THROUGH A ROUTER DARKLY: HOW NEW AMERICAN COPYRIGHT ENFORCEMENT INITIATIVES MAY HINDER ECONOMIC DEVELOPMENT, NET NEUTRALITY AND CREATIVITY

By Peter Groh*

Volume XIII – Fall 2012

On November 1, 2012, Russia enacted a law putatively aiming to protect Russian children from pedophiles.[1] This law authorizes deep packet inspection (DPI), a method used for monitoring, filtering and shaping internet traffic, which has heightened concerns among many leading privacy groups. These groups are concerned with how the government will use such an intrusive method in prosecuting child predators.[2] Central to this concern is DPI's capability to allow the Russian government to peer into any citizens' unencrypted internet traffic and monitor, copy, or even alter the traffic as it moves to its destination.[3] The unresolved question is whether the government's use of DPI will be restrained and utilized primarily to thwart child predators, or whether it will be expanded to lay the groundwork for a new era of national censorship.[4] Although the United States has not yet adopted similar tactics in regulating its citizens' internet use, Russia's implementation of the new DPI monitoring and filtering system will provide an educational opportunity for both privacy advocates and policymakers.

[1] Reuven Cohen, *Russia Passes Far Reaching Internet Censorship Law Targeting Bloggers and Journalists*, FORBES (Nov. 1, 2012, 1:57 PM), http://www.forbes.com/sites/reuvencohen/2012/11/01/russia-passes-far-reaching-internet-censorship-law-targeting-bloggers-journalists/.

[2] Andrei Soldatov & Irina Borogan, *The Kremlin's New Internet Surveillance Plan Goes Live Today*, WIRED (Nov. 1, 2012, 6:30 AM), http://www.wired.com/dangerroom/2012/11/russia-surveillance/.

[3] *Id.*

[4] *Id. See also Russia Deploys a Massive Surveillance Network System*, SECURITY AFFAIRS (Nov. 2, 2012), http://securityaffairs.co/wordpress/9956/intelligence/russia-deploys-a-massive-surveillance-network-system.html.

This paper operates under the premise that conflicts over internet usage have arisen and escalated in a manner that is as coevolutionary as an arms race.[5] For example, as individuals have discovered ways to exchange information in a way that circumvents property rights like copyright, enforcement officials have discovered tactics to limit or frustrate such activity. In response, the infringers have complicated their methods. Russia's implementation of DPI may succeed in the laudable goal of stopping the spread of child pornography or sex trafficking. However, it is possible that this program is actually a domestic spying program merely masquerading as a crime-fighting tool. It is also possible that DPI may begin with the goal of combatting child pornography, but its mission may ultimately expand to serve innumerable other investigatory purposes, including but not limited to investigations into political dissidence, independent journalism, or copyright infringement.[6]

American policymakers face similar issues in regulating Internet usage as Russia but they have been unable to enact legislation similar to Russia. Instead, American policymakers outside the halls of government have attempted to combat copyright infringement through extralegal means that do not require the authority of a sovereign. These solutions can be implemented, maintained, and defended outside of the courtroom as much as possible. This article examines whether a solution such as the Copyright Alert System (CAS) is effective as well as what collateral impacts, if any, there may be on individuals' internet behavior. This article also examines the risk of mission creep (namely, the risk copyright enforcement mechanisms

---

[5] Coevolution may also be considered a parallel evolution, namely the alteration (or even transference) of traits, features or behaviors between two unrelated entities that progressively alter properties of each entity but also their effects upon their environment, such as in a predator/prey relationship. *See* Manuel Soler et al., *Micro-Evolutionary Change and Population Dynamics of a Brood Parasite and Its Primary Host: The Intermittent Arms Race Hypothesis*, 117 OECOLOGIA, no. 3, at 381-90 (1998). This analogy is not without its detractors, however: *see also* Peter Abrams, *Is Predator-Prey Coevolution An Arms Race?* TRENDS ECOL EVOL., 108-10 (1986).
[6] Alissa Cooper, *The Singular Challenges of ISP Use of Deep Packet Inspection*, DEEP PACKET INSPECTION.CA, http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection/ (last visited Nov. 10, 2012).

subsequent to CAS could be utilized to stifle free speech or market competition) in pursuit of such a solution.

Before proceeding further, a disclaimer should be issued. While the remainder of this article discusses what steps are likely to be taken by what content creators and others refer to as 'sophisticated pirates,' this article's premise is that with each development in the realm of enforcement, the interconnected and equalizing nature of the internet has provided access to productive lines of flight that escape the very scheme that it was meant to reign in. Even though this article does not take a stance on the ethics of piracy or copyright enforcement, any extended discussion on this issue is bound to bring up tactics that circumvent or frustrate the purposes of programs such as the CAS. In discussing these developments, it is worth remembering that the tactics discussed herein are benign tools that are capable of innovation or infringement, depending solely upon the circumstances under which they are wielded. The author does not seek to implicitly condone or excuse such uses but believes that the discussion of these alternatives illustrates fundamental shortcomings of the CAS.

This article will first discuss the framers, structure, and historical context of the CAS. Discussion will then turn to the underlying axioms of programs like the CAS and their effects on the infrastructure of the internet and its users. Finally, in discussing the shortcomings of CAS' current implementation, this article will examine several mitigating procedures likely to be used to circumvent the CAS in the future, rendering it functionally irrelevant as an innovative copyright enforcement mechanism. This ineffectiveness is argued to be exemplary of the coevolutionary nature of this conflict between piracy and enforcement, but also calls into questions the premises its framers operated under in an attempt to putatively protect their interests.

THE COPYRIGHT ALERT SYSTEM

Beginning in early 2013,[7] some internet users in the United States will receive a message

from their internet service providers (ISP's).[8] This message will politely inform them that a user

on their network is believed to have infringed upon a copyright, and that such an infringement

violates the ISP's acceptable use policy. It will also notify the user about the serious

consequences of copyright infringement should such behavior continue. The ISP will inform the

user that the message constitutes their first warning of the consequences of such behavior on

their network, and it will list possible ways to avoid future offenses by directing the user to a

variety of lawful media content sites.[9]

The ISP will continue to send this notice to the user should it be notified that copyright

infringement has allegedly been committed again from the same internet account. This second

notice will be almost identical to the first. Should the ISP continue to receive allegations of

copyright infringement from a variety of unnamed content creators, a third and fourth notice will

be sent. This notice will request the internet account subscriber to "acknowledge receipt" of the

messages by clicking on a notice that will redirect the subscriber to educational resources on

copyright infringement and its serious consequences.[10] If the ISP receives information that the

subscriber continues to commit 'infringing behavior,' the Copyright Alert System (CAS) allows

for ISPs to send enhanced alerts that 'mitigation measures' will follow.[11] The form and extent of

---

[7]*Dotting Our "I"s*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/node/714 (last visited Nov. 28, 2012).

[8] AT&T, Cablevision, Comcast, Time Warner Cable and Verizon. *See Frequently Asked Questions*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/faq (last visited Nov. 7, 2012) [hereinafter *FAQ*].

[9] *About*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/about (last visited Nov. 7, 2012).

[10] There are no findings of fact or evidence necessary to provide to the CAS other than an allegation of infringement: the ISP's will not review each notice for validity, and it is up to the subscriber to initiate any appeal. *See FAQ*, *supra* note 8.

[11] *The Copyright Alert System: Moving to Implementation*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/node/709 (last visited Nov. 7, 2012).

such mitigation measures are determined by the ISP and range from requiring the subscriber to review education materials on copyright infringement[12] to temporarily 'throttling' the subscriber's internet access by limiting the internet connection to a fraction of the advertised or normal speed.[13] The Center for Copyright Information (CCI) as a facilitating entity for the CAS highlights that it will not actively participate in the enforcement of mitigation measures but will simply pass along information suggesting that infringement has occurred, and repeatedly mention that there is no risk of termination of service but merely the mitigation of infringing behavior.[14] The CCI will not directly suspend or throttle a subscriber's internet access. Instead, it is just a facilitator in providing the ISP with enough information which results in the ISP sending a notice to the subscriber and/or initiating mitigation measures.

The arrival of the CAS is a generic response to what the MPAA and RIAA regard as the insidious spread of BitTorrent technology into popular knowledge and use. Since 2003, when the BitTorrent protocol's creation allowed utilization of that technology to take advantage of previously unused upload bandwidth, BitTorrent has been routinely used to acquire copyrighted works in the United States to a considerable effect, and to what the MPAA and RIAA regard as a considerable loss of revenue.[15] The murky nature of illegal filesharing makes any analysis of the lost revenue inherently fuzzy. A growing body of literature on movie piracy suggests a wide range of possible effects on sales: from no tangible loss through sales displacement to an exact

---

[12] *Id.*

[13] *Id.*

[14] "These mitigation measures will vary by ISP and range from requiring the subscriber to review educational materials, to a temporary slow-down of Internet access speed. However, termination of a consumer's Internet service is not a part of any ISP's Copyright Alert System program. Contrary to many erroneous reports, this is not a "six-strikes-and-you're-out" system that would result in termination. There's no "strikeout" in this program." (emphasis removed). *Id.*

[15] *Intellectual Property Theft: A Threat to U.S. Workers, Industries, and our Economy*, DEP'T FOR PROFESSIONAL EMPLOYEES, AFL-CIO (2012), http://dpeaflcio.org/wp-content/uploads/IP-Theft-Fact-Sheet-2012.pdf.

1:1 ratio between displaced sales and pirated downloads.[16] The MPAA has repeatedly cited

numbers generated by the Institute for Policy Innovation (IPI) finding that the U.S. economy

annually loses more than $58 billion due to content theft, which it equivocates to "more than

373,000 lost American jobs, $16 billion in lost employee's earnings, plus $3 billion in badly

needed federal, state and local governments' tax revenue."[17]

However, some consider the CAS to be a specific response to the MPAA and RIAA's

failure to successfully lobby for legislative solutions to help prevent this loss of revenue,

including the Stop Online Piracy Act[18] (SOPA) and the PROTECT IP Act (Preventing Real

Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA).[19] Both

SOPA and PIPA exhibited structural similarities to the Combating Online Infringement and

Counterfeits Act (COICA),[20] which would have authorized executive branch representatives and

copyright holders to use a variety of means to curb access to sites that facilitate infringement.

Beginning with COICA's introduction on September 20, 2010,[21] and culminating with SOPA

and PIPA's failure to reach the floor of their respective legislative houses due to unprecedented

online backlash,[22] the lobby interests representing United States content creators have strived to

craft a legislative response to the problem of disseminating infringing material — with limited

success.

---

[16] Brett Danaher & Joel Waldfogel, *Reel Privacy: The Effect of Online Film Privacy on International Box Office Sales*, http://techfleece.com/2012/02/15/reel-piracy-the-effect-of-online-film-piracy-on-international-box-office-sales/.
[17]Press Release, MPAA, MPAA Statement on Strong Showing of Support for Stop Online Piracy Act (Dec. 16, 2011), *available at* http://www.mpaa.org/resources/5a0a212e-c86b-4e9a-abf1-2734a15862cd.pdf.
[18] H.R. 3261, 112th Cong. (2011).
[19] S. 968, 112th Cong. (2011).
[20] S. 3804, 111th Cong. (2010).
[21] *Id.*
[22] Jonathan Weisman, *After an Online Firestorm, Congress Shelves Antipiracy Bills*, N.Y. TIMES (Jan. 20, 2012), http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=0.

Both COICA and PIPA focused on the authority to alter the Domain Name System

(DNS) Registry. The DNS Registry functions as an effective 'map' by which queries directed

from a user's computer system can be resolved to the proper top-level domain that the user is

seeking, such as www.google.com or www.law.pitt.edu. SOPA went even further by authorizing

the content creators' request of court orders via the Attorney General so that they could bar

advertising networks and payment facilities from conducting business with infringing domains,

block various aggregators such as search engines from indexing or linking to the infringing

domains, and enable ISPs to filter infringing domains from being accessed by its subscribers.[23]

Under SOPA, upon the issuance of a notice and intent to proceed by the Attorney General, a

court may issue either: a temporary restraining order, a preliminary injunction, or an injunction

against the allegedly infringing website.[24] Having only received an application from the

Attorney General, and within 5 days of that application having been granted, all of the

advertising networks, payment facilities and/or hosting services would have to grant the

injunction without any further hearing or notice to the alleged infringer.[25]

Since Congress failed to enact either piece of legislation, the lobbying groups

representing American content creators turned to policy solutions that would require as little

legislative or judicial oversight as possible.   To this end, lobbyists for copyright owners had

been collaborating with America's five largest ISPs to form the CCI in September 2011,[26] which

---

[23] H.R. 3261 Bill Summary & Status, 112th Cong. (2011), *available at* http://www.webcitation.org/643NehNoc. *See also* H.R. 3261, 112th Cong. (2011), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf.
[24] H.R. 3261 §102(b)(5) "Relief"
[25] *Id.*
[26] *See Common Framework*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/commonframework (last visited Nov. 9, 2012).

was based on a memorandum of understanding signed between its members in July of 2011.[27]

The production of the CCI went hand-in-hand with its parties' lobbying efforts for legislation, as it was created while SOPA and PIPA had a greater chance of passage and well before the proposed legislation faced public backlash. Consequently, it is apparent that the policy directives reflected in the CAS are a part of what was intended to be a much more multifaceted and complementary approach. They are not simply a one-shot response to the lobby's failure to effectively push for legislation.

BITTORRENT TRAFFIC AND YOU

The CAS most hopes to affect the traffic between users downloading infringing material. The BitTorrent protocol has been indispensable to newer forms of filesharing, whether it is legal or not.[28] A user's computer has a variety of protocols for transferring data over a network. For example, the File Transfer Protocol (FTP) transfers files from one host to the other,[29] and the Real-time Transport Protocol (RTP) streams audio and video for video teleconferencing. BitTorrent is also a protocol for distributing files.[30] One limitation of other file-transfer methods, such as a FTP transfer, is that a central host is necessary in order for many systems to access and download a given file.[31] Another constraint is that other protocols cannot receive information in segments like BitTorrent. The BitTorrent protocol accepts packets of information that allow a

---

[27] Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=214505.
[28] Austin Carr, *BitTorrent Has More Users Than Netflix and Hulu Combined – and Doubled*, FAST COMPANY (Jan. 4, 2011), http://www.fastcompany.com/1714001/bittorrent-has-more-users-netflix-and-hulu-combined-and-doubled.
[29] J. Postel & J. Reynolds, *File Transfer Protocol (FTP)*, NETWORK WORKING GROUP (Oct. 1985), http://tools.ietf.org/html/rfc959.
[30] Brian Cohen, *The BitTorrent Protocol Specification*, BITTORRENT.ORG (June 25, 2009, 1:41 AM), http://www.bittorrent.org/beps/bep_0003.html.
[31] *Id.*

user to index, download, and assemble a large file from a variety of sources[32] in the same manner

that an individual could piece together a puzzle from multiple boxes by referencing the final

image. The BitTorrent protocol makes a more efficient use of limited traffic bandwidth by

sharing information among multiple users who are attempting a download or hosting (seeding)

the torrent file. For example, when a peer finishes downloading a piece and checks its integrity

against the index, it announces that it has that piece to all of its peers (the BitTorrent "swarm"),

which decentralizes the demand for a particular piece of a file by allowing subsequent requests

for that piece to be routed to either the original source or any user in the swarm who has

announced they have it.[33] This decentralization has advantages, but in order to more effectively

manage the bandwidth being used by the swarm to exchange the file, the Internet Protocol (IP)

address of each user in the swarm is revealed.[34] This identifying information may then be used to

track the internet service provider that hosts that IP address and the subscriber to whom it was

assigned.

SIX STRIKES AND YOU'RE THROTTLED

The pending implementation scheme of each ISP pursuant to their partnership with the

CCI of the Six Strike CAS system has already been described at length in this article,[35] and need

not be restated. While analysis of the CAS is in its relative infancy due to its pending status and

genesis as a privately negotiated agreement, rather than a publicly debated piece of legislation,

early appraisals of the CAS's public interest implications are less than glowing.[36] The CAS

grapples with the norms of freedom of expression, privacy, fairness, proportionality, and

---

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *See supra* text accompanying notes 8-16.
[36] *See generally* Bridy, *supra* note 27.

transparency.[37] In particular, the private origins of CAS present a fundamental problem for the

public interest, as Bridy notes:

> Although the same concerns are raised by publicly administered protocols like
> Hadopi, the private nature of CAS [Copyright Alert System] means that there will
> be no public forum for debate over the terms of the MOU [Memorandum of
> Understanding] or the procedures and sanctions it prescribes. CAS was presented
> to the public as a *fait accompli* and will be offered for the public's assent as a
> contract of adhesion for broadband service. There will be, in other words, no
> bargaining about it. Some people will be able to choose a non-party ISP and
> thereby avoid being subject to CAS, but many (if not most) will not have that
> option given the state of the market for residential broadband service and the size
> and reach of the ISPs participating in the MOU. CAS will be the law for millions
> of U.S. broadband subscribers, whether they like it or not. As with the Eircom
> protocol, because there is no state action involved, there will be no judicial review
> of the constitutionality of the MOU's provisions. The CCI advisory board, whose
> members were not even appointed until after negotiations over the substance of
> CAS were closed, is the public's only advocate within the CAS governance
> structure, yet it had no role in the design of the protocol and is not empowered to
> make recommendations about implementation that bind the CCI executive
> committee.[38]

While Bridy concluded that the public interest assessment of the CAS revealed the Six Strike

System to be a decidedly mixed bag for ISP subscribers, this article focuses on the likely

extralegal responses that the CAS necessitates by those whose actions suggest that reform, and

not education, is needed to combat copyright infringement.[39]

The CAS complements a tactic utilized by the MPAA in setting up torrent files of its

intellectual property as 'honey pots,' which monitor BitTorrent swarms that are used to pull

infringing material from a multitude of sources and assemble them at the user's computer.[40] IP

---

[37] *Id.* at 25.

[38] *Id.*

[39] *See* Cory Doctorow, *Accused of infringement? AT&T will take away YouTube and Facebook and send you to Copyright Reeducation Gulag*, BOINGBOING (Oct. 14, 2012), http://boingboing.net/2012/10/14/accused-of-infringement-att.html (depicting leaked training documents from AT&T – suggesting that limited access to or redirection from "popular sites" such as Google or Youtube will be the primary vehicle of "re-education efforts," which is problematic in assuming without any meaningful warrant the premise that it is simply a lack of awareness that causes individuals to infringe).

[40] *See* Brett Thomas, *MPAA Gets Caught Laying Torrent Traps*, BIT-TECH (Jan. 12, 2007), http://www.bit-tech.net/news/bits/2007/01/12/MPAA_gets_caught_laying_torrent_traps/1.

addresses are recorded by the computer monitoring the swarm. Additionally, copyright

enforcement representatives can monitor and record the IP addresses of BitTorrent swarms that

they have merely joined, and not initiated. This form of tracking is the necessary first step that

required the implementation of CAS so that those who are recorded as infringing may be

punished through a manner which is largely immune to meaningful judicial review.

Unfortunately, even as the technical barriers to monitoring are being reduced, this tactic

primarily works for the large, well-situated members of the MPAA who have the resources to

partake in such monitoring.[41] Smaller content creators have begun to utilize this tactic more

recently in propagating lawsuits against a multitude of infringing IPs to leverage settlement for a

fraction of the penalty under the Digital Millennium Copyright Act (DMCA).[42] However, it has

yet to be determined whether smaller content creators will have the same ease of access or

monitoring as the entities that joined the MOU which created the Six Strike System.

Equally unclear is whether the evidentiary value of an IP address in sustaining a lawsuit

against a real party will be altered by the pending hearings in the Eastern District of

Pennsylvania before Judge Michael Baylson.[43] In the past, the existence of an infringing IP

address has created the presumption that the subscriber of the IP address was also the infringing

entity. Should Judge Baylson hold that the tactics of IP address collection are not sufficient to

---

[41] *Independent Expert Assessment of MarkMonitor AntiPiracy Methodologies*, STROZ FRIEDBERG (Nov. 1, 2012), http://www.scribd.com/doc/112296380/Independent-Expert-Assessment-content-cci-Redacted (describing how once a month the Content Owner Representatives provide MarkMonitor lists of titles of copyrighted works they would like monitored). MarkMonitor identifies infringing online versions of these titles through comprehensive scanning across multiple sites. *Id.* Each new instance of an identified work is fully downloaded and reviewed by MarkMonitor personnel to verify that it is in fact an actual infringing copy of the title. *Id.* The purpose of this step is to verify that the file being targeted is the asset intended for monitoring by the content owners. *Id.* This verification step is crucial to ensure that the content owners are not enforcing antipiracy measures on non-protected works and is a key part of MarkMonitor's ongoing success in the proper identification of P2P copyright infringement. *Id.*

[42] *See US judge orders piracy trial to test IP evidence*, BBC (Oct. 9, 2012), http://www.bbc.co.uk/news/technology-19887765.

[43] *Id.*

sustain a copyright infringement suit the CAS may become a primary avenue for accomplishing the same goals of deterrence that an infringement lawsuit represents. However, the remedy available to the aggrieved content creator would be substantially limited by comparison, or it would require further monitoring resources to effectuate the same ends.

SUPPRESSION OF ALTERNATIVES AS DISCIPLINARY POWER: SURVEILLANCE AS CONTROL

The CAS is also being implemented against a backdrop of governmental copyright enforcement as exemplified by the ongoing program, 'Operation In Our Sites.'[44] The National Intellectual Property Rights Coordination Center, managed by the Department of Immigration and Customs Enforcement's (ICE) Homeland Security Investigations arm, is complementing the CAS approach by targeting websites and their operators that it believes are distributing counterfeit and pirated items over the internet.[45] While its success and methods have been controversial and sometimes misapplied,[46] 'Operation In Our Sites' has resulted in the seizure of 758 top-level domains and nearly $900,000.[47] However, of these 758 domains, only seven have been engaged in the sale of counterfeit goods, suggesting that ICE has primarily focused on copyright enforcement of intellectual property.[48] In response, some sites that maintain top-level domains (TLD),[49] managed by the American-based Internet Corporation for Assigned Names

---

[44] *See Operation in Our Sites,* NAT'L INTELLECTUAL PROP. RIGHTS COORDINATION CENTER, http://www.ice.gov/doclib/news/library/factsheets/pdf/operation-in-our-sites.pdf (last visited Nov. 6, 2012).
[45] *Id. See also* Ernesto, *Feds Seize Domain Names of Korean Movie Portals*, TORRENT FREAK (Dec. 4, 2011), http://torrentfreak.com/feds-seize-domains-of-korean-movie-portals-111204/.
[46] *See* Alex Goldman, *Operation in Our Sites Misses Its Mark (Updated)*, ON THE MEDIA (Dec. 8, 2011, 4:31 PM), http://www.onthemedia.org/blogs/on-the-media/2011/dec/08/operation-in-our-sites-misses-mark/; *see also Members of Congress Investigate Dajaz1.com Seizure Based on Unpoven RIAA Claims*, HYPERBOT.COM (Sept. 3, 2012), http://www.hypebot.com/hypebot/2012/09/members-of-congress-investigate-dajaz1com-seizure-based-on-unproven-riaa-claims.html%20.
[47] Enigmax, *Operation in Our Sites: 758 Domains, Nearly $900,000 Seized*, TORRENT FREAK (Apr. 10, 2012), http://torrentfreak.com/operation-in-our-sites-758-domains-nearly-900000-seized-120410/.
[48] *Id.*
[49] For example, ThePirateBay.se, among others used to be ThePirateBay.org, and redirect from .com. With the rounds of ICE seizures ongoing, its administrators made the decision to abdicate to a cc-TLD for protection from

and Numbers (ICANN), have attempted to circumvent ICE's jurisdiction by re-registering with country code top-level domain (ccTLD) names for countries, such as Sweden which are outside the control of U.S. Corporations such as ICAAN.[50] While ICE's approach has enjoyed some success in shuttering domains, it is an incomplete effort given that the internet's infrastructure enables individuals to easily set up the same infringement facilitating material through proxies. ICE has essentially been engaged in a jurisdictional exercise of "whack-a-mole" because for each TLD it takes down a ccTLD may take its place in a jurisdiction beyond its authority.

However, if content creators are able to limit access by forwarding information on facilitators of infringement to ICE for Operation In Our Sites while simultaneously policing subscribers to the five largest ISPs in America, then these subscribers would find it difficult (although maybe feasible) to subscribe to a non-CAS ISP. By suppressing meaningful alternatives, a broad enforcement scheme for policing the periphery of the internet becomes a plausible reality for extinguishing the exchange of speech or data in general. A key feature of such a scheme lies in its claimed capability to continuously surveil a user's internet traffic in such a way that the user cannot ascertain when or if he or she is even being monitored. Resultantly, such a scheme would force the subscribers to act fearfully as if they are always under surveillance.[51]

An incidental complication of the DPI utilized by the Russian government as well as surveillance procedures that are preferred by the CAS is that all traffic for all subscribers must be scrutinized at all times in order for the scheme to be most effective. Public knowledge or even

---

ICE's enforcement. *See* WinstonQ1337, *Site Domain Moved to .se*, THEPIRATEBAY.SE (Feb. 3, 2012), http://thepiratebay.se/blog/205; *see generally* Ernesto, *Kim Dotcom Avoids "Unsafe" .com, Picks Me.Ga for New Megaupload,* TORRENT FREAK (Nov. 1, 2012), http://torrentfreak.com/kim-dotcom-avoids-unsafe-com-picks-me-ga-for-new-megaupload-121101/.

[50] *See* THE PIRATE BAY, http://thepiratebay.se (last visited Nov. 7, 2012).

[51] Bridy, *supra* note 27, at 28.

suspicions of such a capability is imbued with the insidious power of "creating an environment of pervasive and invisible surveillance"[52] that mirrors developments in penal systems, educational experiments and dictatorships alike: sometimes just knowing you are always being watched is enough to coerce compliance from citizens. The sovereign's interest in this setting is the same whether the sovereign is represented for example by a democratically elected government, a prison warden or a vicious dictator: the efficiency of control.[53] This control can only be perfected by simultaneously policing the periphery and limiting the alternatives to being surveilled that may be available to the citizenry. ICE's tactics, as lobbied for by content creators, completes this loop, and allows the economic and practical suppression of infringement as well as other ancillary activities that do not actually constitute infringement.[54] Already, the use of remedies available to content creators under the DMCA often result in collateral damage to parties availing themselves of potentially infringing material under the parameters of fair use.[55] The implementation of CAS would attempt to further this suppression, which is particularly interesting given the failure of private suits as a remedy against infringing activity to stem the use of BitTorrent protocols even in cases where monitoring similar to DPI is available to the ISP.[56]

---

[52] *Id.* at 29.

[53] *Id.* at 29. *See also* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, 66 U. CIN. L. REV. 177 (1997).

[54] Bridy, *supra* note 27, at 29.

[55] *See* Tim Cushing, *Textbook Publisher Pearson Takes Down 1.5 Million Teacher and Student Blogs With a Single DMCA Notice*, TECH DIRT (Oct. 15, 2012), http://www.techdirt.com/articles/20121013/18332220701/textbook-publisher-pearson-takes-down-15-million-teacher-student-blogs-with-single-dmca-notice.shtml.

[56] *See Too Legit to Quit: 124.2m Legal BitTorrent Music Downloads in 2012*, TORRENT FREAK (Sept. 22, 2012), http://torrentfreak.com/too-legit-to-quit-124-2m-legal-bittorrent-music-downloads-in-2012-120922/.

PIRATES ARE GOING TO PIRATE: THE CAS JUST FORCES FLIGHT TO ALTERNATIVES

In all likelihood, monitoring by copyright holders and ISPs will generate a community response. One such response will be the use of remote access to machines in jurisdictions beyond the United States. Such an action would enable individuals to infringe without presenting any meaningful recourse to American copyrights enforcement agencies. Under this paradigm, remote servers in jurisdictions, such as the Netherlands, are remotely accessed and host infringing content through a BitTorrent "swarm", that is, a multitude of different machines that are simultaneously accessing, hosting, and assembling the infringing content in pieces according to a set of instructions included with the torrent file. Because of the structure of the remote access, the last entities perceived as having received and assembled the infringing material via torrent to parties monitoring the swarm as part of a copyright enforcement scheme are left with the identifying information of the foreign server, not the domestic IP address that ordered it to access the infringing content.

Such a "private dedicated server" is called a Seedbox.[57] Numerous Seedbox features would allow infringing parties to skirt the measures promulgated by the CCI and the ISPs that have signed onto the Six-Strike System. An additional benefit to the use of a Seedbox is that there are minimal technical barriers to utilizing a foreign server as a seedbox.[58] The support structure of Seedboxes varies, but a plethora of providers have proliferated with the advertisement and the proposed implementation of the CAS. Many of these providers existed prior to any discussion of American implementation of such a system because foreign

---

[57] *Seedbox – What is it? How it works?*, WICKED SERVERS,
https://tal0ne.co.uk/knowledgebase.php?action=displayarticle&id=191 (last visited Nov. 10, 2012).
[58] *See id.*

jurisdictions' implementation of similar or more draconian measures have created a demand for such services.[59]

In addition to the use of a server in another jurisdiction, sophisticated users may also avail themselves of the services of a Virtual Private Network (VPN) in order to circumvent the surveillance protocols used by their ISP.[60] VPNs enable data encryption as well as the routing of said data through a remote host before it is transferred to the client computer.[61] Many seedbox providers also provide VPN services as a bundle in conjunction with a remote host that manages the bandwidth used to actually obtain infringing material using BitTorrent technology. A VPN is commonly used in corporate environments because of its encryption methods and its ease of access. A VPN is a popular option in the corporate world when employees or clients remotely require resources but do not wish to use a communication method that can be easily eavesdropped upon. The only limitation on use of a VPN to obtain infringing material is whether a 'private tracker'[62] permits a connection over a VPN (many private trackers prohibit such a connection as part of their network infrastructure).[63] Circumventing the encryption between a client computer and its host using a VPN is challenging and of questionable legal status, depending on the circumstances. Cracking such encryption while a subscriber uses their file-transfer protocol to connect to and download from a remote host would be incredibly inefficient. Additionally, it would be statutorily barred except in the matters related to an active

---

[59] *See, e.g.*, *Seedbox List*, SEEDBOX PROVIDERS (Sept. 10, 2010, 12:06 PM), http://www.seedboxlist.com/seedbox/.
[60] Paul Ferguson and Geoff Huston, *What is a VPN? – Part* I, 1 Internet Protocol Journal 1 (June 1998), *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/what_is_a_vpn.html.
[61] *Id.*
[62] *How to Join a Private Tracker*, BITTORRENTGUIDE (Feb. 15, 2011, 10:21 AM), http://bittorrentguide.com/how-to-join-a-private-tracker (a private tracker is a server that manages the communication between peers using the BitTorrent protocol that restricts access to users based on certain criteria such as upload/download ratio or a credentials like a username and password).
[63] *Id.*

criminal investigation. These already significant considerations are multiplied when considered in an international setting.

CUI BONO: HOW WILL CONTENT CREATORS DEAL WITH THIS ESCALATION?

CAS implementation and the accompanying shift of large-scale content creators from mass-IP lawsuits to an extrajudicial disciplinary approach may have ancillary trickle-down effects on content creators of a smaller import. However, whether those trickle-down effects will be beneficial remains to be seen and is indeed an unsubstantiated claim at best. As MPAA membership is limited,[64] so are the voices of smaller innovative content creators, who have arguably benefited from the exchange of their material though mediums such as the BitTorrent protocol.[65] Interestingly, given the inherent uncertainty in determining the economic impact of piracy and that lobbying by smaller content creators fail to match the efforts of the larger studios, it may even be argued that CAS' policing of the periphery will hamper rather than protect the innovation of smaller content creators.[66]

Content creators may feasibly voluntarily forward notification of infringement to ISPs as part of their participation in the CAS system if they aren't already outsourcing their monitoring to a third party company such as MarkMonitor.[67] However, monitoring the network infrastructure and the continued use of DMCA protections in an overly broad and crude scope

---

[64] *About Us*, MOTION PICTURE ASSOCIATION OF AMERICA, http://www.mpaa.org/about (last visited Nov. 5, 2012).
[65] *See* Lauren Dugan, *Crowd Funded, Torrent Distributed Thriller Challenges Hollywood*, SOCIALTIMES (June 21, 2010, 11:09 AM), http://socialtimes.com/crowd-funded-torrent-distributed-thriller-challenges-hollywood_b15624.
[66] *See* Danaher & Waldfogel*, supra* note 16. The article acknowledges the fuzziness of any numerical analysis of piracy at the moment, but is still able to conclude statistically that piracy has an effect on international box office sales and international distribution. The finding is consistent with the suggestion that domestic piracy's direct effect on domestic box office numbers or domestic distribution (as a subset of total revenue generated by a given intellectual property) is attenuated, ambiguous and does not warrant a policy intervention absent further study that isn't being initiated on behalf of the industry itself.
[67] *See supra* note 41 and accompanying text.

will likely continue to hamper efforts and innovation absent a legislative rebuke or redirection from Congress. It seems that we have arrived at an impasse where even the nonprofit entities supporting smaller content creators are in limbo amidst a hydra-like system of enforcement that has a laudable goal, but may have bitten off much more than can be chewed. This is particularly true if the response from the Internet Community is simply to alter its behavior and become more sophisticated, even as the methods of acquisition of infringing material proliferate beyond the borders of the authorities so desperate to curtail it.

Copyright enforcement entities have attempted to manage digital rights with limited success. Furthermore, they have attempted to deter individuals with the threats of unimaginably high financial penalties for infringing behavior. Neither of these tactics nor their predecessors have meaningfully stemmed the exchange of infringing material. It is unlikely that such unrestricted surveillance will enjoy any greater success, but it may very well affect other principles of the internet in a way that is unforeseeable, uncertain and unfortunately undemocratic.[68] While the CAS is certainly not the last shot in the escalating conflict between infringing entities and copyright enforcement, one would hope that its lack of transparency and arguably insufficient consumer safeguards[69] will gradually be addressed in a public manner in the future.

---

[68] "The technology appears to be 'just the way things are'; its origins are concealed, whether those origins lie in state-sponsored scheme or market-structured order, and its effects are obscured because it is hard to imagine the alternative. Above all, technical solutions are less contentious; we think of a legal regime as coercing, and a technological regime as merely shaping -- or even actively facilitating -- our choices." Boyle, *supra* note 53, at 205.
[69] *See* Bridy, *supra* note 27.