

Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.148

<http://tlp.law.pitt.edu>

Cyber-Takings: The War on Crime Moves into the Cloud

Larry McIntyre



This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.



This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

Cyber-Takings: The War on Crime Moves into the Cloud

Larry McIntyre*

[P]rocedural devices rooted in experience were written into the Bill of Rights not as abstract rubrics in an elegant code but in order to assure fairness and justice before any person could be deprived of “life, liberty, or property.”¹

INTRODUCTION

Recent advances in the reliability and availability of broadband Internet connections have allowed technology users to store vast amounts of data remotely.² Cloud services now commonly sync photos, videos, emails, contacts, and other documents across multiple devices. Our craving for ubiquitous access to data, however, is not without limitation. At the forefront of the debate surrounding these services are concerns about privacy and security.³ The thought of a third party gaining access to our private data is understandably troubling. Yet, these concerns frequently overlook the possibility that our digital life may become collateral damage in the course of a criminal investigation. Such digital asset seizures are becoming increasingly prevalent⁴ as the Obama administration increases its use of existing civil forfeiture laws in an effort to deter cybercrime.⁵

Part I of this article discusses the scope of the federal government’s asset forfeiture authority under various statutes, and examines the social and political

* Larry McIntyre is a J.D. candidate at the University of Pittsburgh School of Law, 2015.

¹ Adams v. United States *ex rel.* McCann, 317 U.S. 269, 276 (1942).

² Quentin Hardy, *Big Data Picks Up the Pace*, NEW YORK TIMES, Mar. 5, 2014, http://bits.blogs.nytimes.com/2014/03/05/big-data-picks-up-the-pace/?_php=true&_type=blogs&_r=0.

³ See, e.g., Rosa Golijan, *Is your cloud drive really private? Not according to fine print*, NBC NEWS (Mar. 15, 2013), <http://www.nbcnews.com/tech/internet/your-cloud-drive-really-private-not-according-fine-print-f1C8881731>.

⁴ See Nate Anderson, “*Crime is Crime*”: *Meet the Internet Police*, ARS TECHNICA (Jan. 21, 2011, 5:01 PM), <http://arstechnica.com/tech-policy/2011/01/crime-is-crime-meet-the-internet-police>.

⁵ Exec. Office of the President, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* 20 (July 19, 2011), available at <http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf>.

context leading to their enactment. Part II examines the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act),⁶ a federal statute, which increases both civil and criminal penalties for copyright infringement.⁷ Part III analyzes two notable criminal prosecutions, and distinguishes them from cases that do not involve digital assets.⁸ Part IV argues government seizures of digital assets may implicate the Fifth Amendment's takings clause. Finally, Part V concludes by finding that digital asset forfeitures constitute Fifth Amendment takings.

I. FEDERAL FORFEITURE

Asset forfeiture laws allow the government to permanently deprive an owner of his or her property rights when either the property itself has been used as “an instrumentality of crime,” or “the owner of the property has been involved in a criminal activity.”⁹ Forfeiture is a method by which the government can, without compensation, take title to, or possession over property that has been tainted by a crime.¹⁰ During civil asset forfeitures, this process may take place entirely outside of or without a criminal prosecution.¹¹

Civil asset forfeitures operate *in rem* and are based upon a theory that the property itself is guilty of wrongdoing.¹² Accordingly, the civil forfeiture has become a powerful tool for law enforcement agencies and allows the government to take private property without paying compensation, but does not correspondingly impose the burden of proving an owner's guilt beyond a reasonable doubt.¹³ In the United States, no single statute grants the government general authority to seek civil forfeiture of property gained from, or otherwise

⁶ Pub. L. No. 110-403, 122 Stat. 4256 (2008) (codified in scattered sections of 15 U.S.C., 17 U.S.C., and 18 U.S.C.).

⁷ 18 U.S.C. § 2319 (2012).

⁸ Indictment, *United States v. Dotcom*, No. 1:12CR3 (E.D. Va. Jan. 5, 2012); Sealed Complaint, *United States v. Ulbricht*, No. 13 Mag. 2328 (S.D.N.Y. Sept. 27, 2013).

⁹ *Bennis v. Michigan*, 516 U.S. 442, 453–55 (1996) (Thomas, J., concurring).

¹⁰ Stefan D. Cassella, *Overview of Asset Forfeiture Law in the United States*, 55 U.S. ATT'Y BULL. 8, 8 (2007), available at http://www.justice.gov/usao/eousa/foia_reading_room/usab5506.pdf.

¹¹ In contrast, criminal forfeiture proceedings generally occur during the sentencing phase of a criminal trial. *See id.*

¹² *Id.*

¹³ *Id.*

involved in, the commission of crime.¹⁴ Instead, statutes for specific criminal offenses must allow for asset forfeitures.¹⁵

A. *Our Turbulent History of Zero Tolerance*

In his first State of the Union address, Richard Nixon famously promised to win the “war against crime.”¹⁶ The President called on Congress to pass legislation that would give law enforcement agencies “new and stronger weapons” to eliminate street-level crime.¹⁷ Later that year, Congress enacted the first federal statutes to specifically include asset forfeiture provisions.¹⁸ The first of these statutes, the Racketeer Influence and Corrupt Organization Act of 1970 (hereinafter “RICO”) allows for forfeiture of assets connected to racketeering and organized crime.¹⁹ The second statute, the Comprehensive Drug Abuse Prevention and Control Act of 1970 (hereinafter the “CDAPCA”), permits forfeiture of assets connected to violations of the Controlled Substances Act.²⁰ State enactment of comparable statutes soon followed.²¹ Nixon’s vehement rhetoric continued to intensify until his presidency came to an abrupt conclusion in 1974.²²

Just eight years after its enactment, the CDAPCA was amended to include broader categories of property that could be forfeited to the government.²³ Through this Amendment, Congress gave federal law enforcement officers the power to seek forfeiture of: “all moneys, negotiable instruments, securities, or other things of

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Richard Nixon: Annual Message to the Congress on the State of the Union*, UCSB, <http://www.presidency.ucsb.edu/ws/?pid=2921> (last visited Feb. 18, 2014).

¹⁷ *Id.*

¹⁸ Racketeer Influenced and Corrupt Organizations, 18 U.S.C. §§ 1961-1968 (1970); Comprehensive Drug Abuse Prevention and Control Act of 1970 (CDAPCA), 21 U.S.C. §§ 801-971 (2012).

¹⁹ Racketeer Influenced and Corrupt Organizations, 18 U.S.C. §§ 1961-1968 (1970).

²⁰ Comprehensive Drug Abuse Prevention and Control Act of 1970 (CDAPCA), 21 U.S.C. §§ 801-971 (2012).

²¹ *See, e.g.*, 42 PA. CONS. STAT. §§ 6801-6802 (2012).

²² At one point, Nixon brazenly designated drug abuse as “America’s public enemy number one.” *See Richard Nixon: Remarks About an Intensified Program for Drug Abuse Prevention and Control*, UCSB, <http://www.presidency.ucsb.edu/ws/index.php?pid=3047#axzz1PCJydj15> (last visited Feb. 18, 2014).

²³ Psychotropic Substances Act of 1978, Pub. L. No. 95-633, § 3301, 92 Stat. 3768 (codified at 21 U.S.C. § 881(a)(6) (1988)).

C Y B E R - T A K I N G S

value.”²⁴ The CDAPCA, which was further amended in 1984,²⁵ presently allows for forfeiture of virtually all categories of private property.²⁶

B. Use and Abuse

The list of reported abuses of this formidable tool is far too lengthy to detail fully.²⁷ Some of the more notable stories are, nevertheless, illustrative. One recent example occurred in Texas, when Jennifer Boatright was taken into custody, along with her two sons, while on the way to purchase a used car.²⁸ According to police, Boatright, a Latina, fit the profile of a drug courier.²⁹ Although no drugs were found in the vehicle, the local district attorney presented Boatright with two options, she could be prosecuted for money laundering and child endangerment, or she could agree to forfeit the cash officers had found in her vehicle.³⁰ Boatright signed her hard-earned savings over to the city, and in return no criminal charges were filed.³¹ In another comparable example from a case in Philadelphia, police sought forfeiture of the home of Mary and Leon Adams after their adult son was accused of selling \$20 worth of marijuana to a confidential informant on the couple’s front porch.³² Stories like these share one commonality, the displacement of traditional principles of due process, which are fundamental to the American justice system.

In response to widespread criticism of civil asset forfeitures, Congress passed the Civil Asset Forfeiture Reform Act of 2000 (hereinafter “CAFRA”).³³ CAFRA prevents government agents from forfeiting assets on the basis of probable cause.³⁴ Under CAFRA, before the government is permitted to seize assets, the government must specifically demonstrate by a preponderance of evidence that there is a

²⁴ *Id.*

²⁵ Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976 (1984).

²⁶ See 21 U.S.C. § U881(a)(1)–(11) (2012).

²⁷ See Sarah Stillman, *Taken*, NEW YORKER (Aug. 12, 2013), http://www.newyorker.com/reporting/2013/08/12/130812fa_fact_stillman. See also Isaiah Thompson, *Law to Clean Up ‘Nuisances’ Costs Innocent People Their Homes*, PROPUBLICA (Aug. 5, 2013, 5:39 AM), <http://www.propublica.org/article/law-to-clean-up-nuisances-costs-innocent-people-their-homes>.

²⁸ Stillman, *supra* note 27.

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ 18 U.S.C. § 983 (2012).

³⁴ *Id.*

substantial connection between the crime and the property.³⁵ CAFRA also authorizes the appointment of counsel for any person who has standing to contest a civil forfeiture, but who is unable to afford private representation.³⁶

Perhaps the most important reform within CAFRA, is the creation of an innocent owner defense.³⁷ When the innocent owner defense, which is an affirmative defense, is applicable, an innocent third party's ownership interest in property will not be forfeited.³⁸ The burden is on the innocent party to establish by a preponderance of the evidence that he or she either (1) "did not know of the conduct giving rise to forfeiture," or (2) "did all that reasonably could be expected under the circumstances to terminate such use of the property."³⁹ Courts are split in their application of this defense, which often requires a largely subjective "reasonableness" determination.⁴⁰ As a result, over 80% of all forfeitures still go uncontested even after CAFRA's enactment.⁴¹ In fact, as demonstrated by Jennifer Boatright's, many innocent individuals often refrain from challenging a forfeiture because they are afraid doing so will lead to criminal charges.⁴²

Even though CAFRA provides individuals with a way to challenge forfeitures federally, CAFRA does nothing to inhibit individual states from engaging in civil asset forfeitures.⁴³ States are therefore permitted to enact their own forfeiture laws, which can be either more stringent or more lenient than CAFRA. In Pennsylvania, for example, asset forfeiture laws are comparable to their federal counterparts and do not provide any more leniency in asset forfeiture.⁴⁴ When grading states' forfeiture laws, the Institute for Justice specifically gave the Commonwealth of Pennsylvania a "D."⁴⁵ This grade came in large part from the fact that even though

³⁵ See *id.* § 983(c) (2012).

³⁶ *Id.* § 983(b)(1).

³⁷ 18 U.S.C. § 983(d) (2012).

³⁸ *Id.* § 983(d)(1).

³⁹ *Id.* § 983(d)(2).

⁴⁰ See generally Cassella, *supra* note 10.

⁴¹ *Id.* at 12, 72 (explaining that contested civil forfeitures "provide the government with greater discovery tools and afford the government a right to depose and otherwise take broad civil discovery.").

⁴² See 18 U.S.C. § 1983(a)(3) (2012) (explaining that when an administrative forfeiture is contested the government may either bring a civil forfeiture or a criminal forfeiture).

⁴³ See generally 18 U.S.C. § 983 (2012).

⁴⁴ See, e.g., 42 PA. CONS. STAT. §§ 6801–6802 (2012).

⁴⁵ *Asset Forfeiture Report: Pennsylvania*, INSTITUTE FOR JUSTICE, <http://www.ij.org/asset-forfeiture-report-pennsylvania> (last visited Feb. 12, 2014). See also Isaiah Thompson, *The Cash*

CYBER - T A K I N G S

Pennsylvania's statute provides an all-encompassing grant of authority for asset forfeiture, some trial courts have shown principled restraint in engaging in forfeitures, while some police officials have not.⁴⁶ Allegheny County trial courts, for instance, exercised sufficient restraint whereby the policy was "we had to have a [criminal] conviction and it had to make some reasonable sense why we were going after forfeiture."⁴⁷ Alternatively, police departments such as the Pittsburgh Police have exceeded the encompassing grant of authority involving asset forfeitures.⁴⁸ Recent audits have revealed that the Pittsburgh Police Department has routinely failed to comply with the statutory requirement that forfeiture funds be used only for narcotics-related investigations.⁴⁹ This evidenced by one particularly egregious instance where in 2009, the Pittsburgh Police Department spent approximately \$10,000 of forfeited funds on Gatorade.⁵⁰ Similarly, over \$4,000 of forfeited funds were used to send three bureau employees to Miami in 2012.⁵¹

II. FORFEITURE OF DIGITAL ASSETS

On October 13, 2008, George W. Bush signed the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (hereinafter "the PRO-IP Act").⁵² Content rights-holders such as the Recording Industry Association of America ("RIAA") and the Motion Picture Association of America ("MPAA") staunchly supported the legislation.⁵³ The PRO-IP Act amended existing copyright law to specifically include civil and criminal forfeiture provisions.⁵⁴ Under the PRO-IP Act, the Department of Justice's forfeiture authority may be invoked when

Machine, PHILADELPHIA CITY PAPER (Nov. 28, 2012), <http://citypaper.net/article.php?The-Cash-Machine-19189> (explaining that "[a]s the role of forfeiture in Pennsylvania expanded [Allegheny] county's president judge ordered that forfeitures involving criminal matters be handled in criminal court").

⁴⁶ Thompson, *supra* note 27.

⁴⁷ *Id.*

⁴⁸ Liz Navratil, *Pittsburgh police misuse of drug fund cited*, PITTSBURGH POST-GAZETTE, Mar. 13, 2013, <http://www.post-gazette.com/neighborhoods-city/2013/03/13/Pittsburgh-police-misuse-of-drug-fund-cited/stories/201303130150>.

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Pub. L. No. 110-403, 122 Stat. 4256 (2008) (codified in scattered sections of 15 U.S.C., 17 U.S.C., and 18 U.S.C.).

⁵³ See Nate Anderson, *Big Content gloats as Bush signs PRO-IP Act*, ARS TECHNICA (Oct. 14, 2008, 2:48 PM), <http://arstechnica.com/tech-policy/2008/10/bush-signs-pro-ip-act-big-content-gloats>.

⁵⁴ See 18 U.S.C. § 2323 (2012).

the underlying crime is one of copyright infringement, trademark infringement, or misappropriation of trade secrets.⁵⁵

The PRO-IP Act specifically allows for civil forfeiture of (1) any prohibited articles, (2) property used or intended to be used “to commit or facilitate the commission of an offense,” and (3) “[a]ny property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).”⁵⁶ The PRO-IP Act’s forfeiture provision, however, was not a unique creation of the legislature. Rather, PRO-IP Act incorporated the statutory language used in the Comprehensive Drug Abuse Prevention and Control Act of 1970 (including subsequent amendments) by reference.⁵⁷

Armed with this new enforcement authority, a newly-created IP task force within the Department of Homeland Security got to work seizing website domain names.⁵⁸ On June 30, 2010, Immigration and Customs Enforcement (“ICE”) unveiled a new program to respond to counterfeiting and piracy on the Internet.⁵⁹ The program began with the seizure of ten websites, which were distributing newly released movies.⁶⁰ As time passed, the government’s appetite for seizing domain names swelled. “Operation Fake Sweep” yielded the seizure of 307 websites that had allegedly distributed counterfeit NFL merchandise.⁶¹ “Project Bitter Pill” led to the seizure of 686 websites purportedly selling counterfeit medications.⁶² By December 2013, 2,550 domain names had been seized since the program’s

⁵⁵ *Id.* § 2323(a)(1).

⁵⁶ *Id.* § 2323(a)(1)(A)–(C) (referring to the offenses of criminal copyright infringement, trafficking in counterfeit goods, and the unauthorized recording of Motion pictures).

⁵⁷ *See id.* § 2323(a)(2) (“The provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section.”); 21 U.S.C. § 881(b) (2012) (incorporating by reference the procedures from 18 U.S.C. § 8981(b)).

⁵⁸ *See, e.g.*, OFFICE OF PUBLIC AFFAIRS, DEPARTMENT OF JUSTICE, *Department of Justice Seizes More than \$896,000 in Proceeds from the Online Sale of Counterfeit Sports Apparel* (Apr. 10, 2012), available at <http://www.justice.gov/opa/pr/2012/April/12-crm-447.html> (discussing investigation and seizure of domain names engaged in sale of counterfeit goods).

⁵⁹ “Operation In Our Sites” targets Internet movie pirates, ICE, <http://www.ice.gov/news/releases/1006/100630losangeles.htm> (last modified June 30, 2010).

⁶⁰ *Id.*

⁶¹ *Special agents and officers seize more than \$4.8 million in fake NFL merchandise and seize 307 websites during ‘Operation Fake Sweep,’* ICE, <https://www.ice.gov/news/releases/1202/120202indianapolis.htm> (last modified Feb. 2, 2012).

⁶² *HSI seizes 686 websites selling counterfeit medicine to unsuspecting consumers,* ICE, <https://www.ice.gov/news/releases/1210/121004washingtondc.htm> (last modified Oct. 4, 2012).

C Y B E R - T A K I N G S

introduction 41 months earlier.⁶³ These seizures, however, were only the tip of the iceberg.

III. CHAOS IN THE COURTS

A. *Megaupload.com*

On January 19, 2012, Megaupload, one of the most popular file-sharing services on the Internet was shut down by the United States Department of Justice.⁶⁴ The FBI, working in tandem with various international agencies, executed more than twenty search warrants across nine countries throughout the investigation.⁶⁵ Megaupload's servers were seized along with eighteen associated domain names and approximately \$50 million in assets.⁶⁶ According to the subsequently unsealed grand jury indictment, the government sought forfeiture of among other things a Lamborghini LM002, a Rolls-Royce Phantom, a Maserati GranCabrio, 60 Dell servers, and dozens of international bank accounts.⁶⁷ Each of the seven defendants, including the aptly named CEO Kim Dotcom, were charged with conspiracy to commit racketeering, conspiracy to commit copyright infringement, and two counts of criminal copyright infringement.⁶⁸ Because copyright infringement is one that allows for civil forfeiture, forfeiture was allowed in this case.⁶⁹ Noticeably absent from the indictment is any reference to the non-infringing content stored on Megaupload's servers.⁷⁰ In fact, the government almost certainly has no intention to "use" such files, which were stored at the direction of third party users, in its prosecution. While the FBI may not have deliberately seized the data of every single Megaupload user, their stored files nevertheless became collateral damage in the sweep.

⁶³ *International law enforcement agencies seize 706 domain names selling counterfeit merchandise*, ICE, <https://www.ice.gov/news/releases/1312/131202washingtondc.htm> (last modified Dec. 2, 2013).

⁶⁴ Ben Sisario, *7 Charged as F.B.I. Closes a Top File-Sharing Site*, N.Y. TIMES, Jan. 19, 2012, <http://www.nytimes.com/2012/01/20/technology/indictment-charges-megaupload-site-with-piracy.html>.

⁶⁵ Naomi Tajitsu, *NZ court rules Megaupload warrant legal, dealing blow to Dotcom*, REUTERS (Feb. 18, 2014), <http://www.reuters.com/article/2014/02/19/us-newzealand-megaupload-warrant-idUSBREA1102F20140219>.

⁶⁶ Sisario, *supra* note 64.

⁶⁷ Indictment, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012).

⁶⁸ 18 U.S.C. § 81962(d) (2012); 18 U.S.C. § 9371 (2012); 18 U.S.C. § 71956(h) (2012); 18 U.S.C. § 92319 (2012).

⁶⁹ 18 U.S.C. § 2323 (2012).

⁷⁰ Indictment, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012).

Even legitimate users are prevented from accessing their stored data due to the FBI's seizure of Megaupload's domain names. One example is that of Kyle Goodwin, a former Megaupload customer, who used the service to store videos of high school sporting events.⁷¹ Goodwin's small business used Megaupload to store and distribute these video files.⁷² After the FBI's seizure, Goodwin filed a motion in the Eastern District of Virginia seeking the return of his property.⁷³ According to Goodwin, his personal hard drive crashed just days before federal authorities shut down the service.⁷⁴ As a result, Goodwin's non-infringing video files are presently stored somewhere among the 25 million gigabytes of data rendered inaccessible by the actions of the United States Government.⁷⁵

The sheer magnitude of users and files, which have been implicated in the Megaupload seizure, aptly illustrates the dichotomy between the forfeiture of physical assets and the forfeiture of digital assets. This case also reveals that the CAFRA reforms are of limited benefit when digital assets are at issue. For example, although the Act requires that counsel be made available to indigent claimants,⁷⁶ aggrieved property owners such as Goodwin are unlikely to qualify. This is because Goodwin does not have an ownership interest in the seized property (Megaupload's domain names) and therefore does not have standing to challenge the forfeiture.⁷⁷

Civil forfeitures are a tool of convenience for law enforcement, allowing them to seize first and ask questions later. The burden is then placed on the owner of the property to come into court and contest the forfeiture.⁷⁸ This system is no longer practicable when digital assets are involved, because many Internet services have a user base that is geographically spread across multiple continents. Although our courts have clear jurisdictional limits, the Internet does not. Therefore, it is no longer rational to argue the government is justified in making broad seizures simply because innocent users may challenge them in a United States District Court.

⁷¹ David Kravets, *Feds Say No Dice in Retrieving Your Data Seized in Megaupload Case*, WIRED (Oct. 31, 2012, 5:17 PM), <http://www.wired.com/threatlevel/2012/10/no-dice-megaupload-data>.

⁷² *Id.*

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ 18 U.S.C. § 8983(b)(1) (2012).

⁷⁷ *See* 18 U.S.C. § 983(b)(1) (2012).

⁷⁸ *See* *United States v. Ursery*, 518 U.S. 267, 296 (1996) (Kennedy, J., concurring).

Two years have passed since the initial Megaupload seizure and neither Goodwin nor any other user has been granted access to his or her non-infringing data.⁷⁹ Megaupload's hosting company has agreed to sell the leased servers to Megaupload for \$1,000,000, but the government rejected the plan by refusing to unfreeze any of the company's assets.⁸⁰ The government continues to argue it is not financially or logistically able to return Goodwin's property, and Goodwin should seek other remedies.⁸¹ Paradoxically, the government has requested a sealed *ex parte* order, which would allow them to share Megaupload's data with copyright industry groups such as the MPAA.⁸² The government argues that such disclosure is necessary to ensure that copyright holders can bring civil lawsuits against Megaupload before the statute of limitations expires.⁸³

B. Silk Road

For over two years, an underground website allowed visitors from across the world to buy and sell illegal drugs as easily as purchasing a book on Amazon.com.⁸⁴ Silk Road's revenue surpassed \$22 million in its first year of operation.⁸⁵ The FBI estimates that Ross Ulbricht, the website's alleged owner and operator, obtained over \$80 Million in commissions throughout his tenure.⁸⁶ As a technical matter, Silk Road and its operators sold nothing.⁸⁷ Rather, Silk Road was

⁷⁹ Mike Masnick, *US Court Secretly Lets Government Share Megaupload Evidence With Copyright Industry*, TECHDIRT (Dec. 6, 2013, 7:39 PM), www.techdirt.com/articles/20131206/02524925481/us-court-secretly-lets-government-share-megaupload-evidence-with-copyright-industry.shtml.

⁸⁰ David Kravets, *Feds Tell Megaupload Users to Forget About Their Data*, WIRED (June 11, 2012, 4:58 PM), <http://www.wired.com/threatlevel/2012/06/feds-megaupload-data>.

⁸¹ *Id.*

⁸² Masnick, *supra* note 79.

⁸³ The position of the Department of Justice in this case seems to be that legitimate users are not entitled to the return of their data, but that Hollywood is entitled to a copy. *See id.* (providing a more thorough examination of the Government's position).

⁸⁴ Andy Greenberg, *Black Market Drug Site 'Silk Road' Booming: \$22 Million In Annual Sales*, FORBES (Aug. 6, 2012, 2:28 PM), <http://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales>.

⁸⁵ *Id.*

⁸⁶ Sealed Verified Complaint 4, *United States v. Ulbricht*, 13 Civ. 6919 (S.D.N.Y. Sept. 27, 2013) [hereinafter Sealed Verified Complaint], available at <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2013cv06919/418116/4/0.pdf>.

⁸⁷ David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES, Jan. 18, 2014, <http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html>.

merely a marketplace, which connected buyers and sellers.⁸⁸ For Silk Road's trouble, they would retain a commission of 8–15% of the purchase price.⁸⁹

Even though Silk Road's business model was somewhat analogous to services like eBay and Craigslist, Silk Road's model was distinctive.⁹⁰ Unlike other services, Silk Road's home page was crowded with listings such as "10 x 10mg OxyContin" and "5G Pure Cocaine Cristal."⁹¹ Silk Road was accessible only to visitors using Tor, a free piece of software that makes it theoretically impossible to trace a user's genuine identity.⁹² Similarly, Silk Road did not accept credit cards, PayPal, or any other traditional forms of payment.⁹³ All Silk Road transactions were secured with a digital currency called Bitcoin.⁹⁴ Bitcoins are an anonymous, decentralized form of electronic currency that uses cryptography software to control their creation and transfer.⁹⁵

According to the FBI, Ulbricht made a series of calamitous slipups exposing his identity to federal agents who were, unsurprisingly, monitoring the site.⁹⁶ On October 1, 2013, Silk Road's walls came tumbling down. On that morning, the FBI took Ulbricht into custody at a public library in San Francisco.⁹⁷ Ulbricht was performing administrative maintenance on the site when agents moved in.⁹⁸ Critically, the FBI sought to detain Ulbricht before he could close his laptop thereby preventing the collection of valuable evidence.⁹⁹ Immediately after Ulbricht's arrest, visitors to the Silk Road website were no longer greeted with a

⁸⁸ Sealed Verified Complaint, *supra* note 86, at 4.

⁸⁹ *Id.*

⁹⁰ See Sealed Verified Complaint, *supra* note 86 (discussing the general nature of Silk Road's business).

⁹¹ Segal, *supra* note 87.

⁹² *Tor: Overview*, TOR PROJECT, <https://www.torproject.org> (last visited Feb. 18, 2014). See also Sealed Verified Complaint, *supra* note 86, at 3.

⁹³ Segal, *supra* note 87.

⁹⁴ Greenberg, *supra* note 84.

⁹⁵ Sealed Complaint, United States v. Ulbricht, No. 13 Mag. 2328 (S.D.N.Y. Sept. 27, 2013).

⁹⁶ See Segal, *supra* note 87.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

marketplace of mind altering substances, but were instead redirected to a FBI seizure notice.¹⁰⁰

The FBI seized all Bitcoins, which remained in Silk Road user accounts, as well as Ulbricht's personal stash of Bitcoins.¹⁰¹ On October 13, 2013, the United States posted a notice of forfeiture on its website at www.forfeiture.gov.¹⁰² Ulbricht subsequently filed a claim contesting the civil forfeiture of the Bitcoins found on his laptop.¹⁰³ Ulbricht's assertion is unsurprising considering the stockpile of Bitcoins seized has been valued at over \$130 million.¹⁰⁴ Not a single person, however, was daring enough to claim an ownership interest in any portion of the \$28 million, which had previously been held in individual user accounts on the Silk Road.¹⁰⁵ After District Judge J. Paul Oetken signed a final forfeiture order on January 15, 2014, the United States became the proud new owner of \$28 million worth of allegedly tainted digital currency.¹⁰⁶

The law of civil asset forfeitures allowed the government to avoid the impossible task of identifying each and every Silk Road user and subsequently demonstrating criminal culpability beyond a reasonable doubt.¹⁰⁷ The government was largely able to turn a blind eye to the actual owners of the \$28 million because the Bitcoins were viewed as defendants.¹⁰⁸ The government's allegation that the funds were involved in a money laundering conspiracy was therefore sufficient to

¹⁰⁰ *See id.*

¹⁰¹ Kashmir Hill, *The Feds Are Ready To Sell \$25 Million of Bitcoin Seized From The Silk Road*, FORBES (Jan. 16, 2014, 6:07 PM), <http://www.forbes.com/sites/kashmirhill/2014/01/16/the-feds-are-ready-to-sell-the-silk-road-bitcoin-kind-of>.

¹⁰² Partial Judgment by Default and Order of Forfeiture at 3, *United States v. Ulbricht*, No. 13 Civ. 6919 (S.D.N.Y. Jan. 15, 2014) [hereinafter Partial Judgment by Default], available at <http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2013cv06919/418116/19/0.pdf>.

¹⁰³ *Id.*

¹⁰⁴ Press Release, The United States Attorney's Office, Southern District of New York, Manhattan U.S. Attorney Announces Forfeiture of \$28 Million Worth of Bitcoins Belonging to Silk Road (Jan. 16, 2014) [hereinafter Manhattan U.S. Attorney Announces Forfeiture], <http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php>.

¹⁰⁵ Partial Judgment by Default, *supra* note 102, at 3.

¹⁰⁶ *Id.* at 4.

¹⁰⁷ As of July 23, 2013, there were 957,079 registered user accounts on Silk Road. *See* Lorenzo Franceschi-Bicchierai, *The Silk Road Online Drug Marketplace by the Numbers*, MASHABLE (Oct. 4, 2013, 12:00 PM), <http://mashable.com/2013/10/04/silk-road-by-the-numbers>.

¹⁰⁸ *See United States v. Cherry*, 330 F.3d 658, 668 n.16 (4th Cir. 2003) ("civil forfeiture proceedings are brought against property, not against the property owner; the owner's culpability is irrelevant in deciding whether property should be forfeited.").

justify forfeiture.¹⁰⁹ This notion is a complex legal fiction designed to provide the means to an end. The forfeiture action essentially obscures its real impetus, preventing the purchase and sale of controlled substances on the Internet,¹¹⁰ by pretending that the Bitcoins themselves were “an essential component” of Ulbricht’s alleged money laundering conspiracy (a charge for which Ulbricht is presumed innocent).¹¹¹

The government’s initial forfeiture complaint artfully refers to the goods and services offered on Silk Road as “overwhelmingly illegal.”¹¹² The most in-depth analysis of the Silk Road ever conducted found that 955 items, or 3.9% of all listings, were categorized as “books.”¹¹³ These items are unlikely to constitute contraband.¹¹⁴ More importantly, the First Amendment protects them.¹¹⁵ Yet, the government did not trouble itself with distinguishing users who had purchased books from users who had purchased heroin.¹¹⁶ The government simply seized all user funds without any further inquiry.¹¹⁷ The Silk Road forfeiture is an excellent example of the power of our existing civil asset forfeiture regime.

The Silk Road forfeiture further demonstrates that the money laundering statute provides an effective means for federal prosecutors to forfeit assets, because it eliminates the need to distinguish between the portion of the property traceable to the underlying offense and the portion derived from other sources.¹¹⁸ In fact, the United States Attorney for the Southern District of New York has joyfully conceded:

¹⁰⁹ See Partial Judgment by Default, *supra* note 102.

¹¹⁰ See Manhattan U.S. Attorney Announces Forfeiture, *supra* note 104.

¹¹¹ Partial Judgment by Default, *supra* note 102, at 3.

¹¹² Sealed Verified Complaint, *supra* note 86, at 6.

¹¹³ See Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, CARNEGIE MELLON UNIVERSITY, <http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf> (last modified Nov. 28, 2012).

¹¹⁴ *Id.*

¹¹⁵ U.S. CONST. amend. I. See also *Martin v. Struthers*, 319 U.S. 141, 143 (1943) (“The right of freedom of speech . . . embraces the right to distribute literature, and necessarily protects the right to receive it.”).

¹¹⁶ See Partial Judgment by Default, *supra* note 102.

¹¹⁷ *Id.*

¹¹⁸ Cassella, *supra* note 10, at 11–12.

CYBER - T A K I N G S

[w]e continue our efforts to take the profit out of crime and signal to those who would turn to the dark web for illicit activity that they have chosen the wrong path. . . . The Silk Road hidden website was designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement.¹¹⁹

The clash between reality and legal fiction is blatant in this statement. In the courtroom, the government forfeited these assets because they were an essential component of a money-laundering scheme.¹²⁰ In its press release, however, the Department of Justice openly congratulates itself for seizing \$28 million from persons engaged in the purchase and sale of controlled substances via the Internet.¹²¹

While the United States government should not be rebuked for its efforts to enforce the Controlled Substances Act, the fact that the government has accomplished its ends by sacrificing the rights of potentially innocent persons is concerning. Given that so many persons were impacted by the Silk Road's forfeiture, at least one innocent person had assets improperly forfeited. In fact, one individual, Peter Ward, a head shop owner from Devon, England, claims exactly that by asserting that his assets were seized even though he used Silk Road for exclusively legal transactions.¹²² Unsurprisingly, Ward would like his profits returned to him, which total approximately \$95,000.¹²³ Ward has even retained an attorney and hopes to delay the government's auction of his property.¹²⁴ If Kyle Goodwin's attempts to reclaim his data from Megaupload's servers are any indication, Ward's legal battle may prove to be the ultimate exercise in futility. Still, he remains optimistic and proclaims that "[i]t will be cool if an old hippy can throw a spanner in the big FBI machine."¹²⁵

¹¹⁹ Manhattan U.S. Attorney Announces Forfeiture, *supra* note 104.

¹²⁰ Partial Judgment by Default, *supra* note 102, at 3.

¹²¹ Manhattan U.S. Attorney Announces Forfeiture, *supra* note 104.

¹²² Andy Greenberg, *Silk Road Vendor Fighting To Reclaim Seized Bitcoins, Argues He Sold Legal Products*, FORBES (Jan. 31, 2014, 9:00 AM), <http://www.forbes.com/sites/andygreenberg/2014/01/31/silk-road-vendor-filing-claim-for-seized-bitcoins-argues-he-sold-only-legal-items>.

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ *Id.*

IV. THE FIFTH AMENDMENT

The Fifth Amendment to the United States Constitution prohibits the taking of private property for public use, without just compensation.¹²⁶ The Takings Clause provides: “[n]or shall private property be taken for public use without just compensation.”¹²⁷ This guarantee “was designed to bar government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole.”¹²⁸ It is useful to note the widespread doctrinal uncertainty surrounding the Takings Clause.¹²⁹ This confusion has led one scholar to comment “[t]hroughout constitutional jurisprudence, only the right of privacy can compete seriously with takings law for the doctrine-in-most-desperate-need-of-a-principle prize.”¹³⁰ Similarly, the Supreme Court has conceded “[t]his Court in the past has recognized the difficulty of reconciling the broad scope of traditional forfeiture doctrine with the requirements of the Fifth Amendment.”¹³¹

Just compensation is required whenever the government’s activities, however legitimate, interfere with the use of private property, such that it is effectively taken from its owner for a public use.¹³² Even though it can be argued that every government action to some degree is intended to benefit the public and that the public derives some benefit from the enforcement of our criminal statutes, one recent case clearly contradicts this argument. In *AmeriSource Corp. v. United States*,¹³³ the government seized over \$150,000 worth of AmeriSource’s pharmaceuticals from a Norfolk Pharmacy (Norfolk) warehouse.¹³⁴ The United States Attorney ordered the seizure pursuant to an investigation into two of Norfolk’s principals, who had been indicted for operating an unregistered drug

¹²⁶ U.S. CONST. amend. V, cl. 4.

¹²⁷ *Id.*

¹²⁸ *Armstrong v. United States*, 364 U.S. 40, 49 (1960).

¹²⁹ See e.g., BRUCE A. ACKERMAN, *PRIVATE PROPERTY AND THE CONSTITUTION* 8 (1977) (“I have not encountered a single lawyer, judge, or scholar who views existing case-law as anything but a chaos of confused argument which ought to be set right if one only knew how”). See also Richard L. Settle, *Regulatory Taking Doctrine in Washington: Now You See It, Now You Don’t*, 12 U. PUGET SOUND L. REV. 339, 339 (“Regulatory taking doctrine is the most perplexing area of American land use law.”).

¹³⁰ Abraham Bell & Gideon Parchomovsky, *Takings Reassessed*, 87 VA. L. REV. 277, 278 (2001).

¹³¹ *United States v. U.S. Coin & Currency*, 401 U.S. 715, 721 (1971).

¹³² See *Kelo v. City of New London*, 545 U.S. 469, 477–83 (2005); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982).

¹³³ *AmeriSource Corp. v. United States*, 525 F.3d 1149 (Fed. Cir. 2008).

¹³⁴ *Id.* at 1150.

CYBER - TAKINGS

facility.¹³⁵ The government never initiated forfeiture proceedings against AmeriSource, nor did they introduce AmeriSource’s drugs into evidence at the criminal trial that led to the convictions of Norfolk’s principals.¹³⁶ Rather, the pharmaceuticals were held in storage and rendered worthless due to the passage of their expiration dates.¹³⁷ The United States Court of Appeals for the Federal Circuit rejected AmeriSource’s contention that the government’s decision to retain the drugs beyond the point of expiration constituted a taking.¹³⁸ Specifically, the court reasoned “[p]roperty seized and retained pursuant to the police power is not taken for a ‘public use’ in the context of the Takings Clause.”¹³⁹

This reasoning is questionable in light of well-established Supreme Court precedent that broadly defines public use.¹⁴⁰ The court’s attempt to draw a bright line between police power and public use is similarly dubious.¹⁴¹ The Supreme Court has “long ago rejected any literal requirement that . . . property be put into use for the general public.”¹⁴² The Federal Circuit’s contention that the valid exercise of a state’s police power is not a “public use” also ignores the fact that regulatory takings have, on occasion, gone so far as to require just compensation.¹⁴³ Accordingly, *AmeriSource Corp.* should not be read to preclude the possibility that an overbroad cyber seizure may implicate the takings clause.

V. POLICY AND CONCLUSION

Treating digital asset forfeitures as Fifth Amendment takings would incentivize the government to act with a scalpel rather than a sword. Such an approach would ensure that seizures in cyberspace are conducted narrowly rather

¹³⁵ *Id.*

¹³⁶ *Id.* at 1151.

¹³⁷ *Id.*

¹³⁸ *AmeriSource*, 525 F.3d at 1153.

¹³⁹ *Id.*

¹⁴⁰ See *Berman v. Parker*, 348 U.S. 26, 32 (1954) (“Public safety, public health, morality, peace and quiet, law and order—these are some of the more conspicuous examples of the traditional application of the police power[.]. Yet they merely illustrate the scope of the power and do not delimit it.”).

¹⁴¹ See *Hawaii Hous. Auth. v. Midkiff*, 467 U.S. 229, 240–41 (1984) (holding that public use is “coterminous with the scope of a sovereign’s police powers”).

¹⁴² *Kelo v. City of New London*, 545 U.S. at 481–82 (quoting 467 U.S. at 235, 241–42, 244).

¹⁴³ See, e.g., *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393, 415 (1922) (“The general rule at least is that while property may be regulated to a certain extent, if regulation goes too far it will be recognized as a taking.”).

than carelessly. Broad seizures would only be executed when they could survive a cost-benefit analysis. While some critics may argue that this approach would unduly impede law enforcement, the logic of the law enforcement impediment argument rings hollow. As certain costs and benefits will always accompany criminal investigations, the question should not be what costs are associated with the criminal investigation, but whether those costs should be borne by a select number of innocent individuals or by the public as a whole. The current system is unfair to property owners and promotes the use of investigative tactics whose costs to the innocent far outweigh their benefits to the public. Just as the government must pay for land on which it builds courthouses and prisons,¹⁴⁴ it too should be required to pay for the property it destroys while investigating and prosecuting crime.

Once warned of the abuse that would follow from forfeiture schemes that bestowed upon the government virtually unlimited authority to seize private property, the Supreme Court stated that “[w]hen such application shall be made it will be time enough to pronounce upon it.”¹⁴⁵ Surely that time has arrived when the government may deprive 60 million users of access to their own property or seize \$28 million from persons whom it has not even identified.¹⁴⁶ These two cases illustrate the problematic nature of employing existing law enforcement tools in cyberspace. The problems that have plagued civil asset forfeiture since its inception have only become more evident as the government attempts to blur the line between physical and intangible property.

The rhetoric and policies of the 1970s were, and still remain, utterly counterproductive. Not only did these policies fail to accomplish their stated objectives, but also in the process ignited our tendency to pursue only penal solutions to social problems. Moderate reforms over the last decade have brought an end to a few of the imprudent policies.¹⁴⁷ By any objective measure, these

¹⁴⁴ See *Kelo v. City of New London*, 545 U.S. 469, 477–83 (2005).

¹⁴⁵ *Goldsmith v. United States*, 254 U.S. 505, 512 (1921).

¹⁴⁶ Partial Judgment by Default, *supra* note 102, at 3.

¹⁴⁷ See, e.g., *President Obama Signs Bill Reducing Cocaine Sentencing Disparity*, ACLU, <https://www.aclu.org/drug-law-reform/president-obama-signs-bill-reducing-cocaine-sentencing-disparity> (last modified Aug. 3, 2010); Charlie Savage, *Justice Dept. Seeks to Curtail Stiff Drug Sentences*, N.Y. TIMES, Aug. 12, 2013, http://www.nytimes.com/2013/08/12/us/justice-dept-seeks-to-curtail-stiff-drug-sentences.html?hp&_r=4&; Gary Fields, *White House Czar Calls for End to ‘War on Drugs’*, WSJ, May 14, 2009, <http://online.wsj.com/news/articles/SB124225891527617397?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB124225891527617397.html> (last updated May 14, 2009, 12:01 AM) (discussing several of the laws previously enacted during our nation’s 40-year war on street-level crime).

C Y B E R - T A K I N G S

policies have been a failure.¹⁴⁸ Fittingly, many elected officials, and countless ordinary Americans, have called for an end to the drug war.¹⁴⁹ The armistice, however, will come far too late because many of the most precarious law enforcement tools—born of the 1970s war-on-crime mentality—has already spread like a cancer.

Even though civil asset forfeitures are now deeply rooted in our national strategy to combat cybercrime,¹⁵⁰ the courts should limit the threat of twenty-first century criminal investigations by preventing complete disregard for the property rights of blameless Internet users in digital asset forfeitures. The solution is not novel—it was written into our nation’s most fundamental declaration of individual rights by James Madison 225 years ago. In pursuit of the well-established ideal that certain burdens should, “in all fairness and justice,” be borne by the public as a whole, courts should classify digital asset forfeitures as Fifth Amendment takings.¹⁵¹

¹⁴⁸ Jacob Sullum, *The Wasteful War On Drugs Is Doomed By Economics 101*, FORBES, <http://www.forbes.com/sites/jacobsullum/2013/10/04/the-wasteful-war-on-drugs-is-doomed-by-economics-101> (Oct. 4, 2013, 8:00 AM).

¹⁴⁹ *But see* GEORGE SANTAYANA, *SOLILOQUIES IN ENGLAND AND LATER SOLILOQUIES* 102 (1922) (“Only the dead have seen the end of war.”).

¹⁵⁰ *See* Exec. Office of the President, *Strategy To Combat Transnational Organized Crime: Addressing Converging Threats to National Security* 20 (July 19, 2011), available at <http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf>.

¹⁵¹ *See* *Armstrong v. United States*, 364 U.S. 40, 49 (1960).