 399 (2d Cir. 1986).

Culpability for Mr. Ulbricht under §848(a) in this case would require that he "occup[ied] a position of organizer, a supervisory position, or any other position of management" in regard to those persons engaging in the continuing series of violations giving rise to the criminal enterprise, *i.e.*, those "users" of the Silk Road website who bought and sold "illegal drugs and

other illicit goods and services" through the site. *See* 21 U.S.C. §848(c)(2)(A); Indictment, at ¶ 1.

But, while Mr. Ulbricht is alleged to have played a supervisory role in regard to *administrators* of the Silk Road site (those responsible for keeping the site up and running), and the government characterizes those persons as "employees whom [the defendant] managed and supervised," he is *not* alleged to have supervised, organized, or managed any of the many "users" who were buying and selling drugs and other illicit goods and services on the site. *See* Indictment at ¶3 ("the defendant [] controlled all aspects of Silk Road [] with the assistance of various paid employees who he managed and supervised").

Indeed, the fact that the government characterizes those persons who went on the Silk Road site to buy and sell drugs and other illicit goods and services as "users" and not "employees," makes clear that Mr. Ulbricht did not manage or supervise those persons, in particular when the government uses the term "employee" in the Indictment to identify those persons Mr. Ulbricht allegedly supervised. *See* Indictment at ¶1 ("the defendant, created . . . 'Silk Road' . . . to enable *users* across the world to buy and sell illegal drugs and other illicit goods and services"); ¶ 2 ("the wesbite was *used* by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services") (emphasis added). *See also* Criminal Complaint, at ¶¶ 26-28 (pp. 19-20);

Accordingly, the language in the Indictment makes plain that, at worst, Mr. Ulbricht allegedly acted as a conduit or facilitator for those engaging in illegal activity – "design[ing] [Silk Road] to enable users to buy and sell illegal drugs and other illicit goods and services" and "providing a platform for drug dealers around the world to sell a wide variety of controlled

substances via the Indictment" – but never as the "kingpin" or leader of any continuing criminal enterprise. *See* Indictment at ¶¶ 1, 10(a).

Also, it is obvious that here the role attributed to Mr. Ulbricht falls well short of the outer limits established by the courts. *United States v. Amen*, 831 F.2d 373, 381 (2d Cir. 1987) (it is clear from the legislative history that the "purpose...was not to catch in the CCE net those who aided and abetted the supervisors' activities"). For example, in *Casamento* the Court held that the government had failed to establish that the defendant at issue was directing the activities of at least one of the five individuals required to violate the statute because the defendant's interaction with that person did not demonstrate that the defendant was directing the individual's activity. *Casamento*, 887 F.2d at 1161-62.

The Court in *Casamento* reached that conclusion not only because the government failed to present any evidence that the defendant gave orders directly, or through someone else, to the individual, but also because evidence that the defendant communicated information from his superiors within the conspiracy to one of the individuals was insufficient to demonstrate that the defendant was directing that person's activities. *Id*.

In addition, in *United States v. Walker* the Court concluded that although direct contact is not necessary to establish that the defendant manages, supervises or directs another's activities, in order to prove the requisite management role the government must demonstrate that the "defendant's management ran *down* the enterprise's hierarchy through [someone] acting as a second-level manager." *United States v. Walker*, 912 F.Supp. 646, 650-51 (S.D.N.Y. 1996).

Yet §848(a) has never been applied or interpreted to cover a person operating a website through which illegal transactions were executed, even one allegedly providing mechanisms for

concealing activity accomplished through the site. By alleging only that Mr. Ulbricht owned and operated a website that served as a marketplace or "platform" for illegal transactions conducted by members of the general public, Count Two does not sufficiently allege that he had any control, or even any direct contact, with any of the individuals involved in those transactions, let alone five with whom he undertook a series of violations of federal narcotics laws. As a result, Count Two must be dismissed.

b. ***Count Two Fails to Enumerate the Requisite Predicate Series of Violations Necessary to a Violation of 21 U.S.C. §848***

Count Two of the Indictment alleges that Mr. Ulbricht engaged in a CCE, in violation of §848, by "knowingly and intentionally violat[ing] Title 21 U.S.C. §§841, 843, and 846, which violations were part of a continuing series of violations[.]"

That description abjectly fails to set forth an essential element of the offense – the "series of violations" – in violation of both Rule 7(c), Fed.R.Crim.P., and the Fifth and Sixth Amendments. *See* discussion **ante**, at 7-9. Absent that enumeration, the government is free to amend the Indictment at its pleasure, potentially substituting any alleged illegal drug transactions for those voted on by the grand jury. In addition, given the alleged volume of such transactions – the Indictment numbers them in the potentially hundreds of thousands– without such specificity Mr. Ulbricht will be unable to defend effectively against the particular transactions that form the basis of the CCE allegation.

As detailed **ante**, at 7-9, and **post**, at 18-20, merely tracking the language of the statute, as the Indictment does here, does not satisfy the minimal requirements – under the Federal Rules of Criminal Procedure as well as the Constitution – that the Indictment inform Mr. Ulbricht satisfactorily of the "nature and cause of the accusation," and constrain the government to the

facts "considered by the grand jury." *Pirro*, 212 F.3d at 92.

In particular, when alleging a violation of a statute which includes "generic terms," the Indictment must include some "fact specific enough to describe a particular criminal act, rather than a type of crime." *Pirro*, 212 F.3d at 93.

Regarding §848 specifically, the Supreme Court has indisputably determined that the clause "continuing series of violations" refers to an essential element composed of a particular minimum set of transactions about which a jury must be unanimous in order to find a violation of the statute. *Richardson v. United States*, 526 U.S. 813, 824 (1999) (jury may not simply agree that defendant committed three underlying crimes but must unanimously agree on which of the three or more individual violations constituted the "continuing series"). Thus, the statutory language itself clearly does not "embod[y] all the elements of the crime." *United States v. Guterma*, 189 F.Supp. 265, 270 (S.D.N.Y. 1960) (*citing United States v. Debrow*, 346 U.S. 374 (1953)).

In that context, merely directing Mr. Ulbricht, as the Indictment, at ¶ 12 does here, to three other extremely broad provisions of criminal law, none of which serve to clarify the specific offense with which he has been charged, and all of which employ similarly generic language, cannot cure the failure to sufficiently allege an essential element of the offense. *See Richardson*, 526 U.S. at 817-24.

Nor does Count One, which does not include any specificity with respect to individual substantive transactions, assist in providing the necessary detail. In fact, the volume of transactions alleged generally within Count One aggravate the problem rather than cure it, as the alleged haystack is so enormous that it defies identifying with any confidence the "continuing

series" upon which the grand jury relied, and to which the government must be limited in attempting to prove Count Two.

In *United States v. Gonzalez*, the Second Circuit pointed out that in the context of an indictment that cited the statutory section corresponding to a mandatory minimum quantity would not suffice because "without a factual allegation as to quantity in the indictment, and without factual allegations in the indictment from which the grand jury's determination to charge such a quantity could be inferred, . . ." 686 F.3d at 127.

As the Circuit elaborated in *Gonzalez*, "'[s]tated another way,' the mere citation of a statutory section 'is of scant help in deciding whether the grand jury considered [the] . . . essential element.'" *Id*., at 129, *quoting United States v. Camp*, 541 F.2d 737, 740 (8th Cir. 1976).

Moreover, as the Circuit reasoned in *Gonzalez*, "[i]f citation of the statute were a statement of the facts, nothing beyond a citation would be necessary. Surely no one could assert persuasively that an indictment that merely charged that a defendant violated a cited statute would suffice as an indictment." *Id*., *quoting Camp*, 541 F.2d at 740. *See also id*., at 132 (there was "no reason to believe that members of a grand jury, in determining what charges to bring, think in terms of statutory subsections rather than in terms of facts").

Thus, ultimately, the Court in *Gonzalez* concluded that

> [i]f it was indeed the intention of the grand jury to allege that Gonzalez conspired to distribute and possess with intent to distribute 500 grams or more of cocaine, we would expect the grand jury to have alleged that fact in words, rather than by simply changing a letter in a statutory citation.

Id., at 132.

In addition, Mr. Ulbricht's alleged role – indirect and attenuated, and not involved

directly as seller or purchaser – exacerbates the difficulty of ascertaining the identity of the components of the requisite "continuing series." These impediments are further amplified by the complex, compound nature of the offenses charged, their inchoate nature, and the elements peculiar to them. *See, e.g.*, *LaSpina*, 299 F.3d at 177-78.

In *United States v. Flaharty*, 295 F.3d 182, 197-98 (2d Cir. 2002), the Second Circuit held that an indictment need not articulate the specific ingredients of the "continuing series." However, in *Flaharty*, the Court addressed an indictment returned (and tried) prior to the Supreme Court's decision in *Richardson*. Also, in *Flaharty*, the extensive undercover investigation generated specific sales from the defendants, and searches produced seizures of drugs in locations used by particular defendants. *Id*., at 189-90. Thus, notice was not necessarily an issue in *Flaharty*.

Moreover, it is respectfully submitted that *Flaharty* cannot be reconciled with *United States v. Thomas*, 274 F.3d 655 (2d Cir. 2001), in which the Circuit held that both drug quantity *and* type constituted essential elements that must be pleaded in the indictment (and in which the failure to do so constituted plain error). 274 F.3d at 660. Indeed, *Flaharty* does not even mention *Thomas*.

More recently, in *United States v. Gonzalez*, the Second Circuit reiterated that "it has long been the rule in this Circuit that a deficiency in an indictment's factual allegations of the elements of an offense is 'not cured by' the fact that the relevant count 'cited the statute that [the defendant] is alleged to have violated[.]'" 686 F.3d at 128, *citing United States v. Berlin*, 472 F.2d 1002, 1008 (2d Cir. 1973) (citing cases).

Yet that is precisely what Count Two does herein with respect to the "continuing series"

of violations necessary to §848(a). As the Second Circuit cautioned in *Gonzalez*, "[a]doption of the government's position to the contrary would plainly elevate form over substance, would facilitate indictments that contain no factual allegations, and would provide no assurance that an indictment reflects the judgment of a grand jury rather than only that of the prosecutor." 686 F.3d at 133.

Consequently, by alleging only that Mr. Ulbricht violated three statutes, all of which cover an incredibly broad range of alleged conduct, Count Two fails to allege an essential element of §848, and does precisely what the Fifth and Sixth Amendments prohibit. Accordingly, it is respectfully submitted that Count Two of the Indictment must be dismissed.

3. *Count Three: The Computer Hacking Conspiracy*

Count Three of the Indictment alleges that Mr. Ulbricht participated in a conspiracy to violate the Computer Fraud and Abuse Act (hereinafter "CFAA"), 18 U.S.C. §1030, by "intentionally access[ing] computers without authorization, and thereby...obtain[ing] information from protected computers." *See* Indictment, at ¶ 15-16. However, as detailed below, because Count Three alleges only that the Silk Road website "provided a platform for the [exchange] of malicious software," the Indictment fails to allege facts establishing Mr. Ulbricht's knowing participation in a conspiracy to violate §1030(a)(2)(C) – that Mr. Ulbricht possessed the knowledge and intent to access a protected computer without authorization.

Establishing a violation of 18 U.S.C. §1030(a)(2)(C) requires "proof that the defendant *intentionally* accessed information from a protected computer." *United States v. Willis*, 476 F.3d 1121, 1125 (10th Cir. 2007) (emphasis added). *See also Dedalus Found. v. Banach*, ____ F.Supp.2d ____, 2009 WL 3398595 (S.D.N.Y. Oct. 16, 2009). Accordingly, a conspiracy to

violate §1030(a)(2)(C), requires proof that the defendant agreed to "(1) intentionally access[] a computer, (2) without authorization . . ., (3) and thereby obtained information." *Willis*, 476 F.3d at 1125.

Thus, a conspiracy to violate §1030(a)(2)(C) requires the *mens rea* necessary to violate the substantive statute: the defendant's intentional accessing of information on a protected computer, without authorization. Count Three patently fails to allege that Mr. Ulbricht had the requisite knowledge or intent to conspire. Merely making certain software available to purchasers does not establish *Mr. Ulbricht's* knowledge or intent with respect to the purchasers or ultimate users.

Count Three contends merely that the Silk Road website was used as a "platform" for buying and selling "malicious software designed for computer hacking." *See* Indictment, at ¶ 14. However, providing a marketplace for the purchase and sale of software which may be used illegally, does not even allege knowledge of a conspiracy, let alone intent to access protected computers without authorization.

The intent element in 18 U.S.C. 1030(a)(2)(C) has long been interpreted as requiring that the government prove the defendant intended to gain access to protected computers without authorization, and selling software, even with awareness of its potential illegal uses, does not demonstrate such intent. *See United States v. Morris*, 928 F.2d 504, 207 (2d Cir. 1990).

Indeed, even the direct provision of software with potentially illegal applications cannot, by itself, demonstrate intent to conspire to use that software to access protected computers without authorization. *See e.g. United States v. Zambrano*, 776 F.2d 1091, 1094-96 (2d Cir. 1985) ("that a defendant simply supplies goods, innocent in themselves, to someone who

intended to use them illegally is not enough to support a conviction for conspiracy . . . [without]...some indication that the defendant knew of and intended to further the illegal venture . . . [or] somehow encouraged the illegal use of the goods or had a stake in such use").

Although the government characterizes "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking," these devices have numerous legitimate uses and applications, despite having become associated with illegal activity because of their use in high profile cases or fictional universes. *See* Indictment, at ¶ 14. Moreover, Mr. Ulbricht would not know whether the purchaser or ultimate user was intending to use the software for proprietary research, academic study (by students or professors), security purposes, or merely to satisfy the particular abstract interest of a particular consumer.

Indeed, even the FBI solicits malware. An FBI podcast dated March 14, 2014, announced that "Malware Investigator gives community of interest partners the ability to submit malware files." The podcast announcement explains that "Malware Investigator will determine the damage the file can inflict[,]" and "will provide a technical analysis report to the submitter." *See* <http://www.fbi.gov/news/podcasts/thisweek/malware-investigator.mp3/view>. The FBI even intends to launch Malware Investigator as a web site this summer. *Id.*

Addressing the issue of intent in an analogous context, the case law regarding drug paraphernalia laws, which raised the specter of a merchant being liable for a customer's intent, is instructive. As the Seventh Circuit stated in *Levas and Levas v. Village of Antioch*, 684 F.2d 446 (7th Cir. 1982), "no one can constitutionally be convicted on the basis of someone else's intent." *Id.*, at 450.

Similarly, in the Southern District of New York, three judges expressed serious, and in

some instances dispositive, reservations with respect to local drug paraphernalia ordinances – carrying only minor penalties – that created the danger of "transferred intent," *i.e.*, when the defendant is saddled with the criminal intent of another. *See Brache v. Westchester*, 507 F. Supp. 566, 578, 580 (S.D.N.Y. 1981), *rev'd on other grounds*, 658 F.2d 47 (2d Cir. 1981); *Franza v. Carey*, 518 F. Supp. 342 (S.D.N.Y. 1981); *United States v. Glass Menagerie, Inc.*, 721 F. Supp. 54, 61 (S.D.N.Y. 1989).

The CFAA has never been interpreted to encompass within its scope the provision of a forum for the exchange of software, which could potentially be used by the purchaser or ultimate user in violation of the statute, as has been alleged here. Therefore, Count Three fails to allege facts sufficient to constitute a violation of §1030(a)(2), and must be dismissed.

C. *Two Fundamental Rules of Statutory Construction Further Establish That the Conduct Alleged In Counts One, Two, and Three Is Not Covered By the Statutes*

While, as set forth above, the plain language of the statutes at issue preclude their application to Mr. Ulbricht in this case, to the extent any ambiguity exists two fundamental rules of statutory construction persuasively buttress that conclusion.

1. *The Rule of Lenity Requires a Narrow Reading of the Statutes At Issue*

When interpreting a criminal statute that does not explicitly reach the conduct in question, courts should be reluctant to base an expansive reading of the statute on inferences. *See Williams v. United States*, 458 U.S. 279, 286 (1982) (applying rule of lenity to a false statements statute). As the Supreme Court has instructed, "when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before [choosing] the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *United States v. Bass*, 404 U.S. 336, 347 (1941). *See also Chapman v. United States*,

500 U.S. 453, 463 (1991); *Rewis v. United States*, 401 U.S. 808, 812 (1971) ("ambiguity concerning the ambit of a criminal statute should be resolved in favor of lenity"), *citing Bell v. United States*, 349 U.S. 81, 83 (1955).

In *United States v. Brown*, in the context of 18 U.S.C. §666, the Fifth Circuit declared, in language more applicable to §2339A in this instance in light of the First Amendment interests at stake, "[w]e resist the incremental expansion of a statute that is vague and amorphous on its face and depends for its constitutionality on the clarity divined from a jumble of disparate cases. Instead, we apply the rule of lenity and opt for the narrower, reasonable interpretation that here excludes the Defendants' conduct." 459 F.3d 509, 523 (5th Cir. 2006), *citing McNally v. United States*, 483 U.S. 350, 360 (1987). *See also United States v. Ford*, 435 F.3d 204, 211 (2d Cir. 2006) ("[a]s the Supreme Court noted in its recent decision in [*Arthur Andersen LLP v. United States*, 544 U.S. 696, 703-704 (2005)], restraint must be exercised in defining the breadth of the conduct prohibited by a federal criminal statute out of concerns regarding both the prerogatives of Congress and the need to give fair warning to those whose conduct is affected").

The Supreme Court quite recently reaffirmed and reinforced the rule of lenity. In *Burrage v. United States*, ___ U.S. ___, 134 S.Ct. 881 (2014), the Court explained that "[e]specially in the interpretation of a criminal statute subject to the rule of lenity, *see Moskal v. United States*, 498 U.S. 103, 107–108 [] (1990), we cannot give the text a meaning that is different from its ordinary, accepted meaning, and that disfavors the defendant. *Id*., at *7. *See also* Ginsburg, J. (joined by Sotomayor, J.), *concurring in the judgment*, at *9.

Thus, "given the need for clarity and certainty in the criminal law[,]" *id*., at *8, the Court rejected the government's interpretation of 21 U.S.C. §841(a) in favor of a construction that

resulted in reversal of the defendant's conviction. As the Court emphasized, "[u]ncertainty of that kind cannot be squared with the beyond-a-reasonable-doubt standard applicable in criminal trials or with the need to express criminal laws in terms ordinary persons can comprehend." *Id*., at *8, *citing United States v. L. Cohen Grocery Co.*, 255 U.S. 81, 89–90 (1921).

Thus, as the Court noted in *Skilling v. United States*, ___ U.S.___, 130 S. Ct. 2896, 2933 (2010), with respect to aspects of 18 U.S.C. §1346, which proscribes mail fraud involving deprivation of "honest services," if Congress "desires to go further[,]" and intended to include the conduct alleged against Mr. Ulbricht within the scope of the statutes at issue in Counts One, Two, and/or Three, "it must speak more clearly than it has." ___ U.S. at ___, 130 S. Ct. at 2933, *quoting McNally*, 483 U.S. at 360. *See also United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (in the context of the CFAA, §1030).

2. *The Doctrine of Constitutional Avoidance Also Restricts the Scope of the Statutes At Issue In Counts One, Two, and Three*

In addition, confirming application of the statutes at issue in the extraordinarily expansive fashion attempted in the Indictment would also contravene the doctrine of constitutional avoidance, which applies when "a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, [a court's] duty is to adopt the latter." *United States ex rel. Attorney General, v. Delaware & Hudson Co.*, 213 U.S. 366, 408 (1909). *See also Jones v. United States*, 526 U.S. 227, 239-40 (1999). *Accord Triestman v. United States*, 124 F.3d 361, 377 (2d Cir. 1997); *United States v. Al-Arian*, 329 F. Supp.2d 1294, 1298 & n. 11 (M.D. Fla. 2004) (relative to §2339B); *United States v. Khan*, 309 F. Supp.2d 789, 822 (E.D.Va. 2004) (applying the same principle to "personnel" in the context of §2339A).

As this Court recognized in *Hedges v. Obama*, Not Reported in F. Supp.2d, 2012 WL 1721124 (S.D.N.Y. May 17, 2012),[6] "[t]he Supreme Court has instructed courts to 'refrain from invalidating more of the statute than is absolutely necessary.'" *Id*., at *24, *quoting Alaska Airlines, Inc. v. Brock*, 480 U.S. 678, 684 (1987) (other citation omitted).

Accordingly, the Court noted it was "mindful of its responsibility not to enjoin a statute without considering whether the statute – or the majority of the statute – is susceptible to a limiting construction that renders the statute constitutional." *Id*., (other citations omitted).

Moreover, other canons of statutory construction further support that conclusion. For instance, in *Arthur Andersen LLP*, 544 U.S. at 703, the Court cautioned that,

> "[w]e have traditionally exercised restraint in assessing the reach of a federal criminal statute, both out of deference to the prerogatives of Congress, *Dowling v. United States*, 473 U.S. 207 (1985), and out of concern that 'a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed.' *McBoyle v. United States*, 283 U.S. 25, 27 (1931)."

Id., *quoting United States v. Aguilar*, 515 U.S. 593, 600 (1995).

Also, because, as discussed **post**, at 35-37, First Amendment activity on the internet is implicated by the government's proposed application of the statutes at issue, additional restrictive principles apply. As the Supreme Court explained in *NAACP v. Button*, 371 U.S. 415, 433 (1963) (citations omitted), "[t]hese [First Amendment] freedoms are delicate and vulnerable, as well as supremely precious in our society. The threat of sanctions may deter their exercise almost as potently as the actual application of sanctions. [ ] Because First Amendment freedoms

---

[6] A related opinion by this Court in *Hedges v. Obama*, 890 F.Supp.2d 424 (S.D.N.Y. 2012) was subsequently reversed by the Circuit on other grounds in 724 F.3d 170 (2d Cir. 2013).

need breathing space to survive, government may regulate in the area only with narrow specificity. [ ]" *See also Reno v. ACLU*, 521 U.S. 844, 871-72 (1997); *Humanitarian Law Project v. US Dept of Justice*, 352 F.3d 382, 403-04 (9th Cir. 2003).

D. *The Civil Immunity Afforded Internet Providers By 47 U.S.C. §230 Manifests a Policy That Would Be Seriously Undermined By Allowing the Statutes In Counts One, Two, and Three to Be Applied to the Conduct Alleged Against Mr. Ulbricht*

In 47 U.S.C. §230, Congress manifested an unmistakable support for a free-wheeling internet, including one in which providers or users of interactive computer services can operate without fear of civil liability for the content posted by others.[7] While that civil immunity is not dispositive here, it certainly provides firm and indisputable support for limiting the application of *criminal* statutes in the internet context when the alleged illegal conduct itself is performed not by the defendant, but by others using his web site.

Section 230's "Findings" section includes the following declarations:

> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

---

[7] *See also* Joseph D'Ambrosio and Andrew I. Mandelbaum, "When Does Internet Service Provider Lose Immunity," *The New York Law Journal*, February 20, 2014, available at <http://www.newyorklawjournal.com/id=1202643655229/when+does+internet+service+provider+lose+immunity?mcode=1202615326010&curindex=1&curpage=all>. In discussing attempts to expand the exceptions to §230(c)'s protections, the authors maintain that "[l]imiting such immunity by expanding the exceptions, in addition to sowing "confusion and uncertainty, . . . would also have a chilling effect on legal speech on the Internet because ISP's, hosts, and site owners will have a major financial incentive to avoid exposure to liability." *Id*., at 4. If exceptions are widened, "websites will have to decide whether it is worth the headaches, endless cease and desist letters and threats of litigation to continue operating a blog, website or message board that permits users to post content freely." *Id*.

> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

47 U.S.C. §230(a).

In §230, Congress also announced policy with respect to internet activity. Thus, §230(b) states

> [i]t is the policy of the United States—
>
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> * * *
>
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
>
> * * *
>
> . . . and
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

Implementing that policy, §230(c)(1), entitled "Treatment of publisher or speaker," provides that "[n]o provider or user of an interactive computer service[8] shall be treated as the publisher or speaker of any information provided by another information content provider.[9]" However, §230(e)(1), entitled "no effect on criminal law," states "[n]othing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to

---

[8] An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. §230(f)(2).

[9] An information content provider is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230 (f)(3).

obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute."[10]

As the Fourth Circuit explained in *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997):

> [b]y its plain language, §230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, §230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred.

Id., at 330.

In order to qualify for §230's immunity, one need merely demonstrate that he *provides or uses* an interactive computer service, and that the information contained thereon was provided by a third-party for use on the Internet or other interactive computer service. *Blatzel v. Smith*, 333 F.3d 1018, 1030-35 (9th Cir. 2003). In *Blatzel*, the Ninth Circuit held that an individual who received an email, made minor edits to it, and then posted the edited version on both his website and listserv qualified as a provider or user of an interactive computer service. *Id.*

Thus, one need not be an Internet Service Provider to qualify for immunity under §230; mere operation of a website or moderation of a listserv qualifies as a "user of an interactive computer service." *Id.* at 1030-31; *see also Gentry v. eBay, Inc.*, 121 Cal. Rptr. 2d 703, 99

---

[10] Notwithstanding §230(e)(1)'s caveat, it is anomalous that the law affords greater jurisdictional protection to civil litigants, with money or property at stake, than to defendants in criminal cases whose liberty is in jeopardy. *See United States v. Vilar*, ___ F.3d ___, 2013 WL 4608948, at *5 (2d Cir. August 30, 2013) (extending the presumption against extraterritoriality existing in civil law to criminal statutes).

Cal.App.4th 816, 831 & n.7 (2002) (website is an interactive computer service); *Schneider v. Amazon.com, Inc.*, 31 P.3d 37, 40-41 & n.13 (Wash. Ct. App. 2001) (same). Similarly, providers and users of Internet e-mail groups or chat rooms are protected by §230's immunity when the information complained of was created by a third party. *See Noah v. AOL Time Warner*, 261 F.Supp.2d 532, 538 (E.D. Va. 2003).

Moreover, such immunity is absolute. For instance, the Court in *Blumenthal v. Drudge*, 992 F.Supp. 44, 49 (D.D.C. 1998), noted that "[w]hether wisely or not, [Congress] made the legislative judgment to effectively immunize providers [and users] of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others."

In *Drudge* the Court found defendants immune even though they had contracted with the author, paid the author a monthly salary, promoted their association with the author, and even reserved editorial rights to the author's work. *Id.* at 51. In rejecting the plaintiffs' argument that such involvement effectively removed the defendants from §230's immunity the Court in *Drudge* pointed out that "Congress has made a different policy choice by providing immunity even where the interactive service provider has an *active, even aggressive role in making available content prepared by others.*" *Id.* at 52 (emphasis added); *see also Ben Ezra, Weinstein, and Co., Inc. v. America Online Inc.*, 206 F.3d 980, 985-86 (10th Cir. 2000) (interactive service provider did not transform itself into an information content provider by deleting portion of original content and was therefore immune from suit under §230).

In this environment, the allegations in this Indictment contrast dramatically with the aspirations for an internet free of vicarious liability. In fact, prior to this case, internet service

providers, search engines, or browsers have never been charged criminally for permitting content or even hosting web sites that tolerate or even promote illegal activity – thereby providing those web sites and activities the very same "platform" Mr. Ulbricht is alleged to have provided. *See also* **ante**, at 12.[11] They are not even liable *civilly*, as they are protected by §230(c). In fact, Google is the most common defendant in lawsuits in which §230(c) has been invoked, and other major ISP's and browsers have also regularly availed themselves of §230(c) in civil litigation.[12]

Accordingly, the findings, policy, and civil immunity codified in §230 support a decidedly narrow application of the criminal statutes at issue in this case to the conduct alleged against Mr. Ulbricht.

E. ***If the Statutes At Issue In Counts One, Two, and Three Are Deemed to Cover the Conduct Alleged Therein Against Mr. Ulbricht, They Are Unconstitutionally Vague As Applied to Him In This Case***

1. ***The Principles of the "Void for Vagueness" Doctrine***

As this Court explained in *Hedges v. Obama*,

> [t]o satisfy the Due Process Clause of the Fifth Amendment, individuals are entitled to understand the scope and nature of statutes which might subject them to criminal penalties. Thus, "[a] penal statute must define the criminal offense (1) with sufficient definiteness that ordinary people can understand what conduct is prohibited and (2) in a manner that does not encourage arbitrary and discriminatory enforcement." *Skilling v. United States*, 130 S. Ct. 2896, 2928 (2010). That analysis is performed against the

[11] Also, as noted in D'Ambrosio & Mandelbaum's article (*see* **ante**, at n. 7), "Congress has regularly reiterated and even extended the protections provided by [§230]," as in the SPEECH Act of 2010, 28 U.S.C. §1 was amended to apply §230's immunity to foreign defamation judgments).

[12] As a result, not surprisingly, Facebook, Google, Twitter, and Amazon have submitted *amici* briefs in the Sixth Circuit seeking reversal of a District Court decision finding a web site liable in *Jones v. Dirty World*, 840 F. Supp.2d 1008 (E.D. Ky. 2012).

> backdrop of a strong presumption of validity given to acts of Congress. *Id.*

2012 WL 1721124, at *22. *See also Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972).

The United States Supreme Court has characterized the "void-for-vagueness" doctrine as "the first essential of due process of law." *Connally v. General Construction Co.*, 269 U.S. 385, 391 (1926). Likewise, as the Second Circuit stated in *Farrell v. Burke*, 449 F.3d 470 (2d Cir. 2006), and repeated in *Thibodeau v. Portuondo*, 486 F.3d 61 (2d Cir. 2007), the void-for-vagueness doctrine is one of the "most fundamental protections of the Due Process clause[.]" 486 F.3d at 65, *quoting Farrell*, 449 F.3d at 484.

Thus, in order to survive a vagueness challenge, "[i]n short, the statute must give notice of the forbidden conduct and set boundaries to prosecutorial discretion." *United States v. Handakas*, 286 F.3d 92, 101 (2d Cir. 2002). *See also United States v. Rybicki*, 354 F.3d 124, 132 (2d Cir. 2003) (*en banc*).

The doctrine requires that "laws be crafted with sufficient clarity to 'give the person of ordinary intelligence a reasonable opportunity to know what is prohibited' and to 'provide explicit standards for those who apply them,'" *Betancourt v. Bloomberg*, 448 F.3d 547, 552 (2d Cir.2006), *quoting Grayned v. City of Rockford*, 408 U.S. at 108. *See also Thibodeau*, 486 F.3d at 65.

Also, as the Court in *Grayned* pointed out, "a vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis, with the attendant danger of arbitrary and discriminatory application." 408 U.S. at 108-09 (footnotes omitted). In addition, "criminal laws are more searchingly examined for vagueness, because the consequences of imprecision are severe, than are either pure economic regulation

(with or without quasi-criminal penalties) or civil legislation." *Levas and Levas*, 684 F.2d. at 452, *citing Village of Hoffman Estates, Inc. v. The Flipside, Inc.*, 455 U.S. 489, 494-502 (1982). *See also Record Head Corp. v. Sachen*, 682 F.2d 672, 674 (7th Cir. 1982).

The general standards also govern a vagueness challenge "as applied" to a particular case. *See Farrell*, 449 F.3d at 486; *United States v. Nadi*, 996 F.2d 548, 550 (2d Cir. 1993). *See also Thibodeau v. Portuondo*, 486 F.3d at 67-68; *Handakas*, 286 F.3d at 111 ("[t]he principle that a statute must provide both 'notice' and 'explicit standards' to survive an 'as-applied' constitutional challenge based on vagueness is well established").[13]

Accordingly, in evaluating an as-applied challenge, "in determining the sufficiency of the notice, a statute must of necessity be examined in the light of the conduct with which a defendant is charged." *Farrell*, 470 F.3d at 491. *See also United States v. Sattar I*, 272 F. Supp.2d 348, 357 (S.D.N.Y. 2003) ("[a] 'void for vagueness' challenge does not necessarily mean that the statute could not be applied in some cases but rather that, as applied to the conduct at issue in the criminal case, a reasonable person would not have notice that the conduct was unlawful and there are no explicit standards to determine that the specific conduct was unlawful"), *citing Handakas*, 286 F.3d at 111-12 (other citation omitted).

The First Amendment implications of the application of the statutes at issue add another dimension to the analysis. Thus, if the statute under consideration "is capable of reaching

---

[13] Also, "[i]n the absence of an accompanying First Amendment challenge, a vagueness challenge is generally evaluated on an 'as applied' basis." *Hedges*, 2012 WL 1721124, at *22, *citing Rybicki*, 354 F.3d at 129; *accord United States v. Whittaker*, 999 F.2d 38, 42 (2d Cir.1993). Here, Mr. Ulbricht's vagueness challenge includes a First Amendment component, as well as a separate First Amendment overbreadth element, but with respect to the former nevertheless asserts an "as applied" rather than "facial" basis. *See* **post**, at 35-37.

expression sheltered by the First Amendment, the doctrine demands a greater degree of specificity than in other contexts." *Farrell*, 449 F.3d at 486.

In *NAACP v. Button*, the Supreme Court further explained the different presumptions that apply when First Amendment activities are at issue:

> [i]f the line drawn by the decree between the permitted and prohibited activities of the NAACP, its members and lawyers is an ambiguous one, we will not presume that the statute curtails constitutionally protected activity as little as possible. For standards of permissible statutory vagueness are strict in the area of free expression.

371 U.S. at 432. *See also Kolender v. Lawson*, 461 U.S. 352, 357 (1983).

When Congress has condemned non-speech activity – providing material support to terrorists – and an individual is accused of performing such conduct through speech, the individual acts that are alleged to be criminal must be scrutinized to avoid unconstitutional overreaching into First Amendment protected activity. *Dennis v. United States*, 341 U.S. 494, 505 (1951). *See also Yates v. United States*, 354 U.S. 298, 322-23 (1957).

2. *The Overbreadth Doctrine*

As the Second Circuit explained in *Farrell v. Burke*, "[o]verbreadth challenges are a form of First Amendment challenge and an exception to the general rule against third-party standing." 449 F.3d at 498, *citing Broadrick v. Oklahoma*, 413 U.S. 601, 601-12 (1973). As a result, "[a] party alleging overbreadth claims that although a statute did not violate his or her First Amendment rights, it would violate the First Amendment rights of hypothetical third parties if applied to them." *Id*., *citing Broadrick*, 413 U.S. at 612. *See also American Booksellers Foundation v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) ("[i]n the context of the First Amendment, a party whose speech could be constitutionally regulated is permitted to challenge a statute based

on its overbreadth, the fact that the statute regulates not only their unprotected speech but also a substantial amount of protected speech") (citation omitted).

As the Second Circuit has stated, "[a] law is overbroad, and hence void, if it 'does not aim specifically at evils within the allowable area of State control, but, on the contrary, sweeps within its ambit other activities that . . . constitute an exercise of freedom of speech or of the press.'" *United States v. Rahman*, 189 F.3d 88, 115 (2d Cir. 1999), *quoting Thornhill v. Alabama*, 310 U.S. 88, 97 (1940).[14]

Ultimately, "[w]hen a court finds that a statute suffers from such substantial overbreadth, all enforcement of the statute is generally precluded." *American Booksellers*, 342 F.3d at 104. Also, "[a]ll overbreadth challenges are facial challenges, because an overbreadth challenge by its nature assumes that the measure is constitutional as applied to the party before the court." 449 F.3d at 498.

However, as the Second Circuit noted in *Farrell*, "[o]verbreadth and vagueness are different doctrines." 449 F.3d at 498. In fact, "'[a] clear and precise enactment [for vagueness purposes] may nevertheless be "overbroad" if in its reach it prohibits constitutionally protected conduct.'" *Grayned v. City of Rockford,* 408 U.S. at 114. Thus, as in *Farrell*, even an unsuccessful vagueness challenge will

> not be a barrier to [an] overbreadth challenge[], because overbreadth challenges are based upon the hypothetical application of the statute to third parties. A plaintiff claiming overbreadth need not show that the challenged regulation injured his or her First Amendment interests in any way in order to bring the

[14] In *Rahman*, which involved charges of seditious conspiracy, the Court noted that while speech can be regulated by such statutes, "political speech and religious exercise are among the activities most jealously guarded by the First Amendment." 189 F.3d at 117.

> overbreadth challenge.

449 F.3d at 498-99.

In *Farrell*, the Court instructed that "[i]n order to prevail on an overbreadth challenge, 'the overbreadth of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep.'" *Id*., at 499, *quoting Broadrick*, 413 U.S. at 615. In performing overbreadth analysis, a court,

> [a]s with facial vagueness challenges, [] must consider not only conduct clearly prohibited by the regulation but also conduct that arguably falls within its ambiguous sweep. The purpose of an overbreadth challenge is to prevent the chilling of constitutionally protected conduct, as prudent citizens will avoid behavior that *may* fall within the scope of a prohibition, even if they are not entirely sure whether it does.

Id., at 499 (emphasis in original).[15]

Also, the canons of statutory construction dictate that Mr. Ulbricht's "as applied" challenge be considered first. In *American Booksellers Foundation*, 342 F.3d at 105, the Court stated, "[a]s the Supreme Court held in *Board of Trustees v. Fox*, it is 'generally [not] desirable [ ] to proceed to an overbreadth issue unnecessarily.' 492 U.S. 469, 484-85 (1989). Thus, 'the lawfulness of the particular application of the law should ordinarily be decided first.' *Id.* at 485; *see also Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 504 (1985)." *See also Broadrick*, 413 U.S. at 613 (if the statute is overbroad, it may not be enforced "until and unless a limiting construction or partial invalidation so narrows it as to remove the seeming threat or deterrence to

---

[15] As with the vagueness challenge in *Farrell*, the overbreadth challenge failed for reasons entirely distinguishable from the circumstances here: "First Amendment rights as a paroled sex offender were circumscribed, and because [he] was the only person affected by the Special Condition, we cannot say that the Special Condition's overbreadth was both real and substantial in relation to its plainly legitimate sweep." 449 F.3d at 499.

constitutionally protected expression").[16]

3. *If the Statutes At Issue Herein Cover Mr. Ulbricht's Alleged Conduct, They Are Unconstitutional As Applied to Him In This Case*

As demonstrated **ante** in the analysis of the breadth of the statutes at issue in this case, and their traditional, and in many instances, *exclusive*, usage, if they apply to the conduct alleged against Mr. Ulbricht in the Indictment, those statutes are unconstitutional as applied. The foregoing analysis in sections A, B, C, and D of this Point (which will not be repeated here) establish that §846, §848(a), and §1030 did not provide notice to Mr. Ulbricht, the alleged operator of a web site, that the conduct alleged against him would be covered by those statutes.

In addition, in light of the lack of a single prosecution of a search engine, ISP, or browser for accommodating web sites and/or activity that involve illegal conduct, application of the statutes at issue here would constitute arbitrary and discriminatory enforcement. Indeed, the gulf between civil immunity enjoyed by all other internet providers and the criminal liability and potential punishment Mr. Ulbricht faces is incalculably vast.

Moreover, application of those statutes herein would render them overbroad, as they would undoubtedly chill First Amendment activity on the internet that Congressional policy, via §230, seeks instead to foster, "as prudent citizens will avoid behavior that *may* fall within the scope of a prohibition, even if they are not entirely sure whether it does." *Farrell*, 449 F.3d at 499.

Accordingly, for all the reasons set forth above, it is respectfully submitted that Counts

---

[16] Accordingly, in *American Booksellers*, the Court followed "'the normal rule that partial, rather than facial, invalidation is the required course," and leave for another day an overbreadth challenge to the statute. 342 F.3d at 105, *quoting Brockett*, 472 U.S. at 504.

One, Two, and Three should be dismissed.

POINT II

COUNT THREE SHOULD BE DISMISSED BECAUSE THE CRITICAL STATUTORY TERM "ACCESS WITHOUT AUTHORIZATION" IN §1030(a)(2)(C) IS UNDEFINED, AND THEREFORE UNCONSTITUTIONALLY VAGUE AS APPLIED TO MR. ULBRICHT IN THIS CASE

Congress's primary motivation in enacting the CFAA, the first federal computer crime law, in 1984 was to criminalize "the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695. *See also* S. Rep. No. 99-432, at 7-12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-90 (CFAA is a computer trespass statute that prohibits breaking into a computer much like physical trespass laws prohibit breaking into a home).

The House Judiciary Committee, in recommending enactment of 18 U.S.C. §1030, explained that the newfound ability of "hackers" to use personal computers to circumvent "identification code/password system[s]" had enabled a "recent flurry of electronic trespassing incidents." 1984 U.S.C.C.A.N. at 3696 (describing the hacker threat by reference to the film WAR GAMES (1983), "show[ing] a realistic representation of the … access capabilities of the personal computer"). Targeting this conduct, the Committee added, "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." 1984 U.S.C.C.A.N. at 3706.

Accordingly, when 18 U.S.C. § 1030 was enacted in 1984, it was narrowly limited to computer misuse to obtain national security secrets or personal financial records, or hacking into

government computers. *Id.* Since that time, and despite its originally narrow focus on criminalizing hacking into government computers or financial institution servers, a series of amendments (the first of which were passed just two years after the CFAA's enactment) have vastly expanded the CFAA to potentially criminalize everyday computer use.

In 1996, Congress dramatically expanded the CFAA by extending its reach to any "protected computer," a term that included any computer "which is used in interstate or foreign commerce or communication[.]" 18 U.S.C. § 1030(e)(2) (Supp. II 1996). The 1996 amendments also expanded §1030(a)(2) – which originally prohibited only unauthorized access to obtain financial records from financial institutions, card issuers, or consumer reporting agencies – to include unauthorized access to obtain *any* information of *any* kind from any "protected computer." 18 U.S.C. § 1030(a)(2) (Supp. II 1996).

The stated purpose of expanding the CFAA's scope was to protect additional types of "vital" private information from hacking, rather than just credit records and financial information:

> Section 1030(a)(2) currently gives special protection only to information on the computer systems of financial institutions and consumer reporting agencies, because of their significance to our country's economy and the privacy of our citizens. Yet, increasingly computer systems provide the vital backbone to many other industries, such as transportation, power supply systems, and telecommunications. [Thus, t]he bill would amend section 1030(a)(2) and extend its coverage to information held on (1) Federal Government computers and (2) computers used in interstate or foreign commerce on communications, if the conduct involved an interstate or foreign communication.

S. Rep. No. 104-357, at 7 (1996), 1996 WL 492169.

The language employed in the 1996 amendments essentially extended §1030(a)(2) to *any*

unauthorized access of a computer occurring over the Internet, since the legislature had already interpreted "obtain[ing]" information to include simply reading it, and because nearly all Internet communications are interstate communications. *See* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. Ill. J.L. Tech. & Pol'y 429, 433 (2009); *see also United States v. Fowler*, ____ F.Supp.2d ____, 2010 WL 4269618, at *2 (M.D. Fla. Oct. 25, 2010) (listing cases).

Thus, combined with the ubiquitous use of computers, smartphones, tablets, or any other Internet-enabled device in today's world, the breadth of the CFAA, as it stands today, places special importance on the meaning of "authorization," such that a broad construction of "authorization" potentially criminalizes an enormous amount of routine Internet activity and would, render the CFAA unconstitutionally vague.

Indeed, in the context of an Internet user's access to information on a public website, judicial efforts to construe "authorization" under § 1030(a)(2)(C) have failed to date to provide clear guidance to courts or ordinary citizens within the CFAA's reach. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2007) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive.").

The root of the problem is that restricting access to publicly-viewable information on the Internet based on subjective notions of consent inevitably fails to provide adequate notice to computer users, and criminalizes common Internet use. For example, the Fifth Circuit has approached the "authorization" question by reference to whether a user's access constitutes an "intended use" of a computer owner or website host. *See United States v. Phillips*, 477 F.3d 215,

220 (5th Cir. 2007) (analyzing "scope of a user's authorization to access a protected computer on the basis of the expected norms of the intended use or the nature of the relationship established between the computer owner and the user"); *see also United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010).

This approach, which prohibits accessing public websites based on the intention of the website host (whether communicated or not), has disturbing implications. Also, the divergent opinions on these issues, *see, e.g.*, *Nosal*, 676 F.3d at 856-64 (holding such use as criminalized in *John* did not violate the statute), sows confusion and essentially guarantees arbitrary and discriminatory enforcement.

Other courts have adopted a different approach to the "authorization" question, adopting a standard under which a computer user lacks authorization to access a computer if the user's access violates a website's terms of use. *See e.g.*, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003) (noting that a lack of authorization could be established by a violation of "an explicit statement on the website restricting access"); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000).

But that standard is also flawed because it allows "behavior that wasn't criminal yesterday [to] become criminal today without an Act of Congress, and without any notice whatsoever." *Id.* at 862. Since there are no other textual limitations on the scope of conduct prohibited under §1030(a)(2), the terms-of-use standard makes "section 1030(a)(2)(C) [into] a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]." *Drew*, 259 F.R.D. 449, 467 (C.D.Cal. 2009), *citing City of Chicago v. Morales*, 527 U.S. 41, 64 (1999).

So construed, the statute would be unconstitutionally vague under the Due Process Clause, as it would constitute a trap "for the wary as well as the unwary." *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1048-51 (1991). Accordingly, and in light of the attenuated nature of the conduct alleged against Mr. Ulbricht (discussed **ante**, throughout POINT I), the CFAA is unconstitutionally vague as applied to him here.

POINT III

COUNT FOUR SHOULD BE DISMISSED BECAUSE IT FAILS TO ALLEGE SUFFICIENTLY THE ESSENTIAL ELEMENT OF A "FINANCIAL TRANSACTION[]," WHICH MUST INVOLVE EITHER "FUNDS" OR A "MONETARY INSTRUMENT[]," NEITHER OF WHICH INCLUDES BITCOIN WITHIN §1956'S DEFINITIONS

Count Four, which charges Mr. Ulbricht with participating in a money laundering conspiracy in violation of 18 U.S.C. §1956(h), must be dismissed because the allegation lacks an essential element: that the "financial transactions" alleged involved "monetary instruments." As demonstrated below, confirmed by formal publications issued by the Internal Revenue Service (hereinafter "IRS") and the Department of the Treasury's Financial Crimes Enforcement Network (hereinafter "FinCEN"), Bitcoins, the exclusive means of payment on Silk Road, do *not* qualify as "monetary instruments," and therefore cannot serve as the basis for a money laundering violation.

A. *The Relevant Provisions of the Money Laundering Statute, 18 U.S.C. §1956*

The operative conduct description of a violation of §1956 as alleged in the Indictment is set forth in §1956(a)(1):

> Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

In turn, as provided in §1956(c)(4),

> the term "financial transaction" means
>
> (A) a transaction which in any way or degree affects interstate or foreign commerce
>
> (i) involving the movement of funds by wire or other means or
> (ii) involving one or more monetary instruments, or
> (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or
>
> (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree[.]

The term "monetary instruments" is defined in §1956(c)(5) as

> (i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or
> (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery[.]

See also United States v. Hassan, 578 F.3d 108, 127 (2d Cir. 2009) (discussing elements of a §1956 violation).

The importance of a "monetary instrument" to the violation of §1956 is manifest from the title of the statute: "Laundering of monetary instruments."

B. *The Money Laundering Allegations In Count Four of the Indictment*

Count Four charges that the violation of §1956 involved "financial transactions," *see* Indictment, at ¶¶ 20 (twice) & 21 (twice) (pp. 8-9). The Indictment also alleges that Bitcoin constituted the exclusive "payment system that served to facilitate the illegal commerce conducted on the [Silk Road] site[.]" *Id*., at ¶ 18 (p. 7).

C. *Bitcoin and the Features of Digital Currencies*

As noted by the Congressional Research Service (hereinafter "CRS") in its cogent history and explanation of Bitcoin, Bitcoin is a decentralized, pseudonymous, digital crypto-currency – it is not backed by any nation or central bank, it can be used without the user revealing to the other party his or her identity, it exists in the virtual and not corporeal world, and is based on a cryptographic formula that is designed to facilitate a public record of all Bitcoin transactions and thereby thwart duplication and fraud. *See* Craig K. Elwell, M. Maureen Murphy, and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," *Congressional Research Service*, December 20, 2013 (hereinafter "CRS Report"), available at <http://www.fas.org/sgp/crs/misc/R43339.pdf>.

Also, as CRS notes, "[u]nlike the dollar, a Bitcoin is not legal tender nor is it backed by any government or any other legal entity, nor is its supply determined by a central bank." *Id*., at 1. In addition, "[t]he Bitcoin system is private, but with no traditional financial institutions involved in transactions." *Id*. *See also id*., at 13 ("digital currencies are able to operate without involving a financial institution").

D. *Count Four Must Be Dismissed Because Bitcoins Do Not Qualify As "Funds" Under §1956(c)(4)(A)(i) or "Monetary Instruments" Under §1956(c)(5)*

As the CRS Report points out, it "identified some federal statutes and regulatory regimes that may have some applicability to digital currency, although none contains explicit language to that effect or explicitly mentions currency not issued by a government authority." *Id*., at 9. *See also* Anthony S. Barkow and Nathaniel H. Benforado, "Bitcoin: What It Is and How It's Regulated In the U.S.," *The New York Law Journal*, February 24, 2014, at 2 (hereinafter "Barkow and Benforado"), available at <http://www.newyorklawjournal.com/id=1202643086826/bitcoin+what+it+is+and+how+its+regulated+in+the+us?mcode=0&curindex=0&curpage=all> ("most U.S. regulators have not issued formal guidance or regulations directly addressing Bitcoins or other similar virtual currencies").

1. *The IRS and FinCEN Publications*

However, that was before the IRS issued a Notice earlier this week. *See* Notice 2014-21 (attached hereto as Exhibit 1, and available at <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>). In that Notice, the IRS confirmed that virtual currency "does not have legal tender status in any jurisdiction." *Id*., at 1. Also, in a "Frequently Asked Questions" section of the Notice, the IRS announced its policy position that (1) "virtual currency is treated as property." *Id*., at 2 (A-1); and (2) "virtual currency is not treated as currency . . ." *Id*. (A-2).

The IRS would not, however, adopt a position as to what *type* of property Bitcoin constituted, stating only that "[t]he character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer." *Id*., at 3 (A-7, which proceeds to provide examples of capital assets and non-capital assets without classifying virtual currencies).

The CRS Report had presaged the IRS's decision, pointing out that a General Accounting

Office report "also notes that the tax code lacks clarity about how virtual currency is to be treated for reporting purposes. It is property, barter, foreign currency, or a *financial instrument*?" CRS Report, at 10 (emphasis added). Clearly, according to the IRS, Bitcoin is the first (property) and *not* the last (a financial instrument).

Prior to the IRS's Notice, FinCEN had issued in March 2013 "guidance" with respect to virtual currencies. *See* U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Guidance, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013 (hereinafter "FinCEN Guidance"), available at <http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html>.

FinCEN's Guidance notes that "FinCEN's regulations define current (also referred to as 'real' currency) as 'the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." *Id.*, at 1.

FinCEN's Guidance proceeds to distinguish virtual currencies: "[i]n contrast to real currency, 'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." *Id.* Notably, "virtual currency does not have legal tender status in any jurisdiction." *Id.*

FinCEN's Guidance was explicitly designed to address FinCEN's regulations implementing the Bank Secrecy Act (hereinafter "BSA"), particularly those affecting a money service business (hereinafter "MSB"). *See* CRS Report, at 14 ("FinCEN issued interpretative guidance[] requiring Bitcoin exchanges – individuals and businesses that exchange Bitcoins into U.S. or foreign currency into Bitcoins – to register as money services businesses pursuant to the

BSA").[17]

However, commentators have certainly noticed that the Bitcoin issue "reveals a potential gap in international enforcement regimes[,]" and have remarked that "the U.S. money laundering statutes contain terms such as 'monetary instrument' and 'monetary transaction' that are defined as coin or currency of the U.S. or any other country[,]" concluding that "these terms arguably do not apply to bitcoins." Nicholas M. De Feis and Phillip C. Patterson, "Bitcoins: 'Illegal Tender' or Currency of the Future?" *The New York Law Journal*, January 30, 2014 (hereinafer "DeFeis and Patterson"), available at <http://www.newyorklawjournal.com/cs/Satellite?c=Article_C&childpagename=NY%2FArticle_C%2FArticle%2FLayouts%2FPrinterFriendly&pagename=ALM_Wrapper&cid=1202640562564#>.[18]

Indeed, all the recent coverage of bitcoins, and analysis of its regulatory status, mention *this case* (as well as two other Silk Road-related prosecutions in this District) as the first instance of criminal prosecution of Bitcoin use in the internet marketplace. *See, e.g.*, Barkow and

---

[17] The provisions of the Bank Secrecy Act and the regulations governing MSB's are not pertinent here because (a) the Indictment does not charge violations of the BSA; and (b) Silk Road would not be covered under those regulations because it did not perform the functions that would have classified it as an MSB.

[18] Demonstrating further the confusion and uncertainty regarding bitcoin's status, in December a Norwegian official reportedly stated that "Bitcoin would not be called money and would be treated as an investment asset." Nathaniel Popper and Neil Gough, "Bitcoin, Nationless Currency, Still Feels Governments' Pinch," *The New York Times*, December 19, 2013, available at <http://dealbook.nytimes.com/2013/12/18/bitcoin-collides-with-government-concerns/?_php=true&_type=blogs&_r=0>. Also, in December 2013, China's central bank banned Chinese banks from accepting bitcoins. *Id*.

Benforado; DeFeis and Patterson.[19]

2. *Bitcoin Does Not Qualify As Either "Funds" or "Monetary Instruments"*

As noted **ante**, a violation of §1956 requires a "financial transaction," and the Indictment employs that construction as well. Under §1956's definitional sections, a "financial transaction" requires the involvement of either "funds" [§1956(c)(4)(A)(i)], or "monetary instruments" [§1956(c)(4)(A)(ii)], or "transfer of title to any real property, vehicle, vessel, or aircraft," [§1956(c)(4)(A)(iii)], or the use of a "financial institution" [§1956(c)(4)(A)(iv)].

Bitcoin does not qualify under any prong of that definition. Both IRS and FinCEN have categorically declared that Bitcoins are not "funds." Also, a "monetary instrument" is either "coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders," §1956(c)(5)(i) – again, negated by IRS's and FinCEN's pronouncements – or "investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery[,]" §1956(c)(5)(ii) – a character neither IRS nor FinCEN has ascribed to Bitcoin.

Thus, an essential element of §1956 – a "financial transaction" – is absent because a necessary component thereof – either "funds" or "monetary instruments" – is lacking. Consequently, it is respectfully submitted that Count Four must be dismissed.

---

[19] The Securities and Exchange Commission had previously instituted a civil action – alleging a Ponzi scheme – against an investment firm that touted bitcoins to its customers as an investment vehicle in a fraudulent manner. *See SEC v. Shavers*, 2013 WL 4028182 (E.D. Tx. August 6, 2013). As noted in the CRS Report, at 11, in *Shavers* the SEC convinced a judge Bitcoin was money (and qualified as a "security"), but that decision is now in irreconcilable conflict with the policies of both IRS and FinCEN.

Conclusion

Accordingly, for all the reasons set forth above, it is respectfully submitted that Mr. Ulbricht's pretrial motions addressing the face of the Indictment should be granted in their entirety, and the Indictment against him dismissed.

Dated: 28 March 2014
New York, New York

/S/ Joshua L. Dratel
JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Attorneys for Defendant Ross Ulbricht