Berkeley Technology Law Journal

Volume 32 | Issue 3 Article 3

5-28-2018

DETERRING CYBERCRIME: FOCUS ON INTERMEDIARIES

Aniket Kesari
UC Berkeley School of Law, Jurisprudence & Social Policy

Chris Hoofnagle
UC Berkeley School of Law & School of Information.

Damon McCoy
New York University Tandon School of Engineering

Link to publisher version (DOI)
ttps://doi.org/10.15779/Z387M04086

DETERRING CYBERCRIME: FOCUS ON INTERMEDIARIES

Cover Page Footnote
Damon McCoy: "The author thanks the National Science Foundation under contract 1619620 and a gift from Google for financial support of this project." "The authors thank the Center for Long Term Cybersecurity for financial support of this project, and Laurin Weissinger, Annemarie Bridy, and Zachary Goldman for critical feedback."

DETERRING CYBERCRIME: FOCUS ON INTERMEDIARIES

Aniket Kesari,[†] Chris Hoofnagle[††] & Damon McCoy[†††]

ABSTRACT

This Article discusses how governments, intellectual property owners, and technology companies use the law to disrupt access to intermediaries used by financially–motivated cybercriminals. Just like licit businesses, illicit firms rely on intermediaries to advertise, sell and deliver products, collect payments, and maintain a reputation. Recognizing these needs, law enforcers use the courts, administrative procedures, and self–regulatory frameworks to execute a deterrence by denial strategy. Enforcers of the law seize the financial rewards and infrastructures necessary for the operation of illicit firms to deter their presence.

Policing illicit actors through their intermediaries raises due process and fairness concerns because service–providing companies may not be aware of the criminal activity, and because enforcement actions have consequences for consumers and other, licit firms. Yet, achieving direct deterrence by punishment suffers from jurisdictional and resource constraints, leaving enforcers with few other options for remedy. This Article integrates literature from the computer science and legal fields to explain enforcers' interventions, explore their efficacy, and evaluate the merits and demerits of enforcement efforts focused on the intermediaries used by financially–motivated cybercriminals.

DOI: https://doi.org/10.15779/Z387M04086

† UC Berkeley School of Law, Jurisprudence & Social Policy.

†† UC Berkeley School of Law & School of Information.

††† New York University Tandon School of Engineering. The author thanks the National Science Foundation under contract 1619620 and a gift from Google for financial support of this project.

The authors thank the Center for Long Term Cybersecurity for financial support of this project, and Laurin Weissinger, Annemarie Bridy, and Zachary Goldman for critical feedback.

TABLE OF CONTENTS

I. INTRODUCTION 1094

II. LITERATURE REVIEW 1096

III. BUSINESS CONSTRAINTS, RELEVANT ACTORS, AND ACTIVITIES 1099

A. BOTNETS 1102
B. ILLEGAL AND INFRINGING GOODS SELLERS 1103
C. INTERMEDIARIES AND INTELLECTUAL PROPERTY OWNERS 1103

IV. JUDICIAL INTERVENTIONS 1106

A. RULE 65 INTERVENTIONS 1106
1. Examples from Trademark Infringement 1110
2. Examples from Hacking and DDoS 1113
3. Criticisms of Rule 65 Interventions 1118

V. GOVERNMENT–LED INTERVENTIONS 1121

A. PRO-IP ACT DOMAIN SEIZURES 1121
B. GOVERNMENT INTERVENTION IN FINANCIAL SERVICES INTERMEDIARIES 1123

VI. PRIVATE REMEDIATION PROCEDURES 1125

A. EBAY VERO PROGRAM 1126
B. VISA IP ENFORCEMENT 1126
C. INTERNATIONAL ANTICOUNTERFEITING COALITION (IACC) 1128
D. BACKPAGE.COM: PRIVATE REMEDIATION AS A SCAFFOLD FOR CRIMINAL PROSECUTION 1128
E. COMMENTS ON VOLUNTARY AND SELF–REGULATING PROCEDURES 1130

VII. SUMMARY AND CONCLUSION 1130

I. INTRODUCTION

Businesses that sell illegal pharmaceuticals, counterfeit goods, or offer computer attacks online have similar goals and needs as ordinary firms. These enterprises must acquire new customers, have a supply chain, maintain a web presence, collect payments, deliver a product or service, and, finally, cultivate a positive reputation to encourage repeat sales. In pursuit of profit, the legitimate and illegitimate alike depend on many third parties, including web hosts, payment providers, and shipping companies.

Licit businesses are deterred from illegal acts by punishment, through fines, threats, and regulatory actions. But enforcers often cannot use traditional deterrence against financially–motivated cybercriminals because law enforcement is limited by scarce resources, competing enforcement priorities, and jurisdictional challenges. As a result, enforcers—both public and private—have turned to deterrence by denial approaches. Such approaches attempt to deter conduct by spoiling, reducing, or eliminating the benefits of computer crime. Frustrated by attempts to reach actual illicit actors, enforcers focus on third parties that are critical to business operation, thus denying cybercriminals' access to banking, web resources, or even shipping services. Cybercrime, often presented as ephemeral and stateless, can be reined in through attacking dependencies critical to its operation.

Much of the legal academic scholarship on Internet intermediaries focuses on intermediaries' general immunity from state law actions under the Communications and Decency Act Section 230 (CDA 230) or the provisions of the Digital Millennium Copyright Act (DMCA). CDA 230 creates broad immunity for Internet intermediaries, insulating them from the illegal acts of their users; intermediaries, even when given notice of noxious content, are not required to remove it.[1] The DMCA can shield providers from liability for user's infringing activities if certain steps are taken to receive and respond to takedown requests by intellectual property (IP) owners.[2]

This Article turns away from the CDA 230 and the DMCA procedures to focus on mechanisms that force intermediaries to address alleged user misbehavior. Specifically, this Article focuses on three mechanisms that are used to cause intermediaries to take or refrain from some action related to financially–motivated cybercrime. Parts II and III set the stage for the survey. Part II canvasses the literature on cybercrime and intermediaries. Part III discusses the business constraints of three kinds of actors: botnet operations, sites that offer illegal and infringing goods, and the contests among intermediaries and intellectual property owners. Part IV covers the use of Rule 65 of the Federal Rules of Civil Procedure (FRCP) and its allowance for broad forms of injunctive relief, and the Domain Name Service takedown procedures that use the U.S. government's ability to target infringing websites and make them inaccessible. Part V covers

1. 47 U.S.C. § 230 (2012).
2. 17 U.S.C. § 512 (2012).

administrative remedies focused on financial services intermediaries. Finally, part VI looks at self–regulatory procedures that intermediaries have established to allow IP owners and governments to block user activity.

An intermediary–focused approach raises due process and fairness concerns because intermediaries may not be privy to criminal activity, and enforcement mechanisms affect consumers and other licit firms. Cybercriminals may mask their behavior by commandeering ordinary users' accounts and computers for attacks and monetization of crimes. Thus, when an enforcer investigates and makes interventions, legal demands may fall upon third parties, individuals, and businesses that were merely used as conduits by the suspect. These intermediaries themselves may have been hacked or otherwise be cybercrime victims themselves. Additionally, compliance may impose costs on intermediaries and to civil society in the form of censorship or erosion of Internet anonymity as intermediaries are asked to know their customers[3] and make requirements that ordinary users provide documentation of their identity. Interventions are done *ex parte*, with surprising speed, raising the risk that others' interests may not be fully considered by a court. Finally, there is always the problem of claimant abuse—claims of wrongdoing may be motivated by anticompetitive interests or simple censorship.

In sum, this Article offers an exploratory look at an understudied area of intermediary interventions. Intermediary liability conversations typically surround CDA 230 and the DMCA, but our survey reveals that intermediaries can be subject to costly, broad interventions in cybercrime contexts. This Article highlights the current legal practices in this space, and evaluates their merits and demerits.

II. LITERATURE REVIEW

This Part highlights relevant literature from both a theoretical and legal perspective, starting with a brief overview of the literature on the economics of financially–motivated cybercrime. These pieces link the economics of cybercrime to the economics of crime more broadly, and identify the features of cybercrime that make it amenable to intermediary interventions. The focus then shifts to the legal theory concerning the

3. Anti–money laundering customer identification requirements are known as "Know Your Customer" regulations. *See* 12 U.S.C. § 635(i) (2012); 31 C.F.R. § 1020.200 et. seq. (2016).

extent to which intermediaries should be held liable, before turning to the implementation of legal rules and interventions.

Some cybersecurity literature focuses on intermediaries' centrality in Internet activity. Authors detail the both private and government policies that aim to thwart cybercrime and create secure systems. Goldman and McCoy set up the motivation for our inquiry in their paper, *Deterring Financially Motivated Cybercrime*.[4] For instance, they address how some cybercriminals are dependent upon a handful of payment processors, which empowers those payment processors to effectively combat criminals.[5] They argue that mainstream payment processors adopt policies that help thwart and deter cybercrime, in large part because payment companies want to maintain the integrity and the reputation of their own systems.[6] This is a boon for the government and potential victims of cybercrime because payment processors can interrupt a large portion of cybercrime without imposing direct costs on consumers.

Cybercrime is an increasingly professional endeavor that implicates activities involving American companies, or are otherwise subject to U.S. courts' jurisdiction. In *The Economics of Online Crime*, Moore et al. elaborate on how cybercrime professionalization lends itself to well-understood policy fixes.[7] They explain that criminal firms have emerged that specialize in botnet creation, phishing, and identity theft.[8] They argue, "[w]ith this new online crime ecosystem has come a new profession: the 'botnet herder'—a person who manages a large collection of compromised personal computers (a 'botnet') and rents them out to the spammers, phisher[s], and other crooks."[9] Because cybercrime has become increasingly professionalized, it has started to look more like conventional crime that has been explored at length in the economics of crime literature.[10]

Beyond payment processors and criminals themselves, another area of this literature focuses on internet infrastructure and its relationship to cybercrime. In *The Turn to Infrastructure in Internet Governance*, the

4. Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SECURITY L. & POL'Y 595 (2016).

5. *Id*. at 611–12.

6. *Id*. at 612.

7. *See generally* Tyler Moore, Richard Clayton & Ross Anderson, *The Economics of Online Crime*, 23 J. ECON. PERSP. 3 (2009).

8. *Id.* at 4.

9. *Id.* at 5.

10. *Id*. at 18.

authors look at the fundamental building blocks of the Internet as sources for governance and, consequently, security.[11] For instance, authors discuss the role of the Domain Name System (DNS) and the Internet Corporation for Names and Numbers (ICANN) as the backbones of the Internet.[12] This is important for cybersecurity because of the U.S. government's ability to directly seize domain names and take control of infringing websites, as discussed, in more detail. Essentially, the authors point out that even though the Internet was designed to usher in diffused and ground–up governance, in actuality, governance structures can reduce access to certain resources needed by cybercriminals.[13]

Similarly, in *Holding Internet Service Providers Accountable*, Douglas Lichtman and Eric Posner argue that Internet Service Providers (ISPs) can be essential nodes in cybercrime networks, and should be held to higher legal standards.[14] They argue that the move toward granting immunity to ISPs is ill–advised because it underestimates ISPs' ability to deter cybercrime, and gives them license to allow dangerous behavior.[15] This argument is in line with standard law and economics theory, predicting that always assigning liability to one party (in this case, victims) will cause the other party (in this case, ISPs) to take inefficient levels of precaution.[16] Lichtman and Posner map the theory of indirect liability onto the actions taken by ISPs and conclude that ISPs should share some responsibility for cybercrime.[17]

---

11. THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE (Francesca Musiani, Derrick L. Cogburn, Laura DeNardis & Nanette S. Levinson eds., 2016); *see also* Annemarie Bridy, *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation*, 74 WASH. & LEE L. REV. 1345 (2017).

12. Musiani, Cogburn, DeNardis & Levinson, *supra* note 11, at 9–10.

13. *Id.* at 11–12; JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

14. Doug Lichtman & Eric C. Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 221–58 (Mark F. Grady & Francesco Parisi eds., 2006).

15. *Id.* at 229–30.

16. ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 199–227 (6th ed. 2016).

17. Lichtman & Posner, *supra* note 14, at 222.

> ISPs should to some degree be held accountable when their subscribers originate malicious Internet code, and ISPs should also to some degree be held accountable when their subscribers propagate malicious code by, for example, forwarding a virus over e-mail or adopting lax security precautions that in turn allow a computer to be co-opted by a malevolent user.

Moving from theory to policy, *Operation Seizing Our Sites* raises criticisms of an overbroad intermediary–centered approach.[18] In the article, Karen Kopel discusses federal programs that aim to take down copyright and trademark infringing websites.[19] In particular, she critiques "Operation In Our Sites," a major government initiative for enforcing stricter IP protections.[20] The program's main mechanism allows the Department of Justice and Immigrations and Customs Enforcement (ICE) to seize domain names by ordering intermediaries to reassign them, and make these resources inaccessible to users who try to access a website through its alphanumeric name.[21] She argues that the process largely circumvents normal procedural safeguards, and grants the government wide discretion in pursuing potential infringers.[22] She also notes the risks associated with the approach, namely that the government has taken legitimate websites offline and offered them few due process protections to appeal the decision.[23] In practice, hardly any websites are able to recover their domains after a government seizure.[24]

The next Part turns to the business constraints that financially–motivated cybercriminals face, and examines those actors' various activities, including their dependence on intermediaries. It then summarizes the legal processes used in situations where enforcers—both public and private—attempt to deter financially–motivated cybercrime by interfering with intermediaries.

III. BUSINESS CONSTRAINTS, RELEVANT ACTORS, AND ACTIVITIES

Financially–motivated cybercriminals face many of the same business constraints and challenges that legitimate enterprises do. A paradigmatic example comes from an illegal goods business called Silk Road, which provided a marketplace for drugs, fake identification documents, and

18. Karen Kopel, *Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice*, 28 BERKELEY TECH. L.J. 859 (2013); *see also* Annemarie Bridy, *Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy*, 46 ARIZ. ST. L.J. 683 (2014).
19. Kopel, *supra* note 18 at 862–85.
20. *Id*. at 885–99.
21. *Id*. at 862–71.
22. *Id*. at 885–88.
23. *Id*. at 894.
24. *Id*. at 860.

materials for credit card fraud.[25] Another comes from the infringing goods space, where sellers, often using quickly seized ephemeral domains, market knock–off designer bags and other cheap–to–produce but high–priced items. In the illegal or infringing goods businesses, a successful enterprise needs a prominent web presence, similar to the mainstream brands. Businesses gain such prominence by having easy–to–recognize domain names and search–optimized sites. The website has to be reasonably well–designed and available to users. One also needs to be able to collect payments from users and to deliver the product to the consumer. Even illicit businesses, such as counterfeit pharmacies, care about reputation because they earn up to thirty–seven percent of their gross revenue from repeat purchases.[26] Thus, customer reviews are important.[27] Turning to botnets, operators face business–like costs too. Cybercriminals have specialization and expertise, as do many other actors in the broader economy, creating a complex market for services.[28] Cybercriminals in these markets must advertise their services, deliver them reliably, collect payment, and (in the case of botnets) maintain a collection of compromised computers. In this last function—botnet maintenance—bot herders, who conscript vulnerable machines into botnets, are in constant conflict with both nation states and sophisticated technology companies. To turn a profit, like ordinary businesses, illegal and infringing good sellers must make many sales.

In both the illegal goods and infringing goods contexts, each critical function to monetizing the crime relies on third party intermediaries. Sellers and marketplaces need domain names, hosting services, access to payment systems, banking services, access to postal or shipping networks, and so on. Many of these intermediaries are probably unaware of misconduct.[29] For various practical reasons, the nature of the web causes

25. Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, *in* PROCEEDINGS OF THE 22ND INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 213, 213–24 (2013).

26. Damon McCoy et al., *PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*, *in* PROCEEDINGS OF THE 21ST USENIX CONFERENCE ON SECURITY SYMPOSIUM 1, 7 (2012), http://cseweb.ucsd.edu/~voelker/pubs/pharmaleaks-usesec12.pdf.

27. BRIAN KREBS, SPAM NATION: THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR 81 (2014).

28. Alvaro A. Cárdenas, Svetlana Radosavac, Jens Grossklags, John Chuang & Chris Hoofnagle, *An Economic Map of Cybercrime,* 2009 TPRC 2–9.

29. Sumayah Alrwais et al., *Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks*, *in* 2017 IEEE

businesses to concentrate their services, making entire enterprises dependent on single intermediaries in some contexts. For instance, Levchenko and collaborators found that just three banks processed transactions for ninety–five percent of the goods advertised by spam in their study.[30] In another study, author Hoofnagle showed that among the most prominent online pharmacies, many shared the same shopping cart and same telephone services for sales.[31] It also appears that the rewards from such activities inure to a small number of actors. For instance, McCoy and colleagues performed an in-depth study of the customers and affiliates associated with three online pharmacy networks.[32] The group observed that affiliate marketers are major purveyors of web spam to promote online pharmacies and that a small number of advertisers in the affiliate network captured the most revenue.[33] In particular, the largest earner of commissions was a company that specialized in web spam, and it made $4.6 million.[34] McCoy and colleagues also found that twenty to forty percent of sales from email spam arise from users who actively open their spam folder and click on links to pharmacy sites.[35]

At the root of this discussion are actors who are perpetrating a wide variety of cybercrimes. These crimes are as diverse as illegally distributing copyrighted content, hacking, and engaging in the trade of illicit goods and services (i.e. drugs, sex trade, human trafficking, etc.). These criminals are exceptionally difficult to pin down because they operate with complex social networks that often span international borders.

SYMPOSIUM ON SECURITY AND PRIVACY 805, 805–06 (2017). "Bulletproof" hosting providers promise to keep users' accounts online even in the face of complaints and legal processes, but users must pay a premium for such guarantees. *Id.* at 805; Krebs, *supra* note 27 at 15.

30. Kirill Levchenko et al., *Click Trajectories: End-to-End Analysis of the Spam Value Chain*, *in* 2011 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 431, 443 (2011).

31. Chris Jay Hoofnagle et al., *Online Pharmacies and Technology Crime*, *in* THE ROUTLEDGE HANDBOOK OF TECHNOLOGY, CRIME AND JUSTICE 146, 155 (M. R. McGuire & Thomas J. Holt eds., 2017).

32. McCoy et al., *supra* note 26.

33. *Id*. at 10–11.

34. *Id*. at 12.

35. Neha Chachra, Damon McCoy, Stefan Savage & Geoffrey M. Voelker, *Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting*, *in* 2014 PROCEEDINGS OF THE WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 1, 5–6 (2014).

The next Sections turn to some of the key actors that depend on or attempt to interfere with intermediaries: botnets, sellers of counterfeit goods, and intellectual property owners.

A. BOTNETS

Botnets are networks of infected computers (the "bots") that are used to conduct illegal operations. In particular, botnets can be used to forward communications (i.e. spam emails, viruses, etc.) to other computers and grow the network, and to execute Distributed Denial of Service (DDoS) attacks that can disrupt all internet use. DDoS attacks were a principal tactic in the first nation–state cyberattacks, thus making botnet mitigation a concern for both businesses and nations.[36]

As targets of legal interventions, botnets are tricky to pin down because of their international and self–propagating nature. Individual bots could be in the homes of consumers all over the world, and could be in the form of the computers and software embedded in internet–connected cameras and even routers.[37] Bots take their direction from remote command and control servers that are generally operated by bot herders. Skilled botnet herders mask these systems, and even distribute control to new domains on predefined schedules. Presumably, the botnet herder knows what new domains will be selected and can compromise them in time to issue new instructions to the bots.[38]

The handoff of the command and control infrastructure offers an opportunity to disrupt botnets—in effect by rustling them from the herder. Technically and legally sophisticated actors such as Microsoft Corporation can use legal processes to seize the domains that the botnet will next connect with. Once seized, a company can issue instructions to the bots to update their software and stop new attacks. For example, a "sinkhole" tactic routes the associated domain names to a new DNS server, which then assigns non–routable addresses to the domains. Basically, this prevents anyone from actually accessing the website where the individual bots receive their instructions, rendering the botnet impotent.[39]

---

36. Steve Mansfield-Devine, *The Growth and Evolution of DDoS*, 10 NETWORK SECURITY 13, 13–14 (2015).

37. Elisa Bertino & Nayeem Islam, *Botnets and Internet of Things Security*, 50 COMPUTER 76, 78 (2017).

38. For a fascinating discussion of these dynamics, see generally MARK BOWDEN, WORM: THE FIRST DIGITAL WORLD WAR (2011).

39. Evan Cooke, Jahanian Farnam, & Danny McPherson, *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets*, *in* PROCEEDINGS OF THE 2005 STEPS

B. ILLEGAL AND INFRINGING GOODS SELLERS

People intent on selling illegal and infringing goods use their own websites and online marketplaces to do business and point buyers to other internet resources where infringing content may reside. Similarly, they may use social media and other pages to boost infringing services' prominence in search engines.[40]

These actors pose a challenge for law enforcement because it is difficult to discern legal operations from illegal ones. For example, it is difficult to tell whether a handbag sold on eBay is stolen, counterfeited, or simply from a legitimate owner trying to resell an expensive fashion item. In other cases, sellers set up networks of websites that are obviously in the business of knockoffs.

Domain Name Server (DNS) seizure is a common tool leveraged against these easier–to–identify sellers. Because the sellers are typically outside the United States, they are difficult to physically track down, and therefore enforcers have an easier time directly seizing the infringing web domain and other services. The next Section details the prototypical procedure. The basic notion is that the enforcer can take over a domain and prevent anyone from accessing it, therefore shutting down the illegal operations that were being carried out.

C. INTERMEDIARIES AND INTELLECTUAL PROPERTY OWNERS

This Article focuses on intermediaries' capacity to deter and combat cybercrime, and therefore highlights key players, such as technology companies that provide products and act as online platforms, and IP owners that take actions against infringers. These actors are important because when they invest in cybersecurity, they can produce positive externalities for end users and smaller firms.[41] That being said, there are key distinctions between companies involved with combating botnet activity and companies involved with IP enforcement. The former set of actors is intertwined with the governance and security of Internet

TO REDUCING UNWANTED TRAFFIC ON THE INTERNET ON STEPS TO REDUCING UNWANTED TRAFFIC ON THE INTERNET (SRUTI) WORKSHOP 39, 41–42 (2005) ("A bot must communicate with a controller to receive commands or send back information."), https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke.pdf.

40. McCoy et al., *supra* note 26.

41. Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70, 85 (2011); Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 259–63 (Mark F. Grady & Francesco Parisi eds., 2006).

infrastructure, and therefore regularly cooperates with public and private institutions to maintain a secure Internet.[42] The latter set is mainly concerned with preventing the sales of counterfeit, physical goods over online platforms. But in some cases, the two interests mix—as detailed below, botnets are sometimes used to sell counterfeit pharmaceuticals. Although Internet security and IP enforcement are distinct policy areas, they are discussed in tandem because courts employ similar toolkits in approaching both issues.

On the botnet issue, this Article emphasizes Microsoft's role in cybercrime deterrence because of the company's dominance in operating systems and its centrality in cybersecurity. Microsoft's signature product is its Windows operating system, and protecting the integrity of that product is a major goal for the company. Over the course of several years, Microsoft's reputation suffered as various viruses infected machines running Windows, and for some time, almost by definition a botnet was comprised of Windows machines.[43] In 2002, Microsoft announced a major security rethink. It aggressively invested in cybersecurity infrastructure and participated in legal proceedings aimed at taking down the most expansive botnets, thus rehabilitating its product's reputation.[44] Microsoft has gone so far as to use this mechanism—a kind of privately–waged lawfare—against the "Fancy Bear" hacking group suspected to have aided President Trump in his contest against Hillary Clinton.[45] Microsoft's litigation activity is an illuminating example of private activity that leads to more public cybersecurity, because Microsoft's actions arguably had spillover effects for consumers, businesses running Windows machines, and virtually anyone who was impacted by these botnets.

In terms of IP owners, companies that specialize in goods such as fashion products, rather than music and DVD piracy, are more relevant when discussing intermediary–driven approaches to cybercrime.

42. Professor Kristen Eichensehr explains that botnet takedowns are one form of an institutionalized public-private cybersecurity system, where cooperation between dominant technology companies and the government have resulted in remedies for severe security problems. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–72 (2017).

43. *Gates Finally Discovers Security*, WIRED (Jan. 17, 2002, 10:50 AM), www.wired.com/2002/01/gates-finally-discovers-security/.

44. *Id.*

45. Kevin Poulsen, *Putin's Hackers Now Under Attack—From Microsoft*, DAILY BEAST (July 20, 2017, 10:05 PM), https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network; Complaint, Microsoft Corp. v. Does, 1:16-CV-993 (E.D. Va. Aug. 3, 2016), 2016 WL 4203923.

Generally, fashion products can either be found in brick–and–mortar stores or through online retailers, and are susceptible to being undercut by knockoffs. This is particularly true for fashion products that trade on exclusive, European labels but are actually made in China rather than Italian or French workshops. The exclusive branding of these products drives high prices, but counterfeits often exhibit identical or good enough indicia of quality. Throughout this Article, companies such as Tiffany, Kate Spade, Gucci, and the like provide examples of enforcers that go after infringers. These retailers face challenges in addressing counterfeit sales, which occur in American markets, such as Amazon and eBay, and non–American markets, such as China's Taobao online marketplace. The ease of creating and distributing counterfeit goods in these domestic and foreign marketplaces invites IP infringement.[46] Furthermore, jurisdictional issues leave American courts with few options to directly deter this sort of activity.

As such, IP owners have developed a toolkit for dealing with counterfeit goods that simply circumvents the CDA 230 regime and its immunities. Enforcers bring lawsuits using Rule 65 of the FRCP to quickly obtain equitable relief. Enforcers also join professional alliances and organizations, cooperate with payment intermediaries,[47] and work directly with online marketplaces to remove infringing products. Because their products are so easily counterfeited, these companies have a strong incentive to invest in lawsuits as well as technological infrastructure that detects and prevents this activity. In turn, consumers presumably benefit from not being duped through online marketplaces. However, for many consumers, cheap knock–offs or higher quality "factory counterfeits" (those created by employees of the authorized factory during a secret, "fourth shift") might be a perfect substitute for the real thing.[48]

46. For instance, companies join organizations like the International Anti-Counterfeiting Coalition (IACC) in response to widespread counterfeiting. *See History & Mission*, INT'L ANTICOUNTERFEITING COALITION, https://www.iacc.org/about/history-mission (last visited Feb. 2, 2018).

47. Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1548–54 (2015).

48. MM Houck, *Counterfeit Goods*, *in* MATERIALS ANALYSIS IN FORENSIC SCIENCE 449, 449 (Max M. Houck ed., 2016).

IV. JUDICIAL INTERVENTIONS

A. RULE 65 INTERVENTIONS

Whether enforcers are attempting to police intellectual property rights or fight botnets, they rely on obtaining equitable relief through Rule 65. For all practical purposes, as soon as an enforcer obtains a Temporary Restraining Order (TRO), it has legal authority to order intermediaries to deny services to identified suspects and their internet resources. This deterrence by denial approach is intended to block the defendant from enjoying the gains of their alleged cybercrime.

Figure 1: Outline of Legal Steps in Rule 65 Interventions

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Motion for a Temporary Restraining Order	Plaintiff(s) files a motion (often sealed) in District Court requesting a Temporary Restraining Order against one or more Defendants. In the motion, the Plaintiff lists the trademarks that were infringed upon, the websites involved in the alleged activity, and the requested relief.	At this stage, the Plaintiff demonstrates harm, reasons why injunctive relief is necessary, and lists the domain names they would like to seize, along with exhibits with screenshots of offending sites. The TRO is sought without notice to the defendant.	Preparation for this action presumably takes some time because of the need to document infringements and domain owners.

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Court issues Temporary Restraining Order	Court issues the TRO. The TRO typically includes a Temporary Injunction, a Temporary Transfer of the Defendant Domain Names, and a Temporary Asset Restraint, among others. At this point, the Plaintiff has achieved the most important legal intervention to deny the benefits of cybercrime to the suspect.	Not only does the Order enjoin the Defendants from further infringement, it also extends to intermediaries that are served with it. For instance, domain name registries are required to either change the infringing pages' registrar or make them inactive and untransferable, and registrars must transfer Defendants' domain names to a registrar account of the Plaintiff's choosing.	Approximately 1 week. Under Rule 65, TROs are to be *temporary*, thus courts assign short durations to them and prioritize a follow-up hearing for preliminary injunction.
Preliminary Injunction	Court restrains Defendants from operating their allegedly infringing websites	Interventions from the TRO stage are sustained until trial. However, in practice, enforcers typically obtain a default judgment.	4 weeks

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Summons served	Clerk of the Court issues summons to Defendants. If Electronic Service is granted, e-mail and posting notice on websites serves as sufficient notice	Defendants are put on notice to respond to claims	Within days of granting of preliminary injunction
Motion to Enter Default Judgment/Final Judgment Order	Finalizes the actions undertaken with the TRO and Preliminary Injunction	At this stage, intermediaries are directed to ensure that the Plaintiff gets permanent control over the infringing domain names	Approximately 2 weeks

A TRO is an extraordinary measure because it can be obtained entirely *ex parte*. The plaintiff bears the burden to show "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition" and the plaintiff must both certify its efforts to give notice to the adverse party and explain why notice should not be required.[49] The purposes of this remedy are to preserve the status quo and prevent irreparable harm until a hearing can take place.

As explained below, once an enforcer obtains a TRO, it has a powerful remedy to use against intermediaries. The court order commands top–level

49. FED. R. CIV. P. 65.

domain name systems to replace the names of the infringing authoritative name servers with a new name controlled by the plaintiff. In some cases, IP enforcers operate the newly acquired domain and notify the public that illegal goods were once sold on it.[50] In botnet cases, enforcers can use the TRO to direct the domain into a sinkhole, which prevents anyone from accessing it.[51] Thus, the intermediary, in cooperation with the Registry, routes the names to the sinkhole, then prevents anyone from accessing the names once they have been successfully placed there.

Rule 65 interventions can occur with incredible speed, relative to ordinary litigation in the notoriously overburdened federal court system. Figure 1 gives an overview of the basic steps and timeline that parties can expect in an expeditious Rule 65 intervention. Plaintiffs enjoys a statutory privilege to get a hearing and relief quickly, often with key documents filed under seal. In the next Section, this Article gives context to these steps in a trademark infringement case.

A TRO is not necessarily a "silver bullet" and it can have some negative repercussions. When cybercriminals are attacked through their intermediaries, the intervention can cause fragmentation—a turn to smaller intermediaries, where substitutes are available. In the case of botnets, operators might move their command and control systems to DNS provided by a bulletproof host, switch to a peer–to–peer architecture, or cloak more of their systems using Tor or I2P. Also, the intervention may be overbroad, negatively affecting innocent third parties.[52]

All judicial interventions are also subject to claimant abuse—situations where one invokes the procedures in order to engage in censorship or anticompetitive behavior. Such abuse comes about both intentionally and unintentionally. Yet, Rule 65 interventions have two checks built into them that are not present in private–sector remedial schemes (discussed in Part VI below). First, Rule 65 requires that movants file a security bond to pay the costs and damages of any party "wrongfully enjoined or

50. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322, 2016 WL 8577031 (N.D. Ill. Aug. 25, 2016).

51. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF. No. 32.

52. In forthcoming work, cybersecurity experts Sasha Romanosky and Zachary K. Goldman propose a framework for defining the scope and severity of "collateral damage" in the cyber realm. Sasha Romanosky & Zachary K. Goldman, *What Is Cyber Collateral Damage? And Why Does It Matter?*, LAWFARE BLOG (Nov. 15, 2016, 1:30 PM), https://www.lawfareblog.com/what-cyber-collateral-damage-and-why-does-it-matter.

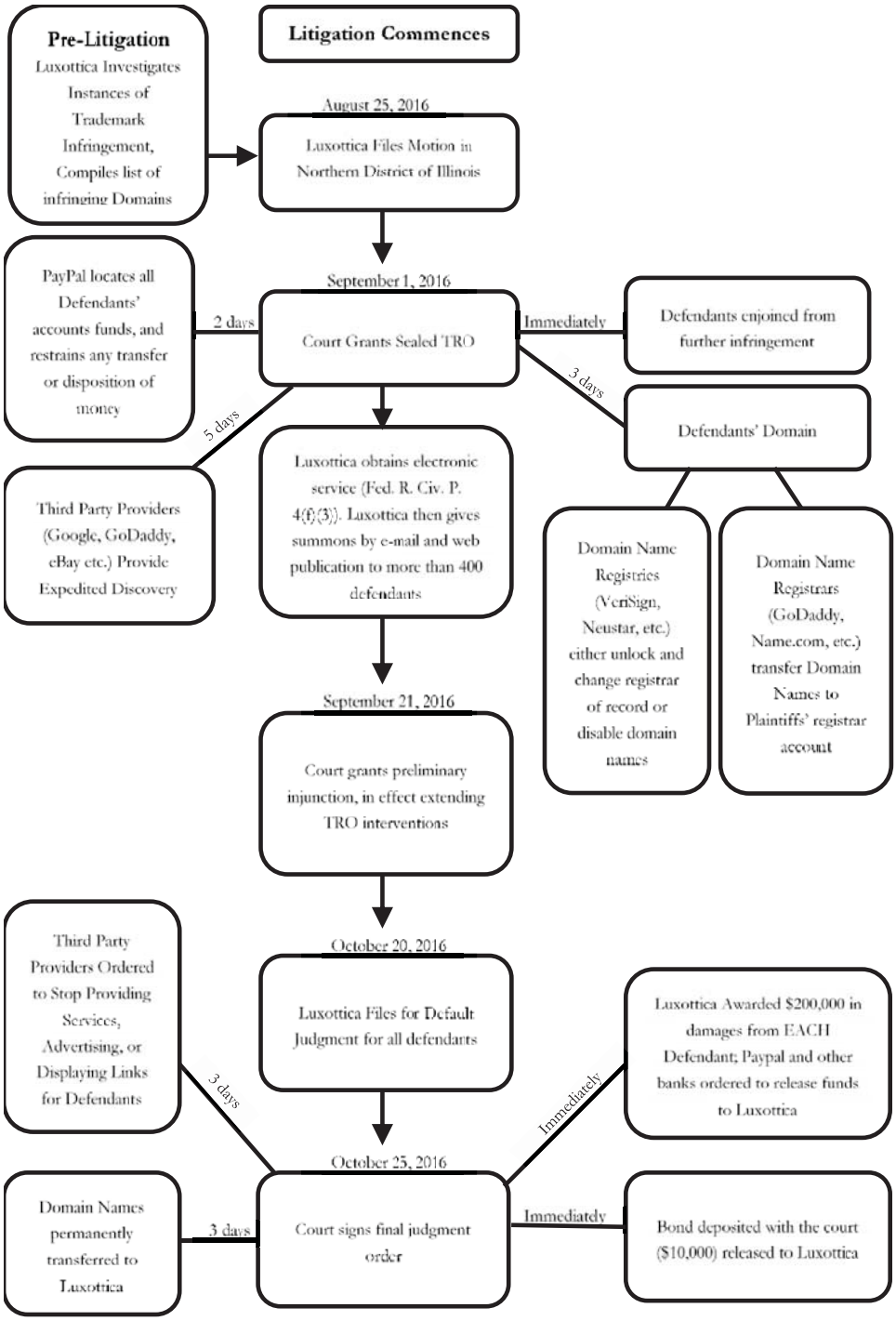
restrained."[53] Notice of this bond is provided to intermediaries served with the court's order. Second, the intervention is court supervised. Thus, lawyers, as officers of the court, will presumably avoid abusive applications of TROs and preliminary injunctions lest they attract negative judicial attention.

1. Examples from Trademark Infringement

In Figure 2, we visualize the typical case flow for a Rule 65 intervention. We chose the *Luxottica* case as it illustrates several of the most notable features of this intervention, namely the rapid pace from the filing of the lawsuit to the final order, and the massive scope given to the IP enforcer for seizing and controlling assets, coopting intermediaries into compliance, and recovering damages.

53. FED. R. CIV. P. 65(C).

Figure 2: Illustration of TRO Procedure with Luxottica Case



Luxottica, a company that owns many sought–after brands of eyewear, provides a paradigmatic example of employing Rule 65 in the IP enforcement context, one that is troubling in scale and presages a kind of automation of litigation. As outlined in Figure 2, in a single 2016 case, Luxottica sued 478 defendants that were allegedly infringing marks in operating 1,024 domains and 52 marketplaces (most of which were "stores" on eBay).[54] The case caption is so long that it occupies five pages in print, and in the electronic filing system, the defendants are listed as "The Partnerships and Unincorporated Associations Identified on Schedule A." Luxottica filed the case on August 24, 2016, and received a TRO nine days later against all the defendants.[55] Luxottica argued that relief without notice was necessary because the targeted domain owners would likely move their operations if told that an enforcement action was afoot. The lack of notice gave Luxottica another advantage—Rule 65 requires that TROs lacking notice receive a hearing as soon as possible, and so Luxottica received a preliminary injunction less than a month from the date the complaint was filed.

Figure 2 outlines the basic steps taken by Luxottica to obtain the TRO and the many varied entities bound by it. Luxottica filed a required form with the PTO to indicate it was about to enforce its trademark. It obtained a $10,000 bond filed with the court per Rule 65.[56] That amount was proposed by Luxottica and approved by the court, but presumably could have been raised or lowered to prevent abuses raised by the facts of the case. Luxottica prepared the motions for equitable relief, and in the process, filed straightforward exhibits, thousands of pages long, with screenshots of websites clearly showing Luxottica's product trademarks. But it did not engage in test purchases, which are required to identify the merchant processing account(s) used by a website to accept credit card payments. Its proof that the targeted websites were infringing was based on an in–house investigator's deductive reasoning: the websites were not

54. Amended Complaint, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Aug. 25, 2016), 2016 WL 8577031.

55. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Sept. 1, 2016), ECF No. 30 (granting temporary restraining order in a minute entry).

56. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Sept. 7, 2016), ECF No. 31 (reflecting posted bond of $10,000).

in Luxottica's approved channel list, the suspect websites had lower prices, and the websites offered shipping to the United States.[57]

Luxottica moved for and obtained approval to give adverse parties electronic notice. It gave notice via email and by posting a notice of the lawsuit on the very web properties it seized with the TRO. But none of the defendants answered the summons within twenty–one days. Thus, just two months after filing the complaint, Luxottica had a final, default judgement in the case—for $200,000 per defendant (in theory, up to $95 million).[58]

Luxottica's relief is also typical of cases in the field,[59] and this relief is broad. The Luxottica court found the defaulting defendants liable for willful trademark infringement and counterfeiting, false designation of origin, cybersquatting, and for violating a state consumer protection law. The final judgment gave Luxottica permanent transfer of the 1,024 domains, and seizure of the defendants' PayPal accounts. It also ordered broad categories of unnamed businesses not to service the defendants when they were displaying Luxottica's marks. Luxottica's order covered marketplaces (such as eBay and Alibaba), web hosts, sponsored search engine and ad–word providers, credit cards, banks, merchant account providers, third party processors, payment processing service providers, search engines, and domain name registrars. These are all the intermediaries critical to operating a web business.

2. Examples from Hacking and DDoS

TROs are also the legal tool of choice for public and private enforcement against botnets.[60] Botnets are notoriously difficult to police

57. Amended Complaint, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Aug. 25, 2016), 2016 WL 8577031.

58. *Id.*

59. We found no cases with the number of defendants in Luxottica, but others follow a similar procedure and have even shorter times to relief. For instance, in one case, a plaintiff received a TRO in one day. *See* Kate Spade, LLC v. Zhou, No. 1:14-cv-05665 (S.D.N.Y. Aug 28, 2014), ECF 9 (granting TRO in a minute order). We cannot assess the frequency of these suits but they appear to be quite common. A search in Bloomberg Law's Dockets search for civil suits where Chanel was a plaintiff and the keywords "trademark infringement" and "domain" were present returned 163 results. The cases date back to 2001 and were initiated in federal courts all over the country. Twenty–six of the cases were "open" as of May 3, 2017.

60. Eichensehr, *supra* note 42, at 470–72. Not covered here are the extraordinary nonlegal efforts private–sector technology companies take to neutralize botnets. One well–documented example comes from the campaign to fight Conficker. *See* BOWDEN, *supra* note 38, at 94–96.

with traditional deterrence by punishment because botnet herders are likely to operate outside the United States.[61] Although botnets are a different security concern, the TRO procedure is remarkably similar to the IP context illustrated earlier. The landscape includes public and private sector collaboration, and the use of civil and criminal mechanisms to obtain information and to seize assets. The basic sequence of events is that either the U.S. government or a sophisticated technology company such as Microsoft files for a TRO in District Court, the TRO is granted under seal, the command–and–control servers are either physically or remotely seized, and finally Microsoft issues a software update that commands infected bots to disengage from the network and cease malicious behavior. The following Sections highlight the use of TROs in the Coreflood, Rustock, and Kelihos cases to illustrate the efficacy and issues to consider.

a) The Coreflood Botnet

Coreflood was a Russian–based botnet that infected computers across the public sector, as well as other critical systems belonging to hospitals, businesses, etc. At its peak, it infected over two million machines, and it could repurpose these computers for several different tasks—to attack other computers with denial–of–service attacks, to provide an anonymous platform for hackers for multi-stage attacks, and to capture user keystrokes, thereby enabling the botnet controllers to discover credit card numbers and bank login information.[62] The privacy and security implications of Coreflood and other botnets are profound, making those infected vulnerable to many different kinds of wrongs.

The government averred that a single Coreflood command server "held approximately 190 gigabytes (GB) of data, recorded from 413,710 infected computers while unsuspecting computer users were browsing the Internet."[63] The government claimed that Coreflood was used to steal six–figure sums from a number of small businesses, even ones that had used two–factor authentication to carefully protect banking accounts.[64]

61. In 2009, the Federal Trade Commission, using its powers to obtain injunctions for unfair and deceptive trade practices, took down 3fn, which was regarded as among the last US-based "bulletproof" hosts. Fed. Trade Comm'n v. Pricewert LLC, No. C-09-2407 RMW, 2010 WL 2105614, at *1 (N.D. Cal. Apr. 8, 2010).

62. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF No. 32.

63. *Id.* at 32

64. *Id.*

In a civil complaint, the government obtained a TRO from a district court, along with several search warrants in different districts. The TRO sought by the Justice Department authorized the Internet Systems Consortium (ISC), a nonprofit, to swap out privately owned command–and–control servers and turn them over to the government.[65] Once this happened, Microsoft released a patch through its Malicious Software Removal Tool, which instructed machines infected with Coreflood to remove the program.[66]

In requesting the TRO in the civil case, the government argued that obtaining a search warrant was impracticable, explaining that botnet situations justified use of the special needs exception to the general preference that the government obtain a warrant for a search or seizure. The government assured the court that it would not collect any protected information or communications from the computers infected with Coreflood. The court granted the TRO but prohibited the agencies from storing, reviewing, or using information unrelated to the data needed to battle the botnet.[67] Interestingly, although the government obtained the TRO through a civil procedure, the Department of Justice also announced that it would pursue a criminal prosecution.[68] The line between civil and criminal procedure blurs as TROs are used as tools to combat criminal activity, which is why this case reflects the basic due process concerns at play when the government, intermediaries, and nonprofits cooperate on operations that implicate constitutional and statutory interests.

b) The Rustock Botnet

Rustock was a self–propagating botnet that was responsible for a large portion of spam emails worldwide. This botnet used a Trojan virus to infect machines that received spam communications, and was difficult to detect. Several previous attempts to bring down Rustock failed due to its ability to quickly restore its capacity after any partial attack.[69]

---

65. *Id.*

66. Press Release, U.S. Dep't of Justice, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

67. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF No. 51.

68. Press Release*, supra* note 66

69. MICROSOFT CORP., BATTLING THE RUSTOCK BOTNET: SECURITY INTELLIGENCE REPORT 7 (2011), https://lammgl.files.wordpress.com/2011/03/battling-the-rustock-threat_english.pdf ("Rustock checks for the presence of kernel debuggers . . . and . . . also tries

Microsoft, in cooperation with Pfizer (which suffered potential reputational and financial harm because Rustock sent spam emails for knock–off Viagra), the U.S. government, and the University of Washington, finally disabled the botnet through Operation b107.[70] Microsoft brought suit in the Western District of Washington, and obtained a TRO that authorized the implementation of the operation under seal.[71] Accompanied by U.S. Marshals, Microsoft seized equipment used in Rustock, performed forensic analysis on it, and concluded that the evidence pointed to a Russian–based operation.[72]

Microsoft gained standing to pursue this action under a combination of the CAN-SPAM Act and the Lanham Trademark Act, in part because Microsoft's trademarks are used to propagate malware.[73] Pfizer's involvement was key for invoking the Lanham Act, and for triggering a sense of urgency—the drugs sold via Rustock were passed off as real, but in test purchases, some proved to differ from those sourced from Pfizer's supply chain.[74] Moreover, Microsoft ensured that the court order was under seal until the operation was complete, so as to avoid tipping off the botnet herders in advance. As in the Coreflood proceedings, the plaintiffs justified their actions by noting that Microsoft would respect due process concerns and that this intervention was the narrowest possible.[75] It also filed a $170,000 bond. Microsoft updated the court weeks after it seized IP

to maintain code integrity by constantly checking itself for modifications using CRC32 checksums, and by scanning itself for software breakpoints (0xCC).").

70. *Id.* at 3.

71. Complaint, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Mar. 1, 2011), 2011 WL 921612.

72. Peter Bright, *How Operation b107 Decapitated the Rustock Botnet*, ARS TECHNICA (Mar. 22, 2011), https://arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/.

73. Microsoft Corporation's Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause Re Preliminary Injunction, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Feb. 9, 2011), 2011 WL 1193746.

74. *Id.* ("Counterfeiters deceive patients into believing that the products they offer are safe and effective medicines from trusted pharmaceutical companies such as Pfizer, upon whose integrity they have relied to receive medicines that permit them to live happier and healthier lives.").

75. Bright, *supra* note 72.

addresses and domain names to report that it had received no requests to reinstate these resources.[76]

c) The Kelihos Botnet

One ongoing example of government and intermediary efforts to thwart a botnet is the Kelihos case.[77] Kelihos is a botnet that functions in a similar fashion to Rustock by using spam to infect peer computers with malware.[78] In this case, the program is able to conduct a range of operations including DDoS attacks and stealing cryptocurrency wallets.[79] On April 10, 2017, the Justice Department announced that it was undertaking actions to dismantle the botnet.[80] Unlike in the Coreflood case however, the government invoked the 2016 Amendments to Rule 41 of the Federal Rules of Criminal Procedure (FRCrP), instead of Rule 65 of the FRCP.[81] Under the new language, the federal government is able to seek a warrant to search a computer that is hidden through the use of technology (such as anonymizing software like Tor or I2P), and sue in just one jurisdiction in cases where devices in five or more districts are implicated (as opposed to all districts).[82] This is an important step because previously the government struggled to remotely search anonymized criminals, and faced high litigation costs arising from the requirement to sue in multiple districts.[83]

As indicated earlier, the government generally used a combination of TROs from civil procedure and criminal investigations to cooperate with intermediaries in botnet cases. In this case, the government relied solely on criminal procedure. However, despite using the FRCrP instead of the FRCP, the technical procedure used looks to be the same as previous

76. Microsoft Corporation's Status Report Re Preliminary Injunction at 2, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Apr. 4, 2011), ECF No. 43.

77. Press Release, U.S. Dep't. of Justice, Justice Department Announces Actions to Dismantle Kelihos Botnet (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

78. *Kelihos*, N.J. CYBERSECURITY & COMMC'S. INTEGRATION CELL (Dec. 28, 2016), https://www.cyber.nj.gov/threat-profiles/botnet-variants/kelihos.

79. *Id*.

80. Press Release, *supra* note 77.

81. FED. R. CRIM. P. 41(B)(6)(B).

82. *Id*.; FED. R. CIV. P. 65.

83. Press Release, *supra* note 77; Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T JUST. (June 20, 2016), www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

botnet cases. The government got authorization to take control of command–and–control servers, identified IP addresses, and then turned them over to an intermediary to sever connections between the botnet herder and the servers. As in the previous cases, Microsoft used its software updates to instruct infected computers to delete the virus that propagated the botnet. This case may signal a legal framework that courts will use going forward, but it substantially represents the same combination of the government cooperating with an intermediary to seize servers and dismantle them via a sealed court order.

3. Criticisms of Rule 65 Interventions

Despite the apparent efficacy of Rule 65 TRO interventions in both trademark and botnet applications, this tool is criticized for potential overbreadth. As demonstrated in *Luxottica*, federal courts, notorious for their slow processes, place these cases at the top of the docket. Because the invocation of Rule 65 expedites litigation, it is possible to get powerful, broad remedies in a matter of days or weeks. Electronic service further greases the wheels by eliminating the labor–intensive but salient event of being physically served with process. These court orders are also usually heard *ex parte*, and the restraining order is granted under seal to avoid alerting infringers and perpetrators.

In the IP context, the orders are broad in that they cover a wide variety of actors. The TRO allowed Luxottica to compel action from hundreds of defendants, domain name registrars, payment processors, search engines, online marketplaces, and advertisers. Not only did the TRO reach a massive number of actors (many of which were intermediaries), it compelled action from them within a matter of days. This breadth reflects that judicial harmony with enforcers that pursue infringers alone is inadequate, and therefore courts lean on intermediaries to undertake actions to punish and prevent unlawful behavior.

Annemarie Bridy mounts a strenuous critique of domain seizure in *Three Notice Failures in Copyright Law*.[84] Bridy argues that seizure without notice to domain owners infringes both First and Fifth amendment rights.[85] Her argument is at its strongest when enforcers seize domains with significant non–infringing purposes, such as file sharing systems. Non–infringing uses may not be apparent to courts, and enforcers may see

84. Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777 (2016).

85. *Id.* at 802–14.

these services as primarily piracy operations. Enforcers tend to target niche players, and as Bridy explains, innocent users of such systems are presumed guilty.[86]

The botnet context suffers from similar concerns, with the additional problem of creating collateral damage for innocent third parties. For instance, Microsoft requested a TRO to sink several computers that were generating dynamic IP addresses to conduct illegal activities. The TRO was directed at NO-IP.com, but inadvertently took down many sites that were using dynamic IP addresses for legitimate purposes.[87] Users, as well as organizations like the Electronic Frontier Foundation, criticized this action.[88] Again, the controversy stemmed from the sudden nature of the action because the TRO was carried out *ex parte* and under seal. Moreover, Microsoft was criticized for its outsized role in seeking and implementing the legal and technical actions necessary for the TRO. In virtually every case examined, Microsoft, in partnership with the federal government and other companies, was responsible for developing and implementing the software that disrupted botnets. Microsoft's role here is natural for the obvious reason of Microsoft's product being a dominant operating system worldwide, and indeed this is an attractive feature in terms of effectively combating large and diffuse botnets. However, this also means that Microsoft is disproportionately powerful, and can cause unintended harms by pursuing an overbroad TRO. Without any way to raise concerns before implementation, potential victims must rely on Microsoft's and a court's foresight of potential harms to innocent parties.

More generally, there is continued discussion about the extent to which preliminary injunctions may properly conscript intermediaries. Rule 65 orders can only bind certain entities, including parties, entities related to the parties (such as their servants, employees, and agents), and those in "active concert or participation" with the parties.[89] What is the status of

86. *Id.* at 806–07 (discussing the case of Megaupload users).

87. Brief in Support of Application of Microsoft Corporation for an Emergency Temporary Restraining Order and Order to Show Cause Regarding Preliminary Injunction, Microsoft Corp. v. Mutairi, No. 2:14-cv-00987 (D. Nev. Jun 19, 2014); *see also* Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237 (2014).

88. *See generally* Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163 (2014); Lerner, *supra* note 87, at 250–60; Robert McMillan, *How Microsoft Appointed Itself Sheriff of the Internet*, WIRED (Oct.16, 2014), https://www.wired.com/2014/10/microsoft-pinkerton/.

89. FED. R. CIV. P. 65(D)(2)(C).

payment providers or domain registrars in these cases? Courts do not specify their precise role in orders. For example, in one case, CloudFlare, which provides reverse–proxy service, complied with a preliminary injunction that required it to terminate user accounts that used specific domain names.[90] CloudFlare, however, opposed obligations to filter on a continuing basis for customers using the domain name "grooveshark."[91] In this effort, CloudFlare found an ally in the Electronic Frontier Foundation (EFF), which argued that this preliminary injunction required CloudFlare to act as "enforcers" of the plaintiff's trademark and could potentially affect customers who were not using the domain name in an infringing matter.[92]

This situation contains many parallels to other cases examined here. As noted, the final judgment order in the *Luxottica* case compelled search engines and online marketplaces to stop serving the defendants, implying an obligation to continue monitoring their systems for infringing behavior.[93] Like with the CloudFlare example, this puts intermediaries in the position of continually enforcing another party's IP rights. While this arrangement is pragmatic, since the fact that infringers will not realistically comply with court orders means that focusing on intermediaries is more effective, intermediaries may challenge overreliance on their capacity and willingness to pursue infringers on behalf of IP owners.

Internet commerce has a different logic than offline business operations. Firms supplying infringing content probably never meet any of the third–party service providers that make their operation possible. Some of the intermediary services may be offered free, or at a very small cost. Additionally, the various intermediaries probably are neither aware of nor wish to be involved with infringement. For these and other reasons, Bridy recommends that enforcers should prove that "nonparty service providers . . . either expressly or tacitly agreed to act in furtherance of a common

90. Arista Records, LLC v. Tkach, 122 F. Supp. 3d 32, 34 (S.D.N.Y. 2015) .

91. *Id*. at 35.

92. Mitch Stoltz, *Victory for CloudFlare Against SOPA-like Court Order: Internet Service Doesn't Have to Police Music Labels' Trademark*, ELECTRONIC FRONTIER FOUND. (July 15, 2015), https://www.eff.org/deeplinks/2015/07/victory-cloudflare-against-sopa-court-order-internet-service-doesnt-have-police.

93. Luxottica Grp. S.p.A. v. Zhou Zhi Wei, No. 17-CV-05691, 2017 WL 6994587, at *3 (N.D. Ill. Sept. 12, 2017)

plan of infringement."[94] Such a burden of proof would render Rule 65 interventions toothless.

V. GOVERNMENT–LED INTERVENTIONS

This Part details two ways in which the government uses the courts and administrative powers to police intellectual property and computer hacking crimes. The first section covers seizures of websites using the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act.

A. PRO-IP ACT DOMAIN SEIZURES

Government and intellectual property owners have used domain name seizures to interdict websites that host, or even simply link to, illegal content. Domain names identify things connected to the Internet, and link them to IP addresses. Domain names are considered a core component of Internet governance, and are a fundamental part of establishing property rights on the Internet.

Special legal authority for domain name seizure comes from the PRO-IP Act, which gave birth to interagency efforts to interdict online IP violations.[95] Basically, the federal government seizes a website accused of engaging in illegal activity, making it impossible to reach it by searching its alphanumeric name. It is still generally possible to reach it by directly entering its numeric IP address. Most consumers probably will never figure this out, so the blocked sites are, in effect, boarded up. Once seized, the government can continue its investigation of the website's alleged infringement, before pursuing further legal action.[96]

DNS seizures are useful because they are effective at targeting internet resources complicit in illegal behavior. For these one–off instances, DNS seizures are easy to undertake, and only require cooperation between the government and domain name registrars. Moreover, they can be used to pursue websites whose owners may be difficult to track down or may live outside the United States, without requiring a lengthy legal proceeding.

---

94. Bridy, *supra* note 84, at 831.

95. Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. 110-403, 122 Stat. 4256.

96. Kopel, *supra* note 18, 863–67; Dave Piscitello, *Guidance for Preparing Domain Name Orders, Seizures & Takedowns*, ICANN (Mar. 7, 2012), www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.

Yet, DNS seizures are controversial because of the potential overbreadth and potential lack of regard for process. They can be overbroad in that the government can identify targets for seizure that are not directly related to illegal activity. Relatedly, it can bring down the websites without the defendants showing up in court. Without strong procedural protections, the government can seize domain names that are not actually associated with illegal activity.[97]

For instance, the Rojadirecta and Dajaz1 cases reflected this flaw in PRO-IP Act DNS seizures. Rojadirecta was a website that linked to other websites illegally streaming sportscasts, and Dajaz1 was a website that offered hip-hop commentary and reviews, as well as song samples. Rojadirecta's legality was upheld in Spanish courts two years prior to the U.S. seizure.[98] In both cases, the government seized the domain names, but the owners of the websites successfully challenged the orders and regained control of the web properties.[99] In the Dajaz1 case, the U.S. government never came up with the adequate evidence to justify a permanent injunction, and thus handed the domain back to its original owner.[100] In both cases, the domain owners were deprived of the properties for over a year. For even the most successful web businesses, a short service outage can be ruinous.[101]

DNS seizures are criticized for the same reason that civil forfeiture has become widely scrutinized: they take control of property whose owners lack the means to challenge the government's allegations. As was the case with TROs, the Rojadirecta and Dajaz1 cases were heard *ex parte* and were seized without notifying the owners beforehand. The owners of these domains successfully challenged their seizure, but the vast majority of the more than 1,000 domains seized never challenge the government.[102] The breadth and muscularity of intellectual property rights obviously raises the specter of these mechanisms being used for censorship.

---

97. *See* Bridy, *supra* note 11, at 1378 (showing illustrative problems in the areas of copyright and child pornography enforcement).

98. Jennifer Martinez, *US Government Dismisses Piracy Case Against Rojadirecta Site*, HILL (Aug. 29, 2012, 9:26 PM), http://thehill.com/policy/technology/246529-us-government-dismisses-case-against-rojadirecta.

99. Kopel, *supra* note 18, at 880–81.

100. David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED (May 3, 2012, 5:00 PM), https://www.wired.com/2012/05/weak-evidence-seizure/.

101. Puerto 80 Projects, S.L.U. v. United States, No. 11-3983 (S.D.N.Y June 20, 2011).

102. Kopel, *supra* note 18, at 860.

B. GOVERNMENT INTERVENTION IN FINANCIAL SERVICES INTERMEDIARIES

Aside from court–authorized actions, the U.S. government also uses administrative power to investigate and disrupt cybercrime. Multiple agencies claim jurisdiction over cybercrime because it implicates financial security, protection of critical infrastructure, criminal statutes, and intellectual property protections. As such, both the Justice Department and the Treasury Department launched financial security programs that touch on cybercrime.

Operation Choke Point was a President Obama-era Justice Department program that focused on banks and their business clients.[103] Specifically, it targeted certain merchant categories that were recognized as being high–risk. For instance, it covered money laundering, consumer exploitation (scams, payday lenders, etc.), and online gambling. Essentially, the program aimed at uncovering information about exploitative and illegal practices by leveraging banks' access to unique insights about the merchants that banks connect to the payments system.[104] The Justice Department, focused on payment providers, targeted banks with subpoenas and investigative attention to determine whether they were aware of or were colluding in fraud perpetrated by partner payment providers.[105] This investigatory attention caused banks to sever relationships with both questionable and lawful merchants, raising the ire of the business community and triggering Congressional blowback.[106] The Trump administration ended operation Choke Point in 2017.[107]

---

103. Jessica Silver-Greenberg, *Justice Department Inquiry Takes Aim at Banks' Business With Payday Lenders*, N.Y. TIMES (Jan. 26, 2014) https://dealbook.nytimes.com/2014/01/26/justice-dept-inquiry-takes-aim-at-banks-business-with-payday-lenders/.

104. *Id.*

105. U.S. HOUSE OF REPRESENTATIVES COMM. ON OVERSIGHT & GOV'T REFORM, THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT": ILLEGALLY CHOKING OFF LEGITIMATE BUSINESSES? (2014), https://oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf.

106. *Id.*

107. Letter from Stephen F. Boyd, Assistant Att'y Gen., Dep't of Justice, to the Honorable Bob Goodlatte, Chair, Comm. on the Judiciary, U.S. House of Representatives (Aug. 16, 2017), http://alliedprogress.org/wp-content/uploads/2017/08/2017-8-16-Operation-Chokepoint-Goodlatte.pdf.

Other examples include President Obama's Executive Order (EO) 13694,[108] which was amended by EO 13757.[109] In EO 13694, the U.S. Department of Treasury was authorized to place a block on all property and property interests in the United States that are associated with cybercrime by placing individuals and entities on the specifically designated nationals and blocked persons list (SDN).[110] This intervention is similar to other Treasury holds placed in response to illegal activities,[111] and its authority stems from the International Emergency Economic Powers Act.[112] With this authority, the Treasury, in conjunction with the Justice Department can freeze bank accounts, deplete them, and generally prevent their owners from accessing them. As of this writing, the government has not placed anyone on the 13694 list.

EO 13757, adopted late in President Obama's tenure, amended the earlier order in light of Russian state–sponsored attacks on American presidential candidates Hillary Clinton and Senator Marco Rubio.[113] EO 13757 specified that activities "interfering with or undermining election processes or institutions" trigger designation on the SDN.[114] Over forty individuals and entities have been placed on the SDN under the EO 13757 process.[115]

These programs are useful in that they can target cybercriminals who are not physically located in the United States. In both cases, the government leverages the fact that financial institutions are central to cybercriminal operations. Because much cybercrime is financially

108. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 FED. REG. 18,077 (Apr. 1, 2015).

109. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 FED. REG. 1 (Dec. 28, 2016).

110. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 FED. REG. 18,077 (Apr. 1, 2015).

111. *See* Transnational Criminal Organizations Sanctions Regulations, 31 C.F.R. § 590 (2017) (using the 2016 classification of PacNet as a significant transnational criminal organization pursuant to E.O. 13581 as an example of SDN interventions against intermediaries for online crime); *see also Specifically Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF TREASURY (Feb. 2, 2018), https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx [hereinafter *Dep't of Treasury SDN*].

112. 50 U.S.C. § 1701 (2012).

113. *Dep't of Treasure SDN*, *supra* note 111.

114. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 FED. REG. 1 (Dec. 28, 2016).

115. *Id.*

motivated, identifying and dismantling perpetrators' financial assets is a key tool for deterring it.

Financial interventions are also more likely to effectively disrupt cybercriminal activity than DNS seizures. Since there are many registrars, DNS seizures may only temporarily take infringing websites offline. A study by Wang and collaborators found that domain name seizures did not significantly reduce the number of counterfeit online stores found in search engine results for luxury goods.[116]

There is evidence suggesting that DNS seizures are not a one–time intervention, and companies must bring a series of lawsuits to continue pursuing infringers, which may help explain why they do not significantly reduce the number of counterfeit stores in the long–run. Indeed, in the *Luxottica* cases, the court order also instructed PayPal to restrain payment accounts based in China and Hong Kong, indicating that simply seizing the domain names in question was not an adequate remedy.[117]

VI. PRIVATE REMEDIATION PROCEDURES

Under pressure from intellectual property owners, some market platforms have developed their own takedown policies. Large platforms allow for their users to report IP infringement, and then take actions to remove the infringing listings or transactions. These interventions do not require the explicit consent of law enforcement, and rather reflect the intermediaries' effort to mitigate the harm done by cybercriminals. The following Section details some examples of these mechanisms, and then discusses the general advantages and disadvantages of self–regulation.[118]

116. David Y. Wang, Matthew Der, Mohammad Karami, Lawrence Saul, Damon McCoy, Stefan Savage & Geoffrey M. Voelker, *Search + Seizure: The Effectiveness of Interventions on SEO Campaigns*, *in* PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT CONFERENCE 359 (2014).

117. Luxottica Grp. S.p.A. v. Zhou Zhi Wei, No. 17-CV-05691, 2017 WL 6994587, at *3 (N.D. Ill. Sept. 12, 2017).

118. The survey here includes efforts focused on large platforms that control a huge transaction space, such as eBay and the Visa payment network. However, the literature includes discussions of countless other private remediation programs. For instance, Liu et al. explore policy changes that affect domain name acquisition in the .cn ccTLD and the effects of a verification service that screened domains for illegal pharmacy activities. He (Lonnie) Liu et al., *On the Effects of Registrar-Level Intervention*, *in* PROCEEDINGS OF THE 4TH USENIX WORKSHOP ON LARGE-SCALE EXPLOITS AND EMERGENT THREATS (2011).

A. EBAY VERO PROGRAM

eBay's Verified Rights Online (VeRO) Program is geared towards helping IP owners prevent sellers from illegally marketing merchandise, unauthorized copies, and other branded materials. The process largely relies on IP owners reporting infractions to eBay, but provides participants with a few different options for large–scale and chronic infringements. This program provides a concrete example of how an online marketplace takes actions against infringers. eBay is a particularly good example because virtually all of the products it sells are supplied by users, therefore breaking the channel controls that some luxury brands use to maintain vertical price fixing and exclusivity. It is thus important to understand that brand owners may be objecting to any sale of their branded merchandise in addition to items that are infringing or counterfeit.

The procedure for VeRO is straightforward and easily accessible. Anyone (including people and companies that do not have listings on eBay) who owns a product or piece of intellectual property is eligible to participate. An interested party must sign up for a VeRO account and provide links to the infringing products. Then, the user emails "vero@ebay.com" to notify eBay that s/he would like to assert IP rights. Finally, the party submits a "Notice of Claimed Infringement (NOCI)" form.[119]

This process is geared toward individual violations, but naturally some parties may have larger needs. eBay provides for users to search for IP infringement through manual monitoring, setting up a "Watch List," or hiring a full–time monitoring agency. eBay imposes no fee for reporting infringement or for creating watch lists, but companies incur expenses in employee time or in hiring boutique monitoring services.[120]

B. VISA IP ENFORCEMENT

Visa, like MasterCard, is a payment network, an ISP–like entity for banks and merchants that exchange money in order to process consumer

119. *Notice of Claim Infringement*, EBAY http://pics.ebay.com/aw/pics/pdf/us/help/community/NOCI1.pdf (last visited Feb. 2, 2018).

120. General information about the program is available on eBay's website. *See Verified Rights Owner Program*, EBAY, http://pages.ebay.com/seller-center/listing/create-effective-listings/vero-program.html (last visited Feb. 2, 2018). A list of participating members is also available. *See VeRO Participant Profiles*, EBAY, http://pages.ebay.com/seller-center/listing/create-effective-listings/vero-program.html#m17-1-tb3 (last visited Feb. 2, 2018).

purchases. Visa thus can monitor aspects of transactions but it cannot track the specific items purchased by the consumer.[121] However, Visa can monitor suspicious merchants and link their activity across different banks.

Visa voluntarily searches for potential IP infringement in its payment systems, and attempts to enforce IP owners' rights.[122] Visa has at least two different procedures that it uses for its IP takedown activities, one of which is an online form that victims can fill out identifying a merchant who has infringed on IP. The website claims that individuals may file five claims per month, and afterward Visa investigates each claim and arbitrates.[123]

More detailed information comes from a 2011 congressional testimony by Visa on the issue of IP takedowns. Visa explained that it deals with complaints directly via emails to "Inquiries@visa.com."[124] One important note is that Visa and other credit card companies do not generally have direct relationships with individual merchants who accept their cards as payment.[125] Instead, merchants have relationships with payment companies that link them to the network. After receiving a complaint, Visa does a test transaction to identify the payment company that signed up the suspected infringing merchant.[126] Visa then instructs the payment company to investigate the merchant, and report within five business days.[127] After reviewing the report, Visa has the payment company send a "comply or terminate" notice to the suspected infringer.[128]

121. Chris Jay Hoofnagle, Jennifer M. Urban & Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (Berkeley Ctr. for Law & Tech., Research Paper 2012), https://ssrn.com/abstract=2045580.

122. *Targeting Websites Dedicated to Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 1 (2011) (statement of Denise Yee, Visa, Inc.), https://www.judiciary.senate.gov/imo/media/doc/11-2-16%20Yee%20Testimony.pdf.

123. *Report Intellectual Property Abuse*, VISA, https://usa.visa.com/Forms/report-ip-abuse-form.html (last visited Feb. 2, 2018).

124. *See* Yee, *supra* note 122, at 12.

125. *Id.* at 6.

126. *Id.* at 12–13.

127. *Id.*

128. *Id.*

C. INTERNATIONAL ANTICOUNTERFEITING COALITION (IACC)

The IACC is a nonprofit that brings together various actors concerned with international IP infringement.[129] The organization is composed of over 250 member organizations, including private businesses, law firms, security firms, and government organizations.[130] It also hosts semiannual conferences dedicated to informing members about best practices, and coordinate efforts to clamp down on IP infringement.[131]

The IACC offers a suite of services to its members, namely the "RogueBlock" and "MarketSafe" features. RogueBlock is a back–end network that connects IP owners to investigators, payment companies, the government, and related actors.[132] When infringement occurs, the IACC processes reports and distributes them to the relevant intermediaries on behalf of its members.[133]

MarketSafe is a direct partnership between the IACC and Alibaba to take down counterfeiting infringers on the online marketplace, Taobao.[134] It includes access to "expedited take–down procedures" that presumably guarantee members a quick turnaround on their reports of IP infringement on the website.[135] Essentially, the IACC provides investigative and administrative services to its members by specializing in searching for infringement, producing relevant evidence, and filing the proper documentation in IP takedown cases.[136]

D. BACKPAGE.COM: PRIVATE REMEDIATION AS A SCAFFOLD FOR CRIMINAL PROSECUTION

Backpage.com is a popular online classified ads site, similar to Craigslist. But Backpage is known for its adult escort ads, which are believed among the not–born–yesterday to be a front for organizing online

129. For an in–depth discussion, see Annemarie Bridy, *supra* note 47, at 1548–54.
130. INT'L ANTICOUNTERFEITING COALITION, supra note 46.
131. *Id.*
132. *IACC RogueBlock®*, INT'L ANTICOUNTERFEITING COAL., http://www.iacc.org/online-initiatives/rogueblock (last visited Feb. 2, 2018).
133. *Id.*
134. *IACC MarketSafe®*, INT'L ANTICOUNTERFEITING COAL., http://www.iacc.org/online-initiatives/marketsafe (last visited Feb. 2, 2018).
135. *Id.*
136. *Id.*

prostitution and child sex trafficking.[137] Experts in human trafficking believe that Backpage does not simply provide a substitute for offline child sex markets, but rather contributes to an explosive growth in reports of child sex trafficking: astonishingly, the National Center for Missing and Exploited Children claims that 73% of the child sex trafficking reports it receives involve Backpage.[138]

Years ago, law enforcement agencies pressured credit card networks to stop accepting payments initiated on Backpage.[139] By July 2015, American Express, Visa, and MasterCard all agreed to stop such payments.[140] In a December 2016 criminal complaint, the State of California charged Backpage's operators with money laundering and conspiracy for creating fake e-commerce sites to evade American Express' payment ban.[141] The state alleges that the defendants instructed escorts and pimps on how to buy "credits" on these third party sites that were actually destined for Backpage's escort business.[142]

The State charged the Backpage operators with financial crimes because an earlier attempt to prosecute them ended in failure—a state court judge held that under CDA 230, the operators we not liable for the classified ads posted by third parties.[143] The State brought the new charges just weeks after the failed prosecution.[144]

---

137. S. COMM. ON HOMELAND SEC. & GOV'T AFFAIRS, BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING 1 (2017) [hereinafter REPORT ON BACKPAGE.COM].

138. *Id.*

139. Rebecca Hersher, *Backpage Shuts Down Adult Ads in the U.S., Citing Government Pressure*, NPR (Jan. 10, 2017, 11:23 AM), https://www.npr.org/sections/thetwo-way/2017/01/10/509127110/backpage-shuts-down-adult-ads-citing-government-pressure.

140. Michelle Hackman, *Backpage Files Suit Against Cook County Sheriff Over Credit Card Service*, WALL ST. J. (July 21, 2015, 2:35 PM), https://www.wsj.com/articles/backpage-files-suit-against-cook-county-sheriff-over-credit-card-service-1437496670.

141. Criminal Complaint, People v. Ferrer, No. 16FE019224 (Cal. Super. Ct. Sept. 20, 2016), 2016 WL 6091120. American Express differs from MasterCard and Visa in that it is a "closed-loop" system, and as such, it operates as a network, processor, and merchant acquirer. This direct relationship with merchants may explain why the California Department of Justice focused on Backpage.com's alleged evasions with respect to American Express and not open-loop systems.

142. *Id.*

143. Trial Order, People v. Ferrer, No. 16FE019224 (Cal. Super. Ct. Nov. 16, 2016), 2016 WL 6905743.

144. Felony Criminal Complaint, People v. Ferrer, No. 16FE024013 (Cal. Super. Ct. Dec. 23, 2016), 2016 WL 7884408.

E. COMMENTS ON VOLUNTARY AND SELF–REGULATING PROCEDURES

Voluntary procedures avoid use of the courts, thereby avoiding costs and delays. Moreover, they allow for the victims of infringement and fraud to directly deal with the infringement. These are important advantages because they avoid the costs associated with lawsuits, and encourage victims to take advantage of these policies. Because of these features, these platforms establish credibility in their services. As seen in the Backpage.com example, voluntary procedures can also lay the groundwork for government enforcement actions.

On the other hand, the lack of transparency obscures actual practices and subtle shifts in policy. Self–regulatory procedures hide the actual penalties levied by intermediaries on various actors. They also make it possible for the intermediary to weaken its posture over time, perhaps by reducing penalties once scrutiny from enforcers eases. Self–regulatory procedures can hide awful practices that indicate the most noxious uses of the platform—for instance, Backpage.com was filtering terms that indicated child sex trafficking such as "Amber Alert."[145] Finally, a lack of transparency obscures how self–regulatory systems distribute seized proceeds from suspected cybercrime.

Another major disadvantage to these approaches is that they all rely on self–reporting from the victim. Although eBay and Visa allow for some automation in their services, they are not inherently designed to deal with large–scale fraud or theft. By default, they are designed to deal with individual complaints, which means they are probably more effective at isolated incidents involving smaller victims.

This feature makes voluntary efforts difficult to rely on when dealing with botnets, large crime networks, and systemic fraud. Although organizations like the IACC attempt to clean up marketplaces like Taobao, self–regulation on its own does not necessarily alleviate the structural problems with these platforms. Perhaps this is why some enforcers have pursued litigation or administrative enforcement actions.

VII. SUMMARY AND CONCLUSION

Cybercrime is often presented as an intractable problem because it can be committed by users under a cloak of anonymity and committed from jurisdictions without effective rule of law. Intermediaries are presented as

145. REPORT ON BACKPAGE.COM, *supra* note 137.

being broadly shielded from liability for their users' actions. This Article explains that these frames obscure the reality of deterring financially–motivated cybercrime: such cybercrime shares characteristics of ordinary businesses. Like ordinary businesses, financially–motivated cybercrime is an activity of scale, not a jackpot activity such as robbing a bank. Criminals need to optimize their processes, make sales, and critically, they rely on many different intermediaries for everything from marketing, to web hosting, to delivery of products. Reliance on intermediary service providers gives enforcers the opportunity to disrupt these networks. While CDA 230 provides intermediaries great cover for demands to take down some material, anti–botnet and IP enforcers have found some success using FRCP Rule 65 to compel intermediaries to hand over or block resources used by cybercrime networks, typically within days of filing suit.

Intermediaries are in a tussle among law enforcement, powerful brands, legitimate users, and rogue users. Enforcers have found effective technical fixes (sinkholes, delisting a website's alphanumeric name, etc.), yet there is no one simple solution that works across all classes of crime.

Narrower gateways offer more powerful interventions. For instance, a prior study by author McCoy and collaborators found that payment platforms, because of their breadth and oligopoly status, have more power over cybercriminals than interventions in the DNS.[146] There is more competition in domain name administration, and far too many top–level–domains (e.g. .com, .net, and so on) to control the entire space.[147]

Moreover, these types of interventions can cause serious collateral damage that disrupt legitimate operations or otherwise impose costs on legitimate users. Considering that these interventions require intensive cooperation among the government, nonprofits, and corporate actors, the motivations of these actors must be balanced as to not interfere with other public policy goals like fair market competition, strong privacy protections, and encouragement of innovation.

It is unlikely that enforcement approaches focused on intermediaries will cause decentralization and turns to harder–to–disrupt technologies, such as cryptocurrencies. This is because financially–motivated

146. Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker & Stefan Savage, *Priceless: The Role of Payments in Abuse-advertised Goods*, *in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 845, 845–46 (2012)

147. He Liu et al., *supra* note 118.

cybercriminals need to appeal to a mass consumer population. For these consumers, PayPal and similarly–mainstream payment mechanisms are accessible, whereas decentralized ones are difficult to use and generally go unused by ordinary consumers.[148] For instance, author McCoy and colleagues found that blocking DDoS–for–hire services from PayPal caused an almost immediate, short term reduction in availability of such services. The McCoy team observed that a DDoS service that only accepted cryptocurrency Bitcoin had a two percent conversion to paid subscriber rate, while two competitors that accepted PayPal had fifteen percent and twenty–three percent conversion rates, respectively.[149] At least for financially–motivated criminal enterprises that depend on sales to average consumers—the purchasers of online pharmaceuticals and counterfeit handbags discussed in this Article—profitmaking will depend on low transaction costs and simple access procedures for consumers. Skeptics may invoke the technically–shrouded, sophisticated marketplace Silk Road as a counternarrative, but Silk Road was small in comparison to the enormity of the international drug trade and there is some evidence that it served a business–to–business function for drug dealers.[150] Presumably drug dealers finding a supply for drugs to resell would be more motivated to learn the intricacies of cryptocurrencies, but many ordinary consumers cannot.

Enforcers will likely continue their focus on intermediaries to police their brands and to break up botnets. These efforts raise concerns over due process, property rights, and privacy rights. This Article shows that IP enforcers are able to take control over thousands of domain names, including those that include goods other than the infringing items. Interventions are often done *ex parte*, and may not require notice to the affected websites under Rule 65. In fact, attacks on botnets must omit this notice for fear that cybercriminals can avoid the attempts to sinkhole the

148. Paul Vigna, *People Love Talking About Bitcoin More Than Using It*, WALL ST. J. (Apr. 12, 2017, 5:30 AM), https://www.wsj.com/articles/people-love-talking-about-bitcoin-more-than-using-it-1491989403.

149. Mohammad Karami, Youngsam Park & Damon McCoy, *Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services*, *in* PROCEEDINGS OF THE 25TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 1033 (2016).

150. Judith Aldridge & David Décary-Hétu, Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation (May 13, 2014) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643.

botnet. It is important that interventions reflect appropriate humility in light of the lack of adversarial process.