# PROTECTING THE INNOCENT—THE NEED TO ADAPT FEDERAL ASSET FORFEITURE LAWS TO PROTECT THE INTERESTS OF THIRD PARTIES IN DIGITAL ASSET SEIZURES·



## INTRODUCTION

Imagine waking up one morning to discover that all of your digital data has been seized by the federal government. Before digital assets existed, seizing someone's property involved physically going and

taking it away from them. However, now that many people have digital assets, seizing all of someone's data may be as simple as seizing the domain name of the storage site that hosts it. Worryingly, in an effort to take assets away from domain name owners, the government has seized entire domain names without considering the impact the seizure might have on the potentially large number of users dependent on that domain name for access to their digital property.[1] In essence, the rise of digital assets has changed the fundamental rules of the game for asset forfeiture, and new third-party protections are necessary to prevent innocent third parties from becoming regular collateral damage in digital asset seizures.

Federal asset forfeiture law was created to deal with the seizure and forfeiture of physical[2] assets, and the third-party protections written into those laws were based on that assumption.[3] Traditional forfeiture proceedings typically involve assets such as cars,[4] money,[5] and stocks,[6] which tend to have a limited range of impact in terms of the total number of innocent third parties affected. However, unlike physical asset seizures, digital asset seizures carry a high risk of having a negative impact on a wide range of innocent third parties.[7] For example, when a car is seized, the impact is limited to the car's owner and to any third parties dependent on that car for transport. On the contrary, when a domain name is seized, it affects all innocent third parties who use that website. While the seized domain name could be a low-traffic website, it could also be a high-traffic cyberlocker like Megaupload, with millions of users dependent on it data access and storage.[8] That potential to negatively affect millions of innocent third parties simply did not exist until the rise of digital asset seizures. Thus, tailored third-party protections are necessary to address the unique challenges presented by digital asset forfeitures.

Asset forfeiture is a key tool for federal law enforcement. By using seizure and forfeiture, law enforcement can remove the assets either

1 *See infra* Part II.B (www.megaupload.com was seized on a court order, effectively blocking all access to the data on Megaupload's servers; after over a year, innocent owners have yet to see the return of their data). For further examples of domain name seizures, see also *infra* Part II.A.

2 Throughout, "physical" will be used in the sense of "non-digital."

3 *See infra* Part I.A (criminal and civil asset forfeiture laws were created in the 1970s, when digital assets did not exist).

4 *See, e.g.*, United States v. One 1967 Ford Galaxie Serial No. 7E55C256256, 49 F.R.D. 295 (S.D.N.Y. 1970).

5 *See, e.g.*, United States v. $80,180.00 in U.S. Currency, 303 F.3d 1182 (9th Cir. 2002) (civil forfeiture); United States v. Reckmeyer, 628 F. Supp. 616 (E.D. Va. 1986) (criminal forfeiture).

6 United States v. Hill, 46 F. App'x 838 (6th Cir. 2002).

7 *See infra* Part II.

8 *See, e.g.*, *infra* Part II.B (describing how the seizure of cyberlocker www.megaupload.com impacted millions of users who still do not have access to the data they stored on Megaupload's servers).

connected to or gained from the crime in question.[9] There are two major categories of forfeiture laws applicable in criminal investigations—civil forfeiture and criminal forfeiture.[10] In general, the two types of forfeiture differ mainly in when and how they are applied, but not in what function they serve. Criminal forfeiture is imposed as a part of the sentence for a convicted criminal, proceeds against the defendant,[11] and can only reach property belonging to the defendant.[12] Civil forfeiture is imposed against the property itself in a separate civil proceeding that runs parallel to the criminal proceeding and its reach is not necessarily limited to property belonging solely to the defendant; unlike criminal forfeiture, there need not be a criminal conviction giving rise to the forfeiture.[13] Since asset forfeiture can reach assets both directly and indirectly involved in a crime, and crimes do not occur in a vacuum, innocent third parties will likely be affected by seizures and forfeitures, making third-party protections imperative.[14] Affected innocent third parties can include property owners, bona fide purchasers, joint tenants, and many others.[15]

Although physical asset seizures and forfeitures did frequently have a detrimental impact on third parties,[16] now that digital assets can be seized and forfeited, the number of potentially affected third parties increases exponentially.[17] This exponential increase occurs because digital asset seizures do not have the same limitations that are imposed on physical asset seizures, as they do not require the government to have large, physical storage areas in which to keep the forfeited assets.[18] Furthermore, it is theoretically less difficult to block access to an online server or domain name[19] than it is to organize a team to seize physical property. For instance, when a cloud server is seized, the government can take petabytes[20] of data all in one simple domain name seizure

9 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.

10 Michael Goldsmith & Mark Jay Linderman, *Asset Forfeiture and Third Party Rights: The Need for Further Law Reform*, 1989 DUKE L.J. 1254, 1260 (1989).

11 *Id.*

12 Cassella *supra* note 9, at 20.

13 *Id.* at 17.

14 Michael Goldsmith & Mark Jay Linderman, *Asset Forfeiture and Third Party Rights: The Need for Further Law Reform*, 1989 DUKE L.J. 1254, 1256–57 (1989).

15 *Id.*

16 *See infra* Part I.

17 *See infra* Part II.A; *see infra* Part II.B.

18 *See, e.g.*, Indictment, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012) (under seal), *available at* http://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf.

19 *See, e.g.*, MEGAUPLOAD.COM, http://www.megaupload.com (last visited Jan. 2, 2013) (access to website and associated data blocked by FBI splash page).

20 One petabyte is a unit equal to one million gigabytes. *Carpathia Seeks Help With Megaupload*

without having to worry about physical storage space.[21] In an equivalent physical data seizure, the government might need a huge supply of warehouses and workers to handle the sheer volume of physical property involved. Thus, the ease of mass seizure in digital assets could be a siren song to government officials, leading them to seize first and ask questions later, rather than taking the time to carefully determine which digital assets were actually involved in or connected with the crime. In short, because (1) digital asset seizures are generally easier procedures than physical asset seizures, and (2) they have the potential to adversely affect millions of innocent third parties as collateral damage, asset forfeiture law must be reformed to address this problem.

This Note explores how federal asset forfeiture law must be reformed to protect innocent third parties from digital asset seizures and proposes new remedies. Part I explores how third-party protections in asset forfeiture have developed since criminal and civil asset forfeiture were first codified in the 1970s, up to the Civil Asset Forfeiture Reform Act of 2000. Part II looks at digital asset seizures and how they highlight the need to change the current system, focusing on the Operation In Our Sites domain name seizures and the *Megaupload* litigation.[22] Finally, Part III proposes new remedies that could be implemented in digital asset forfeiture cases to address these problems.

## I. HISTORY AND DEVELOPMENT OF THIRD-PARTY PROTECTIONS IN CIVIL AND CRIMINAL ASSET FORFEITURE

The United States, unlike many other countries, does not have a generic forfeiture law allowing for forfeiture of any and all property gained from or involved in, directly or indirectly, any crime.[23] Forfeiture laws were developed over time as parts of various criminal statutes, resulting in a patchwork of statutes where some allowed forfeiture in some form as a part of the general operation of the criminal statute and others did not.[24] The first two federal statutes clearly codifying forfeiture as an independent legal tool were passed in the 1970s as a part of Congress's push to use forfeiture as a criminal deterrent[25]: (1) the Racketeer Influence and Corrupt Organization Act of 1970 ("RICO"), which allowed for criminal forfeiture of assets

*Data*, BBC NEWS (Mar. 23, 2012, 06:09 A.M.), http://www.bbc.co.uk/news/technology-17486841.

[21] *See, e.g.*, David Kravets, *Megaupload User Demands Return of Seized Content*, WIRED (Mar. 30, 2012), http://www.wired.com/threatlevel/2012/03/megaupload-seized-content/.

[22] United States v. Dotcom (*Megaupload*), 2012 WL 4788433 (E.D. Va. Oct. 5, 2012).

[23] Cassella, *supra* note 9, at 9.

[24] *Id.*

[25] Heather J. Garretson, *Federal Criminal Forfeiture: A Royal Pain in the Assets*, 18 S. CAL. REV. L. & SOC. JUST. 45, 46 (2008).

associated with racketeering and organized crime; and (2) the Comprehensive Drug Abuse Prevention and Control Act of 1970, which allowed for civil forfeiture of assets related to violations of the drug laws.[26] Both federal statutes have been used extensively since their inception and greatly increased the number of situations in which law enforcement could use seizure and forfeiture.[27] This Part will consider both civil and criminal asset forfeiture, assess how each has tried to protect innocent third parties, and discuss what deficiencies still exist in those protections.

### A. *Criminal Forfeiture*

The fundamental purpose of criminal asset forfeiture is to punish a convicted criminal defendant and thus it is a proceeding *in personam* against that defendant.[28] The criminal forfeiture takes place as part of the sentencing phase of a criminal trial.[29] At that point, the court can order the defendant to pay a money judgment or to provide substitute assets if the actual money or property derived from the criminal enterprise are no longer available.[30] In short, the key feature of criminal forfeitures is that they can only affect property in which the criminal has some form of ownership interest.[31] When assets are initially seized as part of a criminal forfeiture,[32] there is no statutorily defined time frame in which the government must begin the forfeiture proceedings.[33] This has a potentially devastating effect on third parties whose property can be held indefinitely until the criminal trial is concluded and the forfeiture proceedings completed during the sentencing phase.

Although criminal forfeiture can only reach property in which the defendant has some sort of ownership interest, it is not limited to property directly involved in the criminal activity because the decision on what property is forfeited is based on the property's connection to the defendant and not to the crime.[34] Even if a third party also has an ownership interest in a property that was not directly involved in a

---

26 Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, 84 Stat. 1236 (1970); Garretson, *supra* note 25, at 46; Michael Schecter, *Fear and Loathing and the Forfeiture Laws*, 75 CORNELL L. REV. 1151, 1155 (1990).

27 Nicholas Loyal, *Bills to Pay and Mouths to Feed: Forfeiture and Due Process Concerns After* Alvarez v. Smith*,* 55 ST. LOUIS U. L.J. 1143, 1145–46 (2011).

28 Garretson, *supra* note 25, at 45–46.

29 Cassella, *supra* note 9, at 19.

30 *Id.* at 19–20.

31 Amanda Seals Bersinger, *Grossly Disproportional to Whose Offense? Why the (Mis)application of Constitutional Jurisprudence on Proceeds Forfeiture Matters,* 45 GA. L. REV. 841, 851-52 (2011).

32 This is usually the case when property is seized with a criminal seizure warrant. *See* Cassella, *supra* note 9, at 20.

33 *See* 21 U.S.C. § 853(f); *see also* Cassella, *supra* note 9, at 20.

34 Bersinger, *supra* note 31.

crime, that property may still be subject to forfeiture as a part of the defendant's sentence. Some courts have addressed this issue by means of "partial forfeiture," where only the criminal's interest in the property is forfeit, and the innocent co-owner's is not.[35] However, since there is no universal statutory provision applying this concept to all criminal forfeitures, this only provides limited protection to third parties.

The main third-party protection from criminal forfeiture is the limited nature of the tool itself.[36] Since third parties cannot participate in the criminal trial, law enforcement and the courts must carefully avoid forfeiting property that belongs solely to third parties in order to prevent any violation of the third party's due process rights.[37] Thus, in order to ensure that forfeited property belongs at least partially to the defendant, the court will hold an ancillary proceeding after the criminal trial to make this ownership determination.[38] However, an ancillary proceeding occurs only if a third party comes forward to contest the forfeiture proceeding and claims ownership of the forfeited property.[39] This means that the government is not required to make sure that forfeited property even partly belongs to the defendant unless a third party comes forward to contest the seizure and forfeiture of their property. Although this is a form of third-party protection, it is too weak to effectively protect the interests of innocent third parties who are burdened with contesting the government's seizure, especially since they are only allowed to contest the seizure in strictly proscribed proceedings.

Even though the limited scope of criminal forfeiture inherently protects third parties, it is not enough, because third parties can only contest the forfeiture by filing claims in an ancillary proceeding after the defendant has been tried and convicted.[40] Due to the lengthy nature of many criminal trials, this is an unacceptable burden on third parties. Although the indictment must contain notice of the government's intent to forfeit defendant's property,[41] if notice is proper and "the court finds that property is subject to forfeiture," then the court must enter a preliminary order of forfeiture "without regard to any third party's interest in [all or part of] it."[42] This places a third party's property

35 Avital Blanchard, *The Next Step in Interpreting Criminal Forfeiture*, 28 CARDOZO L. REV. 1415, 1416 (2006) (discussing the partial forfeiture allowed to protect third-party interests in *United States v. 1500 Lincoln Ave.*, 949 F.2d 73 (3d Cir. 1991), and *Pacheco v. Serendensky*, 393 F.3d 348 (2d Cir. 2004)).

36 Cassella, *supra* note 9, at 14.

37 *Id.*

38 *Id.*

39 *Id.* at 15.

40 *Id.*

41 FED. R. CRIM. P. 32.2(a) (requiring that the government declare an intent to forfeit Defendant's property, but need not state what property is specifically subject to forfeiture).

42 FED. R. CRIM. P. 32.2(b)(2)(A).

interest in harm's way from the absolute beginning of a criminal trial, while offering no chance to protect it until after the trial is complete. The court need only determine whether the property subject to forfeiture has the requisite degree of "nexus" to the offense required by the statute the defendant is prosecuted under;[43] the court need not inquire into a third party's interest in the property until and unless they file a claim in an ancillary proceeding.[44]

Unlike civil forfeiture law, which was reformed significantly in 2000,[45] criminal forfeiture law has not seen substantial reform since 1984.[46] Now, further reform is needed to address modern concerns, especially in relation to digital asset seizures, which were not even possible in the 1970s when federal criminal forfeiture statutes were first enacted, or in the 1980s, when they were first reformed.[47] Since digital assets did not exist at the time criminal asset forfeiture statutes were created, legislators could not have contemplated the implications of the existing seizure and forfeiture proceedings as applied to the digital sphere, nor could they have contemplated what third-party protections would be necessary when dealing with digital asset seizures. As with all asset forfeiture laws, third-party protections are necessary to shield innocent owners and prevent them from becoming collateral damage in the government's drive to punish a convicted criminal.

### B. *Civil Forfeiture*

In order to obtain a court order allowing law enforcement to carry out an initial seizure, the government need only show probable cause that the property was involved, directly or indirectly, in a criminal act.[48] After property is seized, the property owner has the opportunity to file a claim contesting the seizure; if the owner does not contest, the property defaults to the government.[49] If the seizure is contested, the government must either file a civil forfeiture action against the property[50] or return it to the owner.[51] If the government is also criminally prosecuting the property owner, then the government may file a criminal forfeiture

43 FED. R. CRIM. P. 32.2(b)(2)(A).
44 FED. R. CRIM. P. 32.2(c).
45 *See infra* Part I.B.1.
46 In *Pacheco v. Serendesky*, the Second Circuit interpreted RICO as allowing for partial forfeiture, which only forfeits the criminal defendant's interest in cases where the defendant co-owns property with an innocent third party. *Pacheco*, 393 F.3d at 355; *see also* Blanchard, *supra* note 35, at 1425–26.
47 *See* Blanchard, *supra* note 35, at 1425–26.
48 David Benjamin Ross, *Civil Forfeiture: A Fiction that Offends Due Process*, 13 REGENT U. L. REV. 259, 265 (2000).
49 *Id*. at 265; 18 U.S.C. 983(a)(2)(A) (2012).
50 Cassella *supra* note 9 at 13.
51 18 U.S.C. 983(a)(3)(A)–(B).

action instead of, or in addition to, the civil forfeiture.[52]

### 1. Civil Asset Forfeiture Prior to the Civil Asset Forfeiture Reform Act of 2000

Civil forfeiture is an action *in rem* (against the property itself), so the government does not have to prove that the property owner committed an offense that would independently justify the forfeiture.[53] Rather, to forfeit property the government simply has to prove, by a preponderance of evidence, that the property was either used to commit a crime or that it was acquired as a result of a criminal act.[54] The basis for this type of seizure is the idea that the property is "tainted" as soon as it comes in contact with an illegal substance or activity,[55] and under the doctrine of relation back, title to the tainted, forfeitable property vests in the government upon commission of the offense.[56] In other words, from the first moment property is involved in a crime, the government is entitled to seize it at any point thereafter. This schema is commonly used in cases where cars have been used to transport illegal substances, allowing the government to declare the vehicles open to forfeiture retroactive to the moment they were used as transport.[57]

Civil forfeiture proceedings are not part of a criminal case nor are they part of sentencing.[58] Since the proceedings are not dependent on a criminal conviction, they can occur before an indictment, after an indictment, or even in the complete absence of an indictment.[59] This fluid nature, in addition to the lower burden of proof for civil forfeiture than for criminal conviction,[60] is mainly why civil forfeiture often negatively impacts innocent third parties. Furthermore, since civil asset forfeiture proceeds against the property itself, and it is the property's involvement that must be proven; whether or not the property's owner is guilty of the crime in question is irrelevant.[61] Because of the high risk of

52 18 U.S.C. 983(a)(3)(C). See *supra* Part I.A for a discussion of criminal forfeiture.

53 Tamara R. Piety, *Scorched Earth: How the Expansion of Civil Forfeiture Doctrine Has Laid Waste to Due Process*, 45 U. MIAMI L. REV. 911, 916 (1991).

54 Cassella *supra* note 9, at 15.

55 Piety, *supra* note 53, at 916–17.

56 *Id.* at 917; *see also* 21 U.S.C. 881(h) (2006).

57 *See, e.g.*, United States v. One 1967 Ford Galaxie Serial No. 7E55C256256, 49 F.R.D. 195 (S.D.N.Y. 1970) (involving the civil forfeiture of a car belonging to the wife of an alleged stamp forger, which was seized on suspicion of having been used to transport forged stamps).

58 Cassella, *supra* note 9, at 15.

59 *Id.*

60 Initially, civil forfeiture only required that the government demonstrate probable cause; the Civil Asset Forfeiture Reform Act ("CAFRA") then increased the burden to a preponderance of the evidence. This is still less than the beyond a reasonable doubt standard required by criminal cases. Ross, *supra* note 48, at 273–74.

61 Ross, *supra* note 48, at 263; Roger Pilon, *Statement Before the Criminal Justice Subcommittee of the United States Senate Judiciary Committee*, CATO INSTITUTE, July 21, 1999, *available at*

erroneous deprivation posed by civil forfeiture, a number of protections have been put in place over the years to try to minimize the potential for harm to innocent third parties.

Civil asset forfeiture is a procedure included in a variety of criminal statutes, each of which provides what can be forfeited and under what circumstances civil forfeiture is appropriate.[62] The most common protection among the various permutations of civil forfeiture is the innocent owner defense,[63] which allows the property owner to challenge the forfeitability of the property by showing—by a preponderance of the evidence—that they have an ownership interest in the property and that they are innocent in relation to the criminal activity that prompted the civil forfeiture.[64] However, until the Civil Asset Forfeiture Act of 2000 ("CAFRA") created a universal innocent owner defense,[65] the innocent owner defense was a narrow exception strongly dependent on whether it was provided for in the statute used to initiate the civil asset forfeiture.[66] Without the protection of a statutory innocent owner defense, civil forfeiture proceeds against the property, and the burden shifts to innocent property owners to show that their property was not involved in the crime without any consideration given to the property owner's guilt or innocence.[67] In other words, rather than strictly limiting the court's allowed scope of consideration only to determining the property's involvement in the crime, the innocent owner defense allows the court to consider the property owner's innocence in ruling on whether the forfeiture is appropriate.[68]

Although the innocent owner defense offers significant protection, it can be both difficult and expensive for an innocent property owner to fulfill the requirements of the defense, especially if the seizure involved their monetary assets.[69] Prior to CAFRA, property owners had to file a cost bond of the lesser of five thousand dollars or ten percent of the property value[70] and bring the challenge within ten days of the initial

http://www.cato.org/publications/congressional-testimony/oversight-federal-asset-forfeiture-its-role-fighting-crime.

62 *See* Cassella, *supra* note 9.

63 *Id*. at 16; *see* 18 U.S.C. § 983(d).

64 Once the government has shown probable cause to hold the property subject to forfeiture, the burden of proof then shifts to the innocent owner. Cassella *supra* note 9 at 16; Ross, *supra* note 48, at 263.

65 Cassella, *supra* note 9, at 16.

66 Bennis v. Michigan, 516 U.S. 442 (1996) (the Supreme Court held that, in the absence of legislation providing for an innocent owner defense, the Constitution did not alone confer one upon innocent owners, nor does forfeiture of property without an available innocent owner defense constitute a violation of due process).

67 Ross, *supra* note 48, at 265.

68 *Id.* at 270; Piety, *supra* note 53, at 916–17.

69 Ross, *supra* note 48, at 267.

70 *Id.* at 265; 145 CONG. REC. H4851-01, 1999 WL 419754 (June 1999).

seizure, preventing many innocent owners, especially those who were indigent or poor, from challenging the forfeiture of their property.[71] If the innocent owner did not comply with these requirements, their property was forfeited in a default judgment.[72] One can reasonably assume that these requirements were at least a significant part of the reason only twenty percent of forfeitures prior to CAFRA were challenged.[73]

### 2. The Civil Asset Forfeiture Reform Act of 2000

The Civil Asset Forfeiture Reform Act was passed by the House of Representatives in June 1999,[74] and was enacted April 25, 2000.[75] CAFRA's purpose is to "provide a more just and uniform procedure for Federal civil forfeitures" and made significant strides toward increasing third-party protections.[76]

After CAFRA passed, the government could no longer seize property on the basis of probable cause; the government now must prove by a preponderance of the evidence that the property in question was subject to civil forfeiture before the initial seizure can proceed.[77] CAFRA further required that, if the government based their forfeiture claim on the property's alleged involvement in the commission or facilitation of a crime, then it had to prove a substantial connection between the property and the crime by a preponderance of the evidence.[78] This increased burden on the government was designed to give innocent third parties an additional layer of protection, to limit the impact of the *in rem* nature of civil forfeiture proceedings, and to prevent erroneous forfeiture.[79] In short, because civil asset forfeiture proceedings prior to CAFRA had only targeted the property without regard for the owner's guilt, CAFRA sought to increase the burden of proof the government had to meet in order to deprive owners of their property.[80] Increasing the burden of proof for seizures from probable cause to preponderance of the evidence requires the government to acquire more evidence before they are able to seize property for

71 Ross, *supra* note 48, at 274–75.
72 *Id.* at 265.
73 *Id.*
74 H.R. 1658, 106th Cong. (1999).
75 Civil Asset Forfeiture Reform Act of 2000, 18 U.S.C. § 983 (2012).
76 *Id.*
77 18 U.S.C. § 983(c). Property is first seized and then subjected to forfeiture.
78 *Id.*
79 Ross, *supra* note 48, at 273–74; *see also* H.R. REP. NO. 106–192 (1999), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-106hrpt192/html/CRPT-106hrpt192.htm (only requiring the government to show that probable cause in a civil forfeiture does not "reflect the value of private property in our society, and makes the risk of an erroneous deprivation intolerable.").
80 Ross, *supra* note 48, at 273–74.

forfeiture.[81] This increased burden decreased the ease with which the government could seize property and required more effort on the government's part to provide evidence of the property's guilt before depriving an owner of their property. Thus, CAFRA increases the protections on third parties by restricting the government's latitude in what and when something is subject to seizure for civil forfeiture.

In addition to increasing the government's evidentiary burden, CAFRA also contained provisions that sought to ease the burdens placed on third parties by the prior statutory civil forfeiture procedures. First, CAFRA authorized the appointment of counsel for any person financially unable to pay for representation but who had standing to contest the forfeiture and did so in good faith.[82] This increased the scope of third-party protections to cover all those affected by asset seizure, not just those who could afford to pay for a lawyer. Second, CAFRA extended the time frame during which a third party may raise a challenge to the forfeiture—from ten to thirty days[83]—and eliminated the previously required cost bond.[84] CAFRA also allowed for the return of property during pending civil forfeiture proceedings if the owner could show hardship.[85] Although the aforementioned measures significantly increased third-party protections, the most important aspect of CAFRA for third parties was that it made the innocent owner defense universally available to all third parties contesting civil forfeiture of their property.[86] This addition was a vast improvement from the prior situation in which the innocent owner defense was available under some statutes and not under others, where the determining factor of whether or not the defense would be available turned on the jurisdiction a person was in.[87]

However, while CAFRA represents a major improvement over earlier statutes, it still sets a high standard for innocent owners to meet. In order to prevail, innocent owners must show (1) that they did not know about the criminal conduct that prompted the forfeiture, and (2) that they did all that could reasonably be expected under the circumstances to terminate the criminal use of their property.[88] Both elements are hard to prove, especially since the statute provides little

[81] *Id.*; 18 U.S.C. § 983(c)(1).
[82] 18 U.S.C. § 983(b)(1).
[83] The thirty-day limit to file a challenge is the default; the government may set a longer time frame by sending a personal notice letter to the property owner, in which case the time frame must be, at a minimum, thirty-five days after the notice letter is mailed. 18 U.S.C. § 983(a)(2)(B); *see also* Ross, *supra* note 48, at 275.
[84] *Supra* note 70 and accompanying text.
[85] Ross, *supra* note 48, at 275; 18 U.S.C. § 983(f)(1)(C).
[86] 18 U.S.C. § 983(d)(1).
[87] *See supra* notes 65–66 and accompanying text.
[88] 18 U.S.C. § 983(d)(2).

guidance on how a judge is to determine whether someone knew about criminal conduct, or whether they undertook all reasonable action to terminate said use of the property.[89] Proving lack of knowledge and reasoning attempts at termination may prove especially troublesome in cases where the assets seized are not physical and the owner has less concrete control over, and less knowledge about, where his property is and how it is being used.

Although CAFRA made significant strides toward protecting third parties, providing opportunities to challenge civil seizures and forfeitures, and limiting the government's latitude to conduct seizures, further reform is still required. There is an especially urgent need to adapt CAFRA, or supplement it, in order to properly protect innocent third parties caught up in digital assets seizures.

## II. DIGITAL ASSET SEIZURES AND HOW THEY HIGHLIGHT THE NEED FOR CHANGE IN ASSET FORFEITURE LAW

The rise of digital asset seizures has changed the game for asset forfeiture. When assets are digital, the government can seize potentially limitless assets without having to worry about where it will store them. Furthermore, when the government can seize a digital asset by simply blocking access to it,[90] there is no need to track down the precise location of the assets and physically seize them. These changes significantly increase the ease with which the government can seize property, and could prompt law enforcement to implement forfeitures more regularly and with less care. Moreover, as a result of these factors, cases involving digital asset seizure represent a unique risk: the government could have an incentive to seize as much data as possible rather than taking the time to sort out what data actually belongs to the criminals.[91] Because of this risk, it is imperative that asset forfeiture protections evolve to fully protect third parties in digital asset seizures and forfeitures.

### A. *The First Wave of True Digital Asset Seizures—The Domain Name Seizures*

In 2010, Operation In Our Sites,[92] a joint program run by the Department of Justice ("DOJ") and the Department of Homeland Security's Immigrations and Customs Enforcement ("ICE"), started the

89 *Id.*

90 *See, e.g.*, MEGAUPLOAD.COM, *supra* note 19 (access blocked by FBI splash page).

91 *See, e.g.*, United States v. Dotcom, 2012 WL 4788433 (E.D. Va. Oct. 5, 2012).

92 This spelling "s-i-t-e-s" is a deliberate play on words. 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.

first wave of purely digital asset seizures when it began systematically cracking down on websites that allegedly dealt in copyright-infringing content.[93] Under Operation In Our Sites, federal law enforcement investigates potentially infringing websites and gathers the necessary evidence to obtain seizure warrants for websites' domain name from a federal judge.[94] The websites' domain names are then seized and so that when users try to access the sites, they are re-directed to a federal seizure notice, instead of accessing allegedly copyright or trademark infringing content.[95] ICE has jurisdiction for these seizures through its partnership with the DOJ.[96]

In the summer of 2010, the first wave of Operation In Our Sites seizures took down nine websites accused of selling pirated movies; in November 2010, the second wave targeted eighty-two websites allegedly involved in selling a range of counterfeit goods.[97] Since then, the government has continued to use Operation In Our Sites to seize domain names suspected, however thinly, of copyright or trademark infringement.[98] Since the websites were not physical stores, the seizure orders targeted the domain names in an attempt to disrupt the sale of counterfeit goods and cutoff the flow of cash to these operations.[99]

Operation In Our Sites only seizes domain names, not the associated content on the servers.[100] When someone attempts to navigate to a seized domain name, a splash page appears listing the alleged crimes for which the domain name was seized.[101] However, because only the domain name is seized, and not the server or the content thereon, if a domain name owner wishes to keep operating after the seizure, all the owner has to do to get the project up and running again is to obtain a new domain name for their content.[102] This makes

93 Anderson, *supra* note 92; Matthew Lasar, *Feds Seize 82 Domains Accused of Selling Counterfeit Goods*, ARS TECHNICA (Nov. 29, 2010, 1:58 PM), http://arstechnica.com/business/2010/11/feds-seize-82-domains-selling-counterfeit-goods.

94 NAT'L INTELLECTUAL PROP. RIGHTS COORDINATION CTR., OPERATION IN OUR SITES, http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf (last visited Feb. 28, 2013).

95 *Id.*

96 *Id.*

97 Lasar, *supra* note 93.

98 *See, e.g.*, Mark Masnick*, Congress Begins to Wonder Why ICE & DOJ Censored Popular Hip Hop Blog for a Year,* TECHDIRT (May 9, 2012, 8:32 AM) http://www.techdirt.com/articles/20120508/02352318822/congress-begins-to-wonder-why-ice-doj-censored-popular-hip-hop-blog-year.shtml (mentioning ICE's seizure of 760 websites).

99 Lasar, *supra* note 93.

100 Anderson, *supra* note 92.

101 For examples of DOJ splash pages, see NINJAVIDEO, www.ninjavideo.net (last visited Aug. 22, 2013); David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED (May 3, 2012, 5:00 PM), http://www.wired.com/threatlevel/2012/05/weak-evidence-seizure.

102 Anderson, *supra* note 92.

pure domain name seizures, like those executed under Operation In Our Sites, less of an issue for innocent third parties than seizures of cyberlockers that block access to digital data.[103] For example, when the domain name of torrent site "The Pirate Bay" was faced with potential seizure, it simply switched its domain name from .ORG, which is subject to U.S. seizure,[104] to the Swedish domain .SE, which is not.[105] Even if The Pirate Bay's .ORG domain name had been seized prior to its voluntary move to .SE, The Pirate Bay could have just as easily obtained the new domain name after their old one had been seized. Therefore, although pure domain name seizures of websites hosting infringing content can be circumvented relatively easily, these initial digital asset seizures were merely the prologue to the much larger issue of mass digital data seizures.[106]

Although many of the Operation In Our Sites seizures have affected websites actually trafficking in pirated goods, other seizures have profoundly and negatively affected non-infringing sites. For example, one of the sites seized in the first wave of domain name seizures was "Ninjavideo," a website that allowed users to stream and download high quality pirated movies and television programs.[107] In September 2011, the founder of Ninjavideo pled guilty to criminal copyright infringement and conspiracy.[108] During the course of its operations, Ninjavideo generated $505,000 from advertising proceeds and visitor donations.[109] Ninjavideo encouraged visitors to donate by granting donors access to a private forum that held additional infringing content.[110] Since the goal of Ninjavideo was to provide access to pirated content and to encourage donations in exchange for greater access to said infringing content, shutting it down seems to neatly fit the aims of Operation In Our Sites: to address the growing number of intellectual

103 *See, e.g.*, *infra* Part II.B (The domain name seizure of cyberlocker Megaupload.com also blocked access to users' data because the cyberlocker's domain was the only path through which the data on the associated servers could be accessed.).

104 Any domain that ends in .com, .net, or .org is subject to U.S. seizure because it is U.S. based companies that have the contracts to administer them. David Kravets, *Uncle Sam: If It Ends in .Com, It's .Seizable*, WIRED, Mar. 6, 2012, http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites.

105 *The Pirate Bay Moves to .SE Domain to Prevent Domain Seizure*, TORRENTFREAK (Feb. 1, 2012), http://torrentfreak.com/the-pirate-bay-moves-to-se-domain-prevent-domain-seizure-120201.

106 *See infra* Part II.B.

107 *Founder of Ninjavideo Pleads Guilty to Criminal Copyright Conspiracy*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, Sept. 26, 2011, http://www.ice.gov/news/releases/1109/110926washingtondc.htm.

108 *Id.*

109 *2 Additional Ninjavideo Top Administrators Plead Guilty to Criminal Copyright Conspiracy*, ICE (Oct. 25, 2011), http://www.ice.gov/news/releases/1110/111025washingtondc3.htm.

110 *Founder of Ninjavideo Pleads Guilty to Criminal Copyright Conspiracy,* ICE (Sept. 26, 2011), http://www.ice.gov/news/releases/1109/110926washingtondc.htm.

property crimes and to deter those who seek to unduly profit from the creativity of Americans.[111]

Not all of Operation In Our Sites' seizures have been as clear-cut. The program is controversial because of due process concerns related to the fact that not all the seized domains were guilty of infringement.[112] Questions about the legality of these seizures have focused on the government practice of (1) seizing domains without warning, and often without a criminal case against those behind the sites accompanying the federal seizure order,[113] (2) holding domains for an indefinite period of time, and (3) returning domains without compensation if they are found to be non-infringing.[114]

One clear example of an improper domain name seizure was the case of hip-hop blog Dajaz1.com. Dajaz1 was seized for alleged copyright infringement in spite of the fact that the website's owner was able to provide emails proving that the allegedly infringing songs had been sent to him legitimately by the artists or labels so that he could post them on his website.[115] The government held Dajaz1 for a year without filing a lawsuit against the site or its owner, only to then return it without compensation.[116] This delay is especially concerning given CAFRA's underlying policy that forfeiture should be a quick process with tight timelines for both the government and the person contesting the forfeiture.[117]

In 2011, the seizure of two websites belonging to sports-television "linking site"[118] Rojadirecta—rojadirecta.com and rojadirecta.org—provided yet another example of how digital asset seizures are being

111 *2 Additional*, *supra* note 109.

112 Masnick, *supra* note 98; *see, e.g.*, Timothy B. Lee, *Domain Seizure Oversight Lax and Broken, Targets Out of Luck*, ARS TECHNICA, Dec. 13, 2011, http://arstechnica.com/tech-policy/2011/12/expert-domain-seizure-oversight-too-lax-targets-out-of-luck/ (discussing the improper seizures of RojaDirecta.com and Dajaz1.com).

113 Operation In Our Sites obtains federal seizure warrants before seizing domain names. National Intellectual Property Rights Coordination Center, *Operation in Our Sites*, ICE.GOV, http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf (last visited Feb. 28, 2013).

114 Lee, *supra* note 112; Nate Anderson, *Senator: Domain Name Seizures "Alarmingly Unprecedented,"* ARS TECHNICA (Feb. 3, 2011, 10:04 PM), http://arstechnica.com/tech-policy/2011/02/senator-us-domain-name-seizures-alarmingly-unprecedented/.

115 Timothy Lee, *ICE Admits Year-Long Seizure of Music Blog was a Mistake*, ARS TECHNICA (Dec. 8, 2011, 6:14 PM), http://arstechnica.com/tech-policy/2011/12/ice-admits-months-long-seizure-of-music-blog-was-a-mistake/.

116 Masnick, *supra* note 98; Lee, *supra* note 112.

117 *See* 18 U.S.C. § 983(a) (describing a series of thirty to ninety day deadlines for various aspects of a forfeiture action).

118 A linking site like Rojadirecta is one that provides links to other sites where the content is hosted; it does not itself host content. Nate Anderson, *Government Admits Defeat, Gives Back Seized Rojadirecta Domains*, ARS TECHNICA, Aug. 29, 2012, http://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/.

conducted in an unacceptably lengthy and capricious manner.[119] At first, Rojadirecta simply changed its domain name to Rojadirecta.me and continued to operate.[120] However, when the government sought to forfeit both domains, Rojadirecta challenged the seizure and forfeiture; Rojadirecta's main argument highlights one of the key differences between traditional asset seizures and digital asset seizures: unlike a physical seizure, where only certain self-contained property is seized, when the government seized Rojadirecta's domain names, they effectively seized the entire business as a result of that one digital asset seizure.[121] Although the judge believed that the seizure was not too draconian a measure for crimes that had yet to be proven in court, as Rojadirecta had argued, in August 2012, the government was forced to return the websites to Rojadirecta when it was unable to obtain the evidence necessary to defeat the challenge.[122] Thus, the Rojadirecta case illustrates how traditional asset forfeiture procedure can have a more potent impact when used against digital assets than when used against traditional physical assets.[123]

The Rojadirecta debacle was a similar situation to the one faced by Dajaz1. In both cases, the government was able to easily seize a domain name, hold it for an extended period of time while attempting to gather the evidence necessary for a sustainable claim of infringement, and then return the domain name without compensating the owner. Essentially, these Operation In Our Sites seizures treated the seized websites as "guilty until proven innocent," a dangerous policy to have considering the imbalance of power between the government and the domain name owners.[124] In short, the domain name seizures reveal that the key difference between traditional asset seizures and digital asset seizures is that digital asset seizures have the potential for a far greater of impact on both the property owner and on innocent third parties. Unlike when, for example, an alleged criminal's bank account is seized, which affects only the owner and his dependents, seizing a domain name could have the effect of depriving an owner of his entire business, as with Rojadirecta,[125] or depriving millions of innocent users of access to their data, as with Megaupload.[126] This impact on innocent third-party users is a potentially gross injustice that reveals the need for reforms targeting increased protection of third-party assets.

119 *Id.*
120 *Id.*
121 *Id.*
122 *Id.*
123 *Id.*
124 Anderson, *supra* note 118.
125 *Id.*
126 *See infra* Part II.B.

### B. Megaupload *and Mass Data Seizure*

The Operation In Our Sites was only the prelude to what is perhaps the clearest example highlighting the need for additional third-party protections in digital asset forfeiture—the currently pending *Megaupload* case.[127] The *Megaupload* litigation is a federal criminal copyright infringement case involving Megaupload.com.[128] Megaupload was a "cyberlocker"[129] hosting twenty-five petabytes[130] of data from millions of users[131] around the world.[132] It allowed users to view, share, upload, and download content, either in a limited fashion (for non-paying users) or in an almost unlimited fashion (for paying "premium" users).[133]

On January 5, 2012, in the Eastern District of Virginia,[134] the government sought an indictment against Megaupload, its founder Kim Dotcom, and other high-ranking Megaupload managers on various counts of criminal copyright infringement, racketeering, and money laundering.[135] On February 16, 2012, the government amended the

127 United States v. Dotcom (*Megaupload*), 2012 WL 4788433 (E.D. Va. Oct. 5, 2012); *see generally*, Indictment, *supra* note 18. Please note that this Note will focus only on the U.S. side of this issue, not any international implications.

128 *Id.*

129 A cyberlocker is an online storage service where people can store their files. Indictment, *supra* note 18, at 4. It is comparable to an online version of an external hard drive. Cyberlockers can be used to send large files that are not easily transmittable online by letting the user upload the large file to the cyberlocker and providing a link the user can share with anyone that needs to download that file. Examples of other still operational cyberlockers are Rapidshare, http://www.rapidshare.com, and Dropbox, http://www.dropbox.com.

130 Twenty-five petabytes is equal to twenty-five thousand terabytes, or twenty-five million gigabytes. *Carpathia Seeks Help With Megaupload Data*, *supra* note 20 (one petabyte equals one million gigabytes).

131 Megaupload claims to have had 180 million registered users, but the government contends that there were only 66.6 million users and that only 5.86 million of those users (less than ten percent) used the system to upload files. David Kravets, *Feds Seize $50 Million in Megaupload Assets, Lodge New Charges*, WIRED (Feb. 17, 2012, 5:34 PM), http://www.wired.com/threatlevel/2012/02/megaupload-superseding-indictment/.

132 Brief of Kyle Goodwin in Support of His Motion for the Return of Property Pursuant to 18 U.S.C. § 1963 and/or Federal Rule of Criminal Procedure 41(g) at 1–2, United States v. Dotcom, No. 1:12-cr-00003-LO (E.D. Va. May 25, 2012); Kravets, *Megaupload User Demands Return of Seized Content*, *supra* note 21.

133 Indictment, *supra* note 18, at 2–3.

134 The standing and jurisdiction issues in this case are not the focus of this Note. Megaupload is a Hong Kong company owned by New Zealand resident, Kim Dotcom; but since they rented Virginia-based Carpathia servers to host some of their data, routed money through U.S.-based Paypal for premium account holders, and sent money to U.S. citizens through its "Uploader Rewards" program, Megaupload is subject to criminal charges by the U.S. government. Indictment, *supra* note 18; Nate Anderson, *Explainer: How Can the U.S. Seize a "Hong Kong Site" Like Megaupload?*, ARS TECHNICA (Jan. 20, 2012, 5:05 PM), http://arstechnica.com/tech-policy/2012/01/explainer-how-can-the-us-seize-a-hong-kong-site-like-megaupload/; Indictment, *supra* note 18.

135 The official charges are the following: (1) conspiracy to commit racketeering, (2) conspiracy to commit copyright infringement, (3) conspiracy to commit money laundering, (4) criminal

indictment to include additional charges of criminal copyright infringement by electronic means and wire fraud.[136] The *Megaupload* case is one of the largest criminal copyright infringement cases in United States history.[137] Based on the indictment, the government obtained a court order allowing them to seize Megaupload's domain name, the more than one thousand leased servers housing Megaupload's twenty-five petabytes of user data at Carpathia Hosting,[138] and the defendants' physical property and monetary assets.[139]

In the indictment, the government repeatedly accused Megaupload and its top management of being part of what it dubbed the "Mega Conspiracy," an allegedly massive criminal enterprise focused on criminal copyright infringement as a vehicle for racketeering and money laundering.[140] The government alleges that the Mega Conspiracy caused in excess of $500,000,000 in damage to copyright holders and that it took in over $175,000,000 in profits.[141] The government further claims that Megaupload.com has been used since September 2005 as a vehicle to illegally distribute copyrighted content over the Internet.[142] According to the indictment, Megaupload claims to have had more than 180,000,000 registered users in its lifetime, and it was once estimated to be the thirteenth most frequently visited website on the Internet.[143] Therefore, if the government's allegations turn out to be correct, Megaupload's massive size would have allowed it to grant millions of people access to pirated material.

The government bases its racketeering and money laundering charges on Megaupload's "Uploader Rewards" program, which rewarded users who uploaded content that garnered a lot of hits.[144]

copyright infringement by distributing a copyrighted work being prepared for commercial distribution on a computer network and aiding and abetting of criminal copyright infringement, and (5) criminal copyright infringement by electronic means and aiding and abetting of criminal copyright infringement. Indictment, *supra* note 18, at 1.

136 Superseding Indictment, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Feb. 16, 2012), 2012 WL 602594. Although additional charges were added, the content that was present in the initial complaint was not changed, and it is that initial content on which this Note will focus, relying on the initial complaint for clarity.

137 Kravets, *Feds Seize $50 Million in Megaupload Assets*, *supra* note 131.

138 Brief of Kyle Goodwin, *supra* note 132, at 1–2; Kravets, *Megaupload User Demands Return of Seized Content*, *supra* note 21.

139 Tom Schoenberg, *Megaupload Judge Defers Decision on Seizing Users' Data*, BLOOMBERG (June 29, 2012, 1:57 PM), http://www.bloomberg.com/news/2012-06-29/megaupload-judge-defers-decision-on-seizing-users-data.html; Hayley Tsukayama, *Petition Protests Megaupload Data Seizure*, The WASHINGTON POST, June 29, 2012, http://articles.washingtonpost.com/2012-06-29/business/35460365_1_megaupload-files-valid-legal-process.

140 Indictment, *supra* note 18.

141 *Id.* at 2.

142 *Id.*

143 *Id.*

144 *Id.* at 6.

Megaupload began the rewards program because one of its main sources of revenue was online advertising, and the more hits Megaupload received, the more advertisers it could attract to the site, thus increasing Megaupload's revenue.[145] The easiest way for Megaupload to attract users was by assuring that links to content hosted on Megaupload were distributed as ubiquitously as possible to various third-party linking sites.[146] The government alleges that the Uploader Rewards program provided financial incentive in order to assure that uploaders of popular content would post links to the various third-party linking sites.[147] The key issue underlying the government's allegations about the Uploader Rewards program, however, was that Megaupload's website did not have a search function.[148] Thus, the only ways people could find links to files on Megaupload were if they were sent a link by the initial uploader, or if the user found a link to the content on Megaupload's site by conducting a search on a third-party linking site.[149] Only Megaupload's top management, the so-called Mega Conspiracy members, had access to an index of the actual files stored on their servers.[150]

Megaupload classified itself as a cyberlocker, which allowed private users to store their data on its servers.[151] The length of time a user could store their data on the server depended on whether they were unregistered, registered, or a premium user.[152] Only premium users were capable of using Megaupload for long-term data storage and they paid for the privilege.[153] These users were able to easily use Megaupload as a way to share and transmit large files while also assuring that the files were backed up to the server indefinitely.[154] A significant portion of Megaupload's proceeds was from membership dues paid for premium subscriptions and the associated ability to use Megaupload for storage and transmission of files.[155] Although there are many ways to use such a service illegally, it is just as common to use a cyberlocker legitimately,

145 *Id.* at 3–4.

146 *See* Indictment*, supra* note 18, at 6. An example of a third-party linking site is Releaselog, http://www.rlslog.net, which allows users to search for download links for various movies, shows, and games.

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.* at 7.

151 *Id.* at 4.

152 Users who were not registered had only limited storage allowances and any content not downloaded within twenty-one days of upload was automatically purged from the system. Non-paying but registered members could store data for ninety days without anyone downloading it before it would be deleted. *Id.* at 4–5.

153 *Id.* at 5.

154 *Id.*

155 *Id.* at 3.

especially with large files that are not easily sent online otherwise.[156]

In the indictment, the government included a list of property subject to forfeiture, including various physical properties, bank accounts held by Megaupload and its upper management, and any and all domain names associated with Megaupload and its related companies.[157] The government also declared an intent to seek forfeiture of substitute assets should any of the listed assets be unavailable.[158] However, it is important to note that nowhere does the indictment say that the data stored on Megaupload is on notice for forfeiture, although it does say that the provided list of property subject to forfeiture is non-exhaustive.[159]

When the government seized Megaupload's domain name in mid-January on a court order from the U.S. District Court in Alexandria, Virginia, they effectively blocked access to all data hosted on Megaupload.com for all users.[160] When users tried to access Megaupload, they were directed to a splash page stating that the domain name had been seized and indicating the charges that had been filed against Megaupload.[161] In other words, by simply seizing the domain name "Megaupload.com" and thereby denying all of Megaupload's users access to their data, the government was able to effectively seize the twenty-five million gigabytes of data on the associated servers, whether that data was infringing or not.[162] This is another example of a key difference between traditional physical asset seizures and digital asset seizures: digital asset seizures can potentially impact a much wider range of innocent third parties than a traditional physical asset seizure. For example, even if the government were to seize an entire branch office of a national bank to get at allegedly criminal assets, that seizure would only adversely impact the people with accounts at that bank

156 For example, most email programs have a twenty-five megabyte attachment size limit, and any video file or collection of photos quickly exceeds that limit, making another mode of transmission necessary. It is for this reason that many legitimate users turn to cyberlockers to fulfill their needs. *See, e.g.*, *Attachment Size Limit*, GMAIL HELP, http://support.google.com/mail/bin/answer.py?hl=en&answer=8770 (last visited Aug. 10, 2013).

157 Indictment, *supra* note 18, at 66–71. The full list of seized domain names included Megaupload.com, Megavideo.com, Megaporn.com, and others allegedly involved in the "Mega Conspiracy." *Id.* at 2, 71.

158 *Id.* at 72.

159 Superseding Indictment, *supra* note 139, at 37–42.

160 Chloe Albanesius, *Recovering Legitimate Megaupload Files? Good Luck With That*, PCMAG.COM (Jan. 20, 2012, 4:07 PM), http://www.pcmag.com/article2/0,2817,2399162,00.asp; Department of Justice Office of Public Affairs, *Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement*, U.S. DEPARTMENT OF JUSTICE (Jan. 19, 2012), http://www.justice.gov/opa/pr/2012/January/12-crm-074.html.

161 To view the splash page, visit http://web.archive.org/web/20120211174603/http://www.megaupload.com/.

162 Brief of Kyle Goodwin, *supra* note 132, at 1–3.

branch, not all of the customers of the entire national bank as a whole. In *Megaupload*, however, simply seizing one domain name affected every single one of the millions of users dependent on that site.[163] This major difference in potential scale of impact on third parties makes increased third-party protections during digital asset seizures essential.

On January 30, 2012, the government stated that it had finished copying the data it needed and had concluded its investigation of the data on Megaupload's servers.[164] The government then informed the companies Megaupload had hired to host the data on their servers—Cogent and Carpathia—that they could delete the data from the servers; however, neither hosting company did so.[165] Moreover, in order to fight for the return of the non-infringing users' data, Carpathia Hosting teamed up with the Electronic Frontier Foundation ("EFF") to challenge the seizure of the data.[166] Together, the two organizations created MegaRetrieval.com, a website which directs Megaupload users to contact the EFF with information that can help them understand the scope of the seizure's effect and that can help them build a case for the data's safe return to innocent users.[167] However, due to the slow nature of the legal process, the deferral of hearings on this issue,[168] and the fact that Kim Dotcom's extradition hearing is not until November 2013 at the earliest, there is no clear end in sight for users seeking return of their data.[169] Unfortunately, allowing this issue to remain unresolved harms both the innocent users and the hosting companies paying out of their own pockets to preserve the Megaupload data.[170]

---

163 Albanesius, *supra* note 160.

164 Julie Samuels, *EFF Requests Information from Innocent Megaupload Users*, ELECTRONIC FRONTIER FOUNDATION (Jan. 31, 2012), https://www.eff.org/deeplinks/2012/01/eff-requests-information-innocent-megaupload-users.

165 Jon Brodkin, *US Argues it Shouldn't Have to Give Megaupload User His Legit Files*, ARS TECHNICA (June 11, 2012, 12:02 PM), http://arstechnica.com/tech-policy/2012/06/us-argues-it-shouldnt-have-to-give-megaupload-user-his-legit-files/; Samuels, *supra* note 164.

166 Samuels, *supra* note 164.

167 MEGARETRIEVAL, www.megaretrieval.com (last visited Sept. 14, 2013); Samuels, *supra* note 164.

168 Schoenberg, *supra* note 139.

169 Cyrus Farivar, *Kim Dotcom Could be Safe From Extradition to the U.S. Until 2014*, ARS TECHNICA (June 10, 2013, 3:10 PM), http://arstechnica.com/tech-policy/2013/06/kim-dotcom-could-be-safe-from-extradition-by-us-authorities-until-2014 [hereinafter Farivar, *Kim Dotcom Could be Safe*] (Kim Dotcom's extradition hearing has been delayed again, moving from August 2013 back to November 21, 2013, with a backup date of April 14, 2014); Cyrus Farivar, *Kim Dotcom Offers to Come to U.S. Rather than be Extradited,* ARS TECHNICA (July 10, 2012, 6:30 PM), http://arstechnica.com/tech-policy/2012/07/kim-dotcom-offers-to-come-to-us-rather-than-be-extradited [hereinafter Farivar, *Kim Dotcom Offers to Come to U.S.*].

170 Carpathia Hosting is paying $9,000 per day to preserve the data on the Megaupload servers. Ernesto, *Injustice Continues as Megaupload User Data Negotiations Go Bust*, TORRENT FREAK (Sept. 13, 2012), http://torrentfreak.com/injustice-continues-as-megaupload-user-data-negotiations-go-bust-120913.

1. Fighting for the Innocent Users—The EFF and Kyle Goodwin

In order to try and force the government to return the data, the EFF and other Internet rights supporters[171] rallied behind one particular Megaupload user, Kyle Goodwin, presumably as a test case, and filed a motion for the return of his digital property.[172] Goodwin asserts that he represents the interests of a substantial group of Megaupload users who used the site for legitimate purposes but to whom the government has no plan to return their data.[173]

All parties have agreed that Goodwin is a non-infringing Megaupload user, and yet he is still being denied access to his data, data that is critical to his growing small business.[174] Goodwin's business involves filming local high school sporting events within his state, and he relied on his premium subscription[175] to Megaupload to store and share his large video files.[176] Since the attachment limit for most email services is twenty-five megabytes,[177] Goodwin needed an efficient way to store and share large files with his clients—Megaupload's premium subscription option seemed like the perfect solution.[178] When Megaupload was seized in January 2012, Goodwin, like all other users, lost access to the data he had stored on Megaupload with no recourse provided to petition for its return.[179]

On March 20, 2012, Carpathia, supported by Goodwin on this motion, sought emergency relief from the court in order to try and force the government to create a plan to get innocent users their data back.[180] Then, on April 13, 2012, at the hearing on Carpathia's motion for emergency relief, the court ordered good faith negotiations between all parties to both ensure the data was properly preserved and create a plan to have the data returned to Megaupload users.[181] At an April 26, 2012, meeting with Magistrate Judge Anderson, although the parties made progress on an agreement to preserve the data, the parties failed to

171 Example rights supporters include Abraham Sofaer from The Hoover Institution and John Davis from Williams Mullen. Brief of Kyle Goodwin, *supra* note 132, at 13.

172 Robert Hilson, *Government Seizure of Megaupload Digital Assets Draws Ire of Aggrieved Parties*, ACEDS (June 7, 2012), http://www.aceds.org/government-seizure-of-megaupload-digital-assets-draws-ire-of-aggrieved-parties/.

173 *Id.*

174 Brief of Kyle Goodwin, *supra* note 132, at 13.

175 As stated above, a premium subscription allowed for users to upload and download files practically without limit and allowed for perpetual storage without needing to meet download quotas to preserve the files on the server. *See supra* notes 152–154 and accompanying text.

176 Brief of Kyle Goodwin, *supra* note 132, at 4–5.

177 *See, e.g.*, *supra* note 156 and accompanying text.

178 Brief of Kyle Goodwin, *supra* note 132, at 4–5.

179 Samuels, *supra* note 164.

180 Brief of Kyle Goodwin, *supra* note 132, at 3.

181 *Id.*

finalize a plan to return the data to non-infringing users.[182]

During negotiations, Goodwin, in an effort to negotiate in good faith, agreed to allow the government to delay planning for access to user data in order to first address negotiations for the preservation of the data on the hosting servers, despite the fact that this plan of action could continue to harm his business.[183] However, when the government submitted a proposal that not only failed to include any provisions for access to data, but also proposed to require an additional judicial ruling before any access could be granted, Goodwin decided to take further action.[184] As a result, on May 25, 2012, the EFF filed a brief supporting Goodwin's efforts to reclaim his data.[185] The overarching concern throughout the brief is that Goodwin and other non-infringing Megaupload users have been deprived of their property as a result of the government's seizure of Megaupload's servers and domain name.[186] Further, the brief asserts that if the government is allowed to proceed as they please, those non-infringing users will be so deprived for several years, if not permanently.[187] The brief petitions the court to establish new procedures to protect innocent users from the government's increasing use of domain name and other digital asset seizures; the brief argues that the court should "ensure that such innocent users do not become regular collateral damage" in these types of seizures.[188] Although the brief does not address any specific remedies, it does urge the court to use its ruling in *Megaupload* as a starting point to create the necessary procedures and standards to protect the property and due process rights of innocent users in digital asset seizures.[189] The EFF has clearly seen the danger that digital asset seizures can pose to third parties, and is working to assure that the *Megaupload* court recognizes that danger and acts in a way that will best protect the interests of the innocent.

### 2. The Need to Protect Innocent Users and Preserve the Utility of Cyberlockers

Kyle Goodwin used Megaupload to store and transmit large video files online[190] rather than having to send the data to customers on physical media, such as a DVD or a USB drive; such use is a logical

182 *Id.* at 4.
183 *Id.*
184 *Id.*
185 *Id.* at 13.
186 Brief of Kyle Goodwin, *supra* note 132.
187 *Id.* at 1.
188 *Id.* at 2.
189 *Id.*
190 *Id.* at 4.

and expected legal use of a cyberlocker. Especially for someone with a high data volume business like Goodwin, Megaupload and other similar cyberlockers allow for easy access to data from anywhere with an Internet connection, giving the user greater flexibility in how they manage their data.[191] Using a cyberlocker for data storage also makes it possible to share large files over the Internet, a key component of any data-based business in the digital age and something that typically cannot be done via email.[192] These features make cyberlockers critical for both personal and business data storage, so assuring that asset seizure proceedings have appropriate protections in place to shield innocent third parties from cyberlocker seizures is necessary to assure that people will have continued access to non-infringing data in the event of a seizure targeting the cyberlocker that data is hosted in.

Since Megaupload is a massive cyberlocker,[193] it clearly illustrates the damage that can be dealt upon innocent users when digital seizure is brought to bear on the cyberlocker as a whole rather than simply targeting the infringing data. For instance, seizing the entirety of Megaupload to get at the infringing content allegedly uploaded by a subset of users is arguably analogous to the government attempting to seize the assets of Citibank as a whole in order to get at the bank accounts held by a subset of account holders engaged in criminal activity. After extensive research, it appears that the government does not typically make such broad bank seizures, and any attempt to do so would doubtlessly be deemed excessive. Thus, the *Megaupload* case demonstrates how mass digital seizures disproportionately impact innocent users by failing to target and seize only those infringing assets connected to the crimes.[194]

The fact that the government can make such a broad seizure is another concerning aspect of digital asset seizures. While seizing the entire assets of Citibank would be decried as excessive, it is not yet widely understood that seizing the domain name of a massive cyberlocker impacts innocent users on a similar scale. *Megaupload* clearly shows the dangerous trend toward digital asset seizures that excessively impact innocent users, and thus makes apparent the need for

191 For an example of a cyberlocker still in operation, see RAPIDSHARE, http://www.rapidshare.com (last visited Sept. 15, 2013).

192 *See, e.g.*, *id.* (demonstrating how a key function of cyberlockers is allowing users to quickly and easily send their files to others via email and social media). Most email programs have a twenty-five megabyte attachment size limit, and many video files or collections of photos can quickly exceed that limit, making another mode of transmission necessary. *See, e.g.*, *Attachment Size Limit*, *supra* note 156.

193 Megaupload was a cyberlocker hosting twenty-five petabytes of data. Kravets, *Megaupload User Demands Return of Seized Content*, *supra* note 21.

194 Brief of Kyle Goodwin, *supra* note 132.

immediate reform targeted at making sure digital asset seizures do not make innocent users the criminal justice system's constant collateral damage.

### 3. Upcoming Hearing on Dealing with Seized Data Will Likely Guide How Future Mass Data Seizure Cases Handle Impact on Third Parties

In October 2012, the federal district judge hearing the *Megaupload* case in Virginia, Judge O'Grady, ordered the parties to submit briefs for a hearing on how to deal with the twenty-five petabytes of data held in limbo by the seizure of Megaupload's domain.[195] This is the first significant progress made on this issue since the judge deferred making a decision back in June 2012.[196] The judge feels he cannot rule on the issue of how to handle the seized data without an evidentiary hearing,[197] which is at least suggests that the court is aware that the digital property of innocent third parties hangs in the balance, and that allowing the government to simply delete all the users' data without considering the impact on the parties would be unwise. Since this case will set a precedent for how to handle third-party protections in future digital asset seizures, it is important that any decisions on this issue are carefully made. Moreover, the case could set a precedent with regard to whether or not data on a third-party server counts as protectable personal property, a decision that would likely have wide-ranging repercussions. It is likely that the judge will also have to consider whether or not data someone stores on a server owned by someone else counts as protectable personal property. The way the judge rules on that issue, if indeed he does, would have wide-ranging repercussions on any future case dealing with data seizure. While the case against Megaupload is facing difficulties over extraditing Kim Dotcom from New Zealand,[198] Megaupload has petitioned the court for permission to make a special appearance to support the EFF and others seeking the return of users' data,[199] but has so far been unsuccessful.[200]

---

195 Jeremy Kirk, *Judge Weighs Fate of Orphaned Megaupload Data*, PCWORLD (Oct. 7, 2012, 11:02 AM), http://www.pcworld.com/article/2011289/judge-weighs-fate-of-orphaned-megaupload-data.html.

196 Schoenberg, *supra* note 139.

197 Kirk, *supra* note 195.

198 Farivar, *Kim Dotcom Could be Safe*, *supra* note 169; Farivar, *Kim Dotcom Offers to Come to U.S.*, *supra* note 169; Dave Neal, *Locked Out Megaupload Users Will Get Their Day in Court*, THE INQUIRER (Oct. 5, 2012, 9:38), http://www.theinquirer.net/inquirer/news/2214893/locked-out-megaupload-users-will-get-their-day-in-court.

199 Kirk, *supra* note 195.

200 The last movement on this issue was the government's opposition brief to Megaupload's limited appearance, filed February 14, 2013, but no ruling has yet been issued. Joe Mullin, *Keep Megaupload Out of Our Server Seizure Case, US Lawyers Say*, ARS TECHNICA (Feb. 15, 2013, 7:35 PM), http://arstechnica.com/tech-policy/2013/02/keep-megaupload-out-of-our-server-seizure-case-us-lawyers-say.

So far, the crux of the government's argument that third-party users cannot challenge the seizure of their data has been that the data in question was never physically seized.[201] The government's basic argument has been that since it did not physically seize the servers Megaupload's data is hosted on—rather, it only seized the domain name and copied the data from the servers—the government does not actually possess the users' property and thus cannot return it.[202] This argument is only possible because the government is taking advantage of the fact that digital assets, unlike traditional physical assets, do not need to be physically seized in order to be effectively seized. However, since there is an index of all files on the Megaupload servers,[203] it would be possible for the government to selectively allow access to the Megaupload data for innocent users. Or, the government could simply provide copies of the data to the innocent users by using the file index to determine what data belongs to innocent users as opposed to infringing users.[204] Goodwin has previously countered the government's argument by asserting that it was the government's failure to conclusively seize the data that led to the data's vulnerable position in limbo subject to deletion, and thus the government should have to create a solution to allow innocent users access to their data.[205] These arguments will likely be repeated and consolidated in the briefs for the upcoming evidentiary hearing.

As of now, full briefs on this issue have not been filed, though the government has attempted to limit the breadth of the upcoming hearing by filing a motion to restrict the hearing to cover only the applicability of Federal Rule of Criminal Procedure 41(g).[206] In other words, the government argues that the upcoming hearing on Megaupload user data should be limited to the subject of whether or not Goodwin in fact has the requisite interest in property seized by the government from Megaupload.[207] The government asserts that this interest must be shown before any further action is taken in order to avoid a "fishing expedition" that could negatively impact the *Megaupload* litigation as a whole.[208] Subsequent to the government filing its motion, Megaupload has sought leave to participate as a party to Goodwin's case, rather than

201 Brodkin, *supra* note 165.
202 *Id.*
203 Indictment, *supra* note 18.
204 The Megaupload top management maintained a file index of all data on their servers. *Id.* at 7.
205 Brodkin, *supra* note 165.
206 Brief of the United States Regarding the Breadth and Format of a Hearing to Determine the Applicability of Federal Rule of Criminal Procedure 41(g), United States v. Dotcom, No. 1:12CR3 (E.D. Va. Oct. 30, 2012).
207 *Id.*
208 *Id.* at 1–2.

simply file briefs in support of his motion for the return of his data.[209] The government has opposed this motion,[210] and Goodwin has countered by arguing that Megaupload's particular knowledge regarding the circumstances surrounding the searches and seizures of Megupload.com are vital to the question of whether or not the user data hosted on Megaupload's servers had been properly seized.[211] There has been no recent substantial progress on the issue of user data. However, the fact that LeaseWeb, a Dutch company hosting Megaupload's data in the Netherlands, deleted all Megaupload user data it had been hosting as of February 1, 2013,[212] prompted Megaupload to file a letter in July 2013 urging the court to reopen negotiations on the issue of user data as soon as possible in order to prevent further deletions and to protect the data of innocent users.[213]

Although the issue at hand in the case deals with asset seizure and forfeiture, the underlying issue in *Megaupload* is how digital data stored in a cyberlocker should be treated. In short, the *Megaupload* court has to determine the essence of what a digital asset seizure consists of; is seizing a domain name and blocking access to data a seizure and forfeiture subject to third-party protections, or is the lack of any physical seizure and possession enough to prevent the government's actions from crossing the line into a seizure within the territory of existing forfeiture laws? Ultimately, the court's decision as to whether or not the domain name seizure of Megaupload.com was also a seizure of all associated data will have a huge impact on all future digital asset seizure cases and will necessarily impact what remedies, if any, innocent third parties will have access to going forward.

The government has also asserted that Goodwin's claimed business-related revenue loss is not an "irreparable harm" and therefore

---

209 Opposition of the United States to Defendant Megaupload Limited's Appearance and Participation in Proceedings Relating to Non-Party Kyle Goodwin's Motion for Return of Property Pursuant to Rule 41(g), United States v. Dotcom, No. 1:12CR3 (E.D. Va. Feb. 14, 2013).

210 *Id.*

211 Brief of Kyle Goodwin in Response to Opposition of the United States to Defendant Megaupload's Limited Appearance and Participation in Proceedings Relating to Non-Party Kyle Goodwin's Motion for Return of Property Pursuant to Rule 41(g), United States v. Dotcom, No. 1:12-cr-00003-LO (E.D. Va. Feb. 28, 2013).

212 LeaseWeb, Megaupload's former hosting provider in the Netherlands, deleted user data from all 690 of its servers on February 1, 2013. The data on those servers was mostly from European Megaupload users. Ernesto, *Leaseweb Wipes All Megaupload User Data, Dotcom Outraged*, TORRENT FREAK (June 19, 2013), http://torrentfreak.com/leaseweb-wipes-all-megaupload-user-data-dotcom-outraged-130619.

213 Letter from William A. Burck, Quinn Emanuel Urquhart & Sullivan, LLP, and Ira P. Rothken, The Rothken Law Firm, to The Honorable John F. Anderson, U.S. Magistrate Judge, U.S. Dist. Court for the E. Dist. of Va. (July 3, 2013), *available at* http://www.techfirm.com/storage/usmega/Ltr%20to%20Judge%20Anderson%207%203%2013.pdf.

cannot outweigh the heavy burden the government would have to undertake to return the data.[214] The government suggests Goodwin and others in his position hire forensic data retrieval experts or sue Carpathia or Megaupload for the return of their data.[215] However, neither remedy is sufficient to protect innocent third parties, since each requires additional time and resources to hire experts and lawyers to fight for the return of data that was seized as a result of someone else's crimes. Given that the government is meant to protect the interests of the innocent, in situations where law enforcement efforts harm innocent third parties, the government should be required to both minimize and remedy that harm without requiring extra effort from those third parties.

In short, the judge's ruling in the upcoming hearing, and in the *Megaupload* case as a whole, will help to dictate how and if innocent third parties will be able to retrieve data in this sort of mass digital asset seizure going forward. If the judge does not curtail the government's actions in this case, then it is likely that the use of federal asset forfeiture will become both more common and more harmful as it moves into digital asset seizures, the potential for which was shown in both the Operation in Our Sites seizures and *Megaupload*. If, however, the judge takes a more circumspect approach and lays the foundation for clear third-party protections in digital asset seizures like *Megaupload*, then the law will have taken its first major step toward making the changes necessary to protect innocent third parties in digital asset seizures.

## III. POTENTIAL REMEDIES TO ADDRESS PROBLEMS HIGHLIGHTED BY DIGITAL ASSET SEIZURES

Faced with the fundamental differences between traditional physical assets and digital assets, the law of asset forfeiture must adapt to provide proper third-party protections in digital asset seizures. As discussed above, the third-party protections in place for more traditional seizures and forfeitures were already showing signs of insufficiency before digital asset seizures exacerbated the problem.[216] The subsequent Operation In Our Sites domain name seizures highlighted the weaknesses inherent in existing third-party protections and the inability of those protections to properly guard innocent owners against digital asset seizures.[217] The currently pending *Megaupload* case displays those same problems to such an extent that these failings can no longer be

214 Brodkin, *supra* note 165.
215 *Id.*
216 *See supra* Part I.
217 *See supra* Part II.A.

ignored.[218]

Although there must be a balance between protecting third parties and allowing the government to continue to use asset forfeiture as a deterrent against criminal activity in the digital sphere, that balance needs to be heavily weighted toward protecting innocent third parties. Protections as they stand either force the innocent owner to wait until after a criminal conviction to challenge a criminal asset forfeiture,[219] or require an innocent user to meet a high burden of proof in a potentially lengthy parallel civil forfeiture proceeding.[220] The domain name seizures showed the government's ability to delay for months, if not years, and the delays in *Megaupload* highlight the same problem.[221] Worst of all, the government is attempting to circumvent asset forfeiture laws entirely by arguing that digital asset seizures cannot become true forfeiture actions—nor gain the use of the associated third-party protections—because digital asset seizures do not require the government to physically possess the property.[222] If this argument prevails, then the potential for abuse will be immense and innocent third parties will likely suffer from data seizures they cannot challenge and from which they may never be able to recover their data.

Digital asset seizures should be considered seizures within the traditional definition even though the assets in question are digital in much the same way that digitally pirating a movie is considered theft.[223] For many years, the Motion Picture Associate of America ("MPAA") has been at the forefront of the fight against digital piracy.[224] The MPAA vows to work toward increasing copyright protections in federal and state laws and commits to working with local, federal, and international law enforcement to combat and prosecute pirates.[225] Moreover, there is no question that law enforcement agencies treat piracy as theft even though a pirated copy is simply one of a theoretically unlimited number of copies that could be made of a movie without ever depriving the owner of the original or restricting the owner's ability to make his own copies in any way.[226] Even though

218 *See supra* Part II.B.
219 *See supra* Part I.A.
220 *See supra* Part I.B.
221 *See supra* Part II.A–B.
222 *See supra* Part II.B.
223 *Content Protection*, MOTION PICTURE ASSOCIATION OF AMERICA, http://www.mpaa.org/contentprotection (last visited Aug. 11, 2013)
224 *Id.* (outlining the MPAA's approach to content protection, which includes pushing for strong intellectual property rights legislation and working with law enforcement to combat piracy).
225 *Id.*
226 *See, e.g.*, *Types of Content Theft*, MOTION PICTURE ASSOCIATION OF AMERICA, http://www.mpaa.org/contentprotection/types-of-content-theft (last visited Aug. 11, 2013) (the MPAA lists peer-to-peer (P2P) sharing and streaming as examples of content theft, both of which

copying and distributing movies or other digital media does not result in the same physical deprivation as a physical theft, pirates, downloaders, and the websites that host pirated files[227] are strictly punished.[228]

If this kind of piracy is considered theft, then there is precedent for thinking of digital assets as property that can be stolen, even if what is stolen is a copy. If the owner of the original copy of a movie has property rights sufficient to pursue action against those who make illegal copies, those property rights should similarly serve to protect him against wrongful seizure and forfeiture whether actual or digital. If merely copying a movie counts as piracy,[229] then the government copying the data on Carpathia's servers, and blocking access to the data by seizing Megaupload's domain name, should also count as a violation of the rights of the innocent owners caught up in the seizure targeting infringing content. Until measures are put in place to ensure the return of digital assets to innocent third parties, the law should consider the Megaupload seizure, like piracy,[230] to be theft.[231] In fact, when done outside any form of formal forfeiture proceedings, the *Megaupload* seizure is perhaps even more analogous to traditional theft than piracy because there the government both copied the data and deprived the innocent owner of all access rights to the original—in the case of piracy, the pirated copy does not deprive the owner in this way.

If the government's actions in *Megaupload* can represent a form of theft by depriving innocent owners of access to their data, then the same should be true in the case of the domain name seizures. As with the *Megaupload* seizure, domain name seizures take a digital asset—the domain name and its associated content—and block all access to it by the owner.[232] Although a domain name, like any digital asset, cannot be physically seized and forfeited, the government can deprive innocent owners of their domain names and the associated data without providing proper recourse to challenge the seizure (and indeed, the government

work in purely digital copies); *see also A Warning With Teeth – N.Y. Rolls Up Movie Piracy Rings*, FEDERAL BUREAU OF INVESTIGATION (Jun. 30, 2006), http://www.fbi.gov/news/stories/2006/june/iprny063006.

227 When the federal government took down Megaupload.com, one of the main reasons cited was that both websites hosted a vast amount of pirated media. *See, e.g.*, Indictment, *supra* note 18, at 1 (Megaupload indicted for criminal copyright infringement by electronic means).

228 *See, e.g.*, Kurt Orzeck, *Ninjavideo Co-Founder Sentenced to 22 Months for Piracy*, REUTERS (Jan. 6, 2012, 3:23 PM), http://www.reuters.com/article/2012/01/06/idUS233397294820120106 (Ninjavideo co-founder convicted for criminal copyright infringement—piracy—sentenced to twenty-two months, five hundred hours of community service, and must pay back the approximately $210,000 she made on Ninjavideo).

229 *Content Protection FAQs*, *supra* note 223.

230 *Id.*

231 *Supra* Part II.B (the government and the innocent owners have yet to come to an agreement about how, or if, the seized data will be returned to the innocent owners).

232 *Supra* Part II.A–B.

has done just that).[233] Thus, if piracy is considered punishable theft even when the owner is never deprived of access to the original asset,[234] then digital asset seizures that do deprive innocent owners of access to their digital assets, like domain name seizures and *Megaupload*, should most certainly be considered a violation of the data owner's rights on an at least equal level to that of piracy. Whether or not the law goes that far and treats seizure as theft, at the very least, the situation calls for legal protections to guard against digital asset seizures causing undue harm to innocent third parties.

This reasoning creates the more straightforward potential remedy for mass data seizures like that in *Megaupload*—declare that seizing a domain name or copying files off a server counts as theft if done outside proper seizure and forfeiture procedures.[235] Existing asset forfeiture laws dictate procedures that must be followed for an asset to be seized subject to forfeiture;[236] at the very least, digital asset seizures should be subject to the same procedures to avoid being considered theft of an innocent owner's data.[237] Additionally, requiring digital asset seizures to follow existing asset forfeiture procedure would allow innocent owners to invoke existing third-party protections, at least until more tailored protections for digital assets are created. Furthermore, although the Operation In Our Sites seizures and Megaupload's seizure were all carried out with a proper court order,[238] the government's attempt to avoid following existing forfeiture procedure could lead to abuse of the seizure and forfeiture system.[239] Additionally, the original seizure orders likely did not take into account exactly how broad an impact a digital asset seizure could have on innocent third parties. Unlike seizing a car or bank account, seizing a domain name, like Megaupload.com, can have a negative impact on millions of innocent users.[240] Unless the government is required to consider the impact on third parties and target their seizure requests so as to cover, to the extent possible, only the data connected to the alleged crime, mass digital asset seizures will likely continue to plague innocent third parties.

The need for more governmental consideration of third parties leads to yet another potential remedy—requiring that the government

233 *Id.*

234 *Types of Content Theft*, *supra* note 226 (piracy functions by making a copy of the copyrighted material, not by stealing the original).

235 An opposing idea is the one illustrated by the government's argument in *Megaupload*—seizing a domain name does not count as a seizure of the data associated with that domain if the government is not in physical possession of the data. *See, e.g.*, Brodkin, *supra* note 165.

236 *Supra* Part I.A–B.

237 *Id.*

238 *Supra* Part II.A–B.

239 *Id.*

240 *Supra* Part II.B.

target only the data that is either necessary for the investigation or is connected to the alleged crime or criminal. This seems a particularly apt solution for situations where a file index exists, like *Megaupload*,[241] since an index provides the government with the necessary tools to distinguish between the files of infringing and non-infringing users. When the website is a cyberlocker or similar large storage site with a large user base, it is imperative that the government take precautions to avoid as much damage to innocent owners as possible. The government's seizure of the domain name of another cyberlocker like Megaupload would effectively block access to all data for millions of innocent users should never be allowed to happen again.

Another potential remedy would be to create individualized copies of the seized data to return to innocent owners. This is possible because the inherent nature of digital data files means that they can theoretically be endlessly and perfectly copied—the very feature that allows them to be seized without taking physical possession.[242] Thus, the government could hold onto the original data and create copies of the data to return to innocent users; because digital assets do not need to be physically possessed, it is possible to copy the required segment of data and return it to an innocent third party while still preserving the entire original body of seized data for the government's use.[243] Although this would require more work on the part of the government, that should not disqualify it as a potential remedy.[244] Current seizure laws are highly deferential to the government, favoring convenience to government investigators over third-party protections.[245] However, given that digital seizures completely alter the scope of asset deprivations and the burden of returning property—thousands, if not millions, of innocent users can be affected by a single digital asset seizure, and returning property could be as simple as reinstituting third parties' access to the files online—the balance of interests in asset seizure and forfeiture law needs to be recalibrated.

It is also important to consider the impact of weak third-party protections in digital asset seizures on the growth of business. Now that so many websites and businesses rely on either large cyberlockers or other cloud-based storage services,[246] allowing the government to continue having as much freedom as they have had in Operation In Our

241 Indictment, *supra* note 18 at 7.

242 Brodkin, *supra* note 165.

243 *Id.*

244 *Id.*

245 *Supra* Part I.B; *supra* Part I.A.

246 *See, e.g.*, cloud-based storage site DROPBOX, www.dropbox.com, (last visited Sept. 18, 2013), cloud-based email service provider GMAIL, www.gmail.com, (last visited Sept. 18, 2013) and cloud-based cyberlocker RAPIDSHARE, www.rapidshare.com (last visited Sept. 18, 2013).

Sites and *Megaupload* could have a devastating effect on businesses.[247] If the government can easily seize and hold an entire storage site or cloud server based on the actions of a subset of users, no business will be able to rely on the availability or safety of their data and would shy away from using such services. Such a result could slow down the progress of digital and Internet-based businesses and could cause people to rightfully doubt the security of their files hosted by any digital or cloud-based service. If cloud-based businesses are to continue to develop, increased third-party protections against digital asset seizures are absolutely required. If cases like *Megaupload* become the norm, it will be extremely difficult to conduct a business centered on digital or cloud-based assets.

In sum, because seizing digital assets does not necessarily require physical possession,[248] and because digital asset seizures and forfeitures can potentially have a much wider range of impact on innocent third parties than traditional physical asset forfeitures, tailored third-party protections are necessary to prevent injustice. In both *Megaupload* and future digital asset forfeiture cases, courts must balance the rights of the government to use seizure and forfeiture to combat crime against the rights of innocent third parties to have the data they stored in cyberlockers or other digital storage services protected from capricious seizure and forfeiture. Because digital asset seizures have a broad range of impact on third parties, the government must either be required to target data for seizure more carefully, or to copy and return portions of seized data that belong to innocent owners. It may be that traditional physical asset forfeiture cannot be fully adapted to deal with digital assets without losing its effectiveness against physical property. In that case, an entirely new asset forfeiture procedure must be implemented to deal with the unique problems created by digital assets.

## CONCLUSION

In conclusion, the history of asset seizure and forfeiture law shows a consistent weakness in third-party protections that is highlighted and exacerbated by digital asset seizures and forfeitures. The *Megaupload* case and the Operation In Our Sites seizures are clear examples of the potentially massive scope of damage to innocent third parties that can be caused by digital asset forfeiture. These weaknesses show that

247 *See, e.g.*, Nicole Perlroth & Quentin Hardy, *Antipiracy Case Sends Shivers Through Some Legitimate Storage Sites*, N.Y. TIMES, (Jan. 20, 2012), http://www.nytimes.com/2012/01/21/technology/antipiracy-case-sends-shivers-through-some-legitimate-storage-sites.html?_r=0 (describing how cloud-based services and storage sites defend themselves and distinguish their services from the Megaupload model).

248 Brodkin, *supra* note 165.

increased third-party protections tailored to address digital asset seizures and forfeitures are necessary to prevent gross injustice.

*Elizabeth Friedler**

* Staff Editor, CARDOZO ARTS & ENT. L.J. Vol. 31, J.D. Candidate, Benjamin N. Cardozo School of Law (2014); B.A. Double Major in Philosophy and Japanese Language & Literature, Wellesley College (2010). I would like to thank Professor Brett Frischmann for his guidance and for sharing his time and knowledge with me throughout this process. 