SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013

TABLE OF CONTENTS

The Inevitable Television Revolution:
the Technology is Ready, the Business is Lagging, and the Law Can Help
Blaine Bassett..... 1

Neutrality in the Digital Battle Space:
Applications of the Principle of Neutrality in Information Warfare
Allison Gaul..... 51

Artificial Intelligence and the Patent System:
Can a New Tool Render a Once Patentable Idea Obvious?
William Samore..... 113

The Usefulness of the International Trade Commission as a Patent Forum
in the Wake of Certain Personal Data and Mobile Communications Devices
and Related Software (Apple v. HTC)
Stephen Burke..... 143

Sending Servers to the Sky:
Can Bit Torrent Piracy be Perpetuated by the Use of Unmanned Drones?
David Hutchinson..... 171

Use of Patented Inventions after FDA Approval:
How to Define the Hatch-Waxman Safe Harbor in Light of Momenta *and* Classen
Madeline Schiesser..... 193

Review of "Legally Poisoned: How the Law Puts Us at Risk from Toxicants"
by Carl F. Cranor
Alessandra Baldini..... 220

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013

In Memoriam

Professor Theodore Hagelin
April 7, 1943 - May 18, 2013

Professor Hagelin served as the faculty advisor for the Syracuse Journal of Science and Technology Law up until his passing earlier this year. As an advisor, he was an integral part of the journal community. He was an expert in technology innovation law and the technology commercialization process. His mentorship of journal members year after year helped to produce the prestigious works that we share with the legal community. While he is no longer with us, his commitment and passion for the Syracuse Journal of Science and Technology Law lives on.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 1, PAGE 1

THE INEVITABLE TELEVISION REVOLUTION: THE TECHNOLOGY IS READY, THE BUSINESS IS LAGGING, AND THE LAW CAN HELP

Blaine Bassett

I. Introduction:

A Revolution Is Happening

SPOILER ALERT: A revolution is transpiring that will leave television so changed twenty years in the future as to make it unrecognizable to viewers from twenty years in the past. What is more, this proposition is hardly controversial. The ubiquity of the phrase "SPOILER ALERT" itself—now commonly applied in reference to scripted television shows,[1] reality shows,[2] sports contests,[3] and other television programs[4] to warn those who have not yet watched

1 *See, e.g.*, Shawna Malcom, *SPOILER ALERT: All About* Lost's *Number Game*, PEOPLE.COM TV WATCH (Feb. 17, 2010, 12:00 AM), http://www.people.com/people/article/0,,20421411,00.html (employing the "spoiler alert" phrase to warn users that had not yet seen particular episodes of the popular television drama *Lost* that the article would disclose details surrounding key plot elements of the show); Dean Bexter, *Spoiler Alert: The Office Spoilers*, BUDDYTV (Oct. 6, 2011), http://www.buddytv.com/articles/the-office/spoiler-alert-the-office-spoil-42083.aspx (employing the "spoiler alert" phrase prior to disclosing details about a new season of popular sitcom *The Office* to fans who had not yet watched the episodes).

2 *See, e.g.*, Jennifer Bowen, *Spoiler Alert: And the Next American Idol Is…*, MYFOXAL.COM (May 23, 2012, 7:35 PM), http://www.myfoxal.com/story/18610168/spoiler-alert-and-the-next-american-idol-is- (employing the "spoiler alert" phrase before announcing the season's winner of popular singing reality show *American Idol* for users who had not yet viewed the finale).

3 *See, e.g.*, Mike Gruss, *Olympics are Fair Game for Spoiler Alerts*, THE VIRGINIAN-PILOT (Aug. 1, 2012), *available at* http://hamptonroads.com/2012/07/olympics-are-fair-game-spoiler-alerts (arguing that the "spoiler alert" phrase is applicable to the outcome of Olympics contests).

the referenced program that possibly unwanted plot disclosures are to follow[5]—illustrates the reality of the television revolution as well as anything. When people limited their television viewing to live television programs on the days and times scheduled by television stations, there was no need for such a phrase in the television context. But "SPOILER ALERT" is seen everywhere today because, to exaggerate only slightly, "the nation's greatest secrets no longer are housed in military installations. They exist in the last seven minutes of . . . television shows. The country's greatest fear is . . . accidentally hearing what happened 20 minutes into your third-favorite television show on Wednesday nights, the ending everyone else watched two days ago."[6]

The television revolution may be alarming to the "Big Media" establishment who has controlled the television industry for decades,[7] but no one can seriously dispute that it is occurring. Television viewers today demand to watch television on their terms in a way that they

---

4 The "spoiler alert" phrase has even been used in the context of television commercials. Caffeinegoddess, **Spoiler Alert* Super Bowl 2013 Ads*, ADLAND.TV ADNEWS (Feb. 3, 2013, 5:47 PM), http://adland.tv/adnews/spoiler-alert-super-bowl-2013-ads-watch-them-now-and-know-what-will-air/1359910076. Additionally, some websites have been devoted exclusively to divulging information from recent and future episodes of popular television shows. *See, e.g.*, TVLINE.COM SPOILER ALERT, http://tvline.com/tag/spoiler-alert/ (last visited Mar. 1, 2013).

5 Wikipedia explains that "[a] spoiler is any element of any summary or description of any piece of fiction that reveals any plot element which will give away the outcome of a dramatic episode within the work of fiction or the conclusion of the entire work. . . . The words 'spoiler alert' in all capitals are usually used to warn readers of a spoiler." WIKIPEDIA, http://en.wikipedia.org/wiki/Spoiler_(media) (last visited Mar. 1, 2013).

6 Gruss, *supra* note 3.

7 Throughout this Comment, the phrase "Big Media" will be used to refer collectively to the powerful networks, corporations, agencies, and other entities that have traditionally controlled the television industry. For example, Big Media may refer to major television networks (e.g., ABC, CBS, NBC, Fox, etc.), cable companies and others controlling the distribution of television content (e.g., Dish Network, Verizon, Comcast, etc.), government agencies (e.g., the Federal Communications Commission ("FCC")), major advertisers, and others who significantly influence the industry.

did not demand twenty years ago. As this demand for control swells in the viewers, television becomes less and less recognizable as an extension of the "boob tube" of the Twentieth Century.

The ongoing television revolution is not the first media revolution that mankind has experienced.[8] Experience shows that, while people want to believe that they have a grasp on where things are going during a revolution, no one actually does.[9] Revolutions are inherently unpredictable. As Clay Shirky—a "prominent thinker on the social and economic effects of Internet technologies"[10]—describes it, revolutions distort the perceived reality of the people living through them, particularly those who stand to lose the most as the revolution transpires.[11] Such people tend to be willing to look at any and every prediction of the future other than "the unthinkable one"—the one where the old model is not only broken, but where nothing will work to fix it.[12] Analyzing the newspaper industry in light of the revolution it is now going through, Shirky explained:

---

8 For example, the technological revolution brought about by the advent of the printing press was truly world changing. *See* ELIZABETH EISENSTEIN, THE PRINTING PRESS AS AN AGENT OF CHANGE (1980).

9 In an article outlining an ongoing revolution occurring in the printed newspaper industry, Clay Shirky refers to Eisenstein's THE PRINTING PRESS AS AN AGENT OF CHANGE as a "magisterial treatment of Gutenberg's invention." Discussing the famous revolution from hand-copied texts to printed books, Shirky explains that the revolution progressed in a particularly unpredictable way: "As novelty spread, old institutions seemed exhausted while new ones seemed untrustworthy; as a result, people almost literally didn't know what to think [and] experiments were only revealed *in retrospect* to be turning points." Clay Shirky, *Newspapers and Thinking the Unthinkable*, SHIRKY BLOG (Mar. 13, 2009, 9:22 PM), http://www.shirky.com/weblog/2009/03/newspapers-and-thinking-the-unthinkable (emphasis added).

10 Chris Anderson, himself a prominent influence in the world of technology and the Internet as editor-in-chief of *Wired* magazine from 2001-2012 and as a popular author and speaker, used these words to describe Clay Shirky. CHRIS ANDERSON, THE LONG TAIL 158 (2006).

11 Shirky, *supra* note 9.

12 Shirky, *supra* note 9.

> That is what real revolutions are like. The old stuff gets broken faster than the new stuff is put in its place. . . . [B]ig changes stall, small changes spread. Even the revolutionaries can't predict what will happen. Agreements on all sides that core institutions must be protected are rendered meaningless by the very people doing the agreeing. . . . Ancient social bargains, once disrupted, can neither be mended nor quickly replaced, since any such bargain takes decades to solidify.
>
> And so it is today. When someone demands to know how we are going to replace newspapers, they are really demanding to be told that we are not living through a revolution. They are demanding to be told that old systems won't break before new systems are in place. They are demanding to be told that ancient social bargains aren't in peril, that core institutions will be spared, that new methods of spreading information will improve previous practice rather than upending it. They are demanding to be lied to.
>
> There are fewer and fewer people who can convincingly tell such a lie.[13]

And so it is with the television industry. I will show that television technology has been revolutionized already, that television business models drastically lag the technology, and that the law can help resynchronize the technology and the business models into a revolutionized new form. What is more, I will show that the television revolution is a good thing for television viewers, that it is inevitable, and that the law *should* encourage and facilitate the revolution whenever possible.

---

13 Shirky, *supra* note 9.

To this end, I proceed in three parts. First, I examine television technology—where it began and how it has evolved—to show that it is revolutionized already. Starting with the early days of television, where all content was broadcast over the air by a small handful of powerful media companies,[14] I continue through various stages of the technology evolution such as cable and satellite signals and networks, videocassette recorders, and digital video recorders.[15] I finish surveying the technology with an examination of Internet streaming technology today and its ability to deliver limitless on-demand content choices with nearly unlimited flexibility.[16] I conclude that the technology is "there"—the technology is revolutionized already.

Second, I explore the business side of television to determine that it is arbitrarily inhibiting the technology and thereby slowing the revolution. In particular, I examine the traditional model of television to discover three major assumptions on which the industry has been built: 1) Big Media alone is capable of producing quality content, 2) Big Media alone is capable of suitably distributing that content, and 3) Big Media can guarantee advertisers that the "eyeballs"[17] they pay for are actually watching.[18] I analyze advantages and disadvantages of this traditional model.[19] Then, in light of these advantages and disadvantages, I scrutinize modern

---

14 *See infra* Part II.A.

15 *See infra* Part II.B.

16 *See infra* Part II.C.

17 The term "eyeballs" is commonly used in the vernacular of the advertising industry to refer to the attention of viewers within a desired demographic. *See, e.g.*, Steve Janke, *TV Advertising Primer*, ANGRY IN THE GREAT WHITE NORTH (Mar. 23, 2009, 3:45 PM), http://stevejanke.com/archives/284761.php ("[A]dvertisers pay the TV broadcasters for eyeballs. We, the television viewing audience, are the product being bought and sold. The television programming content is not the product. . . . Content is the lure to get those eyeballs.").

18 *See infra* Part III.A.

19 *See infra* Part III.B.

television business models and show that they are significantly lagging the technology and inhibiting the revolution.[20] The business is not revolutionized yet.

Third, I explore how the law can promote policy to facilitate the revolution and explain why the law should do so. I identify possible business models for the future of television, recognize that no one knows which ones will prove to be viable, and assert that the best policy is for the law to "shake up" the industry to encourage experimentation.[21] I illustrate how the law may accomplish this "shaking up" using *Fox v. Dish Network*—a case currently before the Ninth Circuit—as a vehicle.[22] Finally, I summarize and conclude.[23]

II. Awaiting A Chance to Shine: The Technology Is Revolutionized Already

A. The Early Days—The Advent of Television and Over-the-Air Broadcasting

To appreciate the complexities of the television industry today, it is helpful to first understand something about the history of television and the underpinning technology that has largely defined its development. Beginning with reports of the first, crude electronic television transmission in 1927 by Philo T. Farnsworth,[24] the public imagination was ignited by the idea of

20 *See infra* Part III.C.

21 *See infra* Part IV(A).

22 *See infra* Part IV(B).

23 *See infra* Part V.

24 As described in the biographical note accompanying the *Philo T. and Elma G. Farnsworth Papers*: "On 7 September 1927, [Farnsworth's employer] watched with staff members as Farnsworth slowly turned on the controls. An unmistakable line appeared across the small bluish square of light on the end of the Oscillite tube. Although fuzzy at first, it became distinct with adjustment, and through the visual static each could see the side of a black triangle previously inserted by [Farnsworth's brother-in-law], Cliff Gardner." Biographical Note, *Philo T. and Elma*

television.[25] A 1928 article in *Popular Mechanics* magazine posed a question "asked by untold millions" of people of the day: "When will radio television and radio movies be available to the average radio fan for home reception?"[26] The answer, as it turned out, was "not long." The first television drama was broadcast in 1928,[27] several experimental broadcast stations appeared between 1928 and the early 1930s,[28] and the first regular "seven-days-a-week" broadcasts began in 1931.[29] The industry was stifled significantly by the Great Depression in the 1930s and World War II in the 1940s, but it grew exponentially thereafter—by 1950, there were 3.8 million households in America with television.[30] By 1951, there were 10.3 million.[31]

G. Farnsworth Papers, SPECIAL COLLECTIONS, http://content.lib.utah.edu/cdm/ref/collection/UU_EAD/id/2160 (last visited Mar. 8, 2013).

25 *See What Television Offers You*, POPULAR MECHANICS, November 1, 1928, at 820 (*available at* http://books.google.com/books?id=wd4DAAAAMBAJ&pg=PA820#v=onepage&q&f=false).

26 *Id.* Notably, the fact that the question existed in the public consciousness did not mean that there was an easy answer available at the time. The experts of the day apparently could not agree on what was necessary for television to be sold to the mainstream, nor on the timeline it might take: "There are five different views [for how long television will take to become mainstream], ranging from right now up to ten years—and probably every one of them is correct—a paradox that arises not through disagreement, but through different interpretations." *Id.*

27 The first televised drama—"The Queen's Messenger," by J. Harley Manners—was broadcast by W2XB in New York in September 1928. *The Queen's Messenger*, EARLY TELEVISION MUSEUM, http://www.earlytelevision.org/queens_messenger.html (last visited Mar. 8, 2013). "The Queen's Messenger" was "a blood and thunder play with guns, daggers, and poison," and was such a technical challenge that more technicians were required for the production and its rudimentary special effects than actors, and only one actor's face or hands could be displayed at a time on the small television screens of the day. *Id.*

28 One early experimental broadcaster was W2XBX, the predecessor to WNBC. WIKIPEDIA, http://en.wikipedia.org/wiki/History_of_television (last visited Mar. 8, 2013).

29 *Id.*

30 Robert Shagawat, *Television Recording – The Origins and Earliest Surviving Live TV Broadcast Recordings* at 12, EARLY TELEVISION MUSEUM, http://www.earlytelevision.org/pdf/Television_Recording_Origins.pdf (last visited Mar. 8, 2013).

In these early days, a very limited amount of television content was available. NBC, CBS, ABC, and DuMont broadcast over the air for most of the nation during limited hours each day.[32] Color television followed closely behind, and further increased the demand for television sets, television broadcasts, and programming content.[33] By the end of the 1950s, the dream of the 1928 *Popular Mechanics* article was a reality: "Average" people across the nation enjoyed television on a daily basis. Television was here to stay.

B. Continuing Evolution—Technology Paradigm Shifts Over the Decades

No sooner had these millions of average people experienced television technology than they began to develop an appetite for technologies that would give them more of what they wanted when they wanted it. The evolution of television technologies that more flexibly catered to viewers began with the advent of cable and satellite television, and continued with videocassette recorders, on-demand services, and digital video recorders.

Cable television was first developed in 1948 as a method for providing television signals to users in remote areas with poor over-the-air reception.[34] Within a decade, nascent cable companies began offering cable as a vehicle for accessing new programming choices.[35] Satellite distribution of cable network signals followed another decade and a half after that in the 1960s.[36]

---

31 *Id.*

32 WIKIPEDIA, *supra* note 28.

33 *Id.*

34 National Cable & Telecommunications Association, *History of Cable Television*, http://www.ncta.com/About/About/HistoryofCableTelevision.aspx (last visited Mar. 5, 2013).

35 At first, cable broadcasters offered content only from over-the-air television stations in other cities; "cable networks" as they are today appeared later. *Id.* For example, "the first pay-TV network, Home Box Office (HBO)" was launched in 1972. *Id.*

36 *Id.*

Sixteen million households were cable subscribers by the end of the 1970s and, in response, the industry spent $15 billion between 1984 and 1992 to thoroughly "wire" America in the largest private construction project since World War II.[37] By the end of the 1980s, fifty-three million American households subscribed to cable and the number of cable networks had increased to seventy-nine.[38] Americans had spoken—they wanted more television content and they were willing to pay for it.

As cable grew in the late 1970s and the 1980s, a second trend began to develop that established Americans' hunger not only for more content on their television sets, but for more control over that content. While devices capable of recording television broadcasts had existed since the 1950s, it was during the late 1970s and early 1980s that electronics manufacturers began to mass-produce videocassette recorders ("VCRs") at a price point[39] that allowed a few consumers to begin purchasing them.[40] As VCR prices fell during the 1980s, adoption of VCRs

37 *Id.*

38 *Id.*

39 "When the studios first sued Sony in 1979, the company's Betamax [VCR] cost between $875 and $1000." Maribel Rose Hilo, Note, *TiVo and the Incentive/Dissemination Conflict: The Economics of Extending Betamax to Personal Video Recorders*, 81 WASH. U. L.Q. 1043 (2003) (citing Universal City Studios, Inc. v. Sony Corp. of America, 480 F. Supp. 429, 435 (C.D. Cal. 1979), *rev'd*, 659 F.2d 963 (9th Cir. 1981), *reaff'd*, 464 U.S. 417 (1984)). Granted, this high price was surely still prohibitive to many and may seem exorbitantly high to modern readers (especially when considering that $1000 was worth much more in 1979 than it is today, due to inflation). That demand grew while VCRs still commanded such high prices, however, only illustrates further the demand that people had for more flexible television.

40 The People History, *The Changes To Video Recorders And VCR Technology Over The Last 50 Years*, http://www.thepeoplehistory.com/vcr.html (last visited Mar. 7, 2013). The simple explanation in the text regarding the advent of VCR technology is, of course, a simplification of the actual tumult that occurred in the industry before the market selected a single technology. *See id.* For many years, various electronics companies competed for market share with VCRs (or, in many cases, machines they referred to as videotape recorders or "VTRs") utilizing different technologies, features, and tape formats. *Id.* Ultimately the "Home Video System" ("VHS")

grew rapidly because the technology offered consumers a number of significant new ways of controlling television content.

First, VCRs added a second tuner to the television cabinet, allowing viewers to record one program while they were watching something else.[41] With the purchase of a single device, the limitations of network scheduling conflicts that viewers had lived with for decades just disappeared. Suddenly, viewers did not have to choose between two prime time shows—they could watch both.[42]

Second, electronic clocks and timers built into VCRs allowed recording operations to be automated so that viewers could set the VCRs to record television programs that were scheduled for times when the viewers were not home or when the viewers had something better to do.[43] The significance of viewer's newfound ability to "time-shift" the viewing experience—to automatically record programming and watch it later—is difficult to overstate. With the same magical device, viewers suddenly became unchained from broadcasters' schedules. Viewers could watch television shows when *they* wanted to watch them.[44]

Finally, VCRs offered navigation features that acted to free viewers from constraints inherent in "live" television, at least when they were watching programming they had previously

---

format became the standard (winning over major competitors such as Betamax, which was considered by many videophiles to be the higher quality technology). *Id.*

41 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 422 (1984).

42 As the *Sony* court explains it, viewers could watch two simultaneously broadcast programs "by watching one live and recording the other for later viewing." *Id.* Significantly, this could be done even with the purchase of only one videocassette tape, since "[t]apes [could] be reused, and programs that [had] been recorded [could] be erased either before or after viewing." *Id.*

43 *Id.* at 422-23. ("Thus a person may watch a program at home in the evening even though it was broadcast while the viewer was at work during the afternoon.")

44 *See id.*

recorded. Instead of enduring long commercial breaks and portions of a program not of interest to them, viewers could navigate past unwanted material with the VCR's "fast-forward" feature.[45] Instead of missing important plot elements of a program when viewers were interrupted or needed a bathroom break, viewers could pause the program.[46] Like the second tuner and the automated recording capability of VCRs, these navigation features further shifted the paradigm for how people watched and thought about television.

With highly demanded technology in place and popularity among consumers attained, a final crucial element to the VCR's success was the Supreme Court's approval of the industry-changing technology in *Sony v. Univeral Studios*.[47] *Sony* held that recording television programs in order to "time-shift" the viewing of those programs to a time more convenient to the viewer was a copyright fair use, rather than an illegal copyright infringement.[48] This holding allowed Sony and other manufacturers to continue marketing VCRs and later television-recording devices as long such devices had "substantial non-infringing uses" such as time-shifting.[49] By extension, the holding also allowed viewers to use technology to make television convenient without fear of legal repercussions.[50] With traditional limitations out of the way, viewers began getting used to watching exactly what *they* wanted to watch, when *they* wanted to watch it.

---

45 *Sony*, 464 U.S. at 423.

46 *Id.*

47 *See id* at 456.

48 *Id.* at 454-55 ("When these factors are all weighed in the 'equitable rule of reason' balance, we must conclude that this record amply supports the District Court's conclusion that home time-shifting is fair use").

49 *Id.* at 454-56.

50 *See id.*

The commercial success and legal viability of VCRs, in combination with an exponential growth of digital computer technology and an increasing quantity of high-quality content from ever more cable networks, led to the creation of digital video recorders ("DVRs"). Introduced in the late 1990s and garnering mainstream adoption in the early 2000s, DVRs were VCRs for the digital age. Referred to as "God's Machine" by FCC chairman Michael Powell, DVRs contain all the features of VCRs, and they augment those features and add additional ones to make television even more flexible and consumer control even more comprehensive.[51] For example, while VCRs provided consumers with one extra tuner to allow them to watch one show while recording another, some modern DVRs offer three tuners and the capability to watch or record the four major broadcast networks on one tuner, making it possible to record six programs at once.[52] With all of this built on a two-terabyte hard drive capable of storing 2,000 hours of programming,[53] the situation where anyone is "conflicted out" of watching anything he or she wants to watch is becoming increasingly rare.

Further improving on the VCR, DVRs make it trivially simple to schedule recordings. Rather than fussing with setting clocks and navigating complicated interfaces to setup recording

---

51 *See* Laura Weinstein, *TiVo: The Rise of God's Machine*, WIRED, Feb. 3, 2003, http://www.wired.com/entertainment/music/news/2003/02/57505. *See also* Randal C. Picker, *The Digital Video Recorder: Unbundling Advertising and Content*, 71 U. CHI. L. REV. 205, 205-06 (2004)("The DVR is just one manifestation of the possibilities of adding intelligence and easy storage to a box in your living room. In so doing, we are changing the amount of control that can be exerted over the content on the TV screen. As the tech seers have predicted, television is changing from a synchronous medium—you watch content delivered in real time—to one in which content is captured for viewing at a later time. The VCR hints at all of this, but the DVR, which substantially reduces transaction costs relative to the VCR, may very well realize these changes").

52 Fox Broadcasting Co. v. Dish Network, L.C.C., No. CV-12-4529 DMG, 2012 WL 5938563 at *3 (C.D. Cal. Nov. 7, 2012).

53 *Id. See also* DISH NETWORK HOPPER FEATURES, http://www.dish.com/technology/receivers-dvrs/ (last visited Mar. 7, 2013).

times as was required with VCRs, DVRs allow users to easily navigate program guides and select individual programs or even series of programs to record.[54] Finally, DVRs give users supreme control over what they want to watch. Along with the VCR's capability of pausing and fast-forwarding *pre-recorded* television, DVRs add the capability to pause *live* TV and, in some cases, to skip commercials in more effortless ways than VCR fast-forward buttons ever could.[55]

Additionally, in parallel with the evolving VCR and DVR technologies, which allow viewers to control their television viewing habits with *internal* technology associated with their televisions within their homes, cable and satellite companies began offering viewers similar options to control their television experience with *external* technology.[56] Specifically, content providers began to offer opportunities for viewers to access private telecasts of premium content via "pay-per-view" events[57] and to receive "on-demand" access to other premium content or content that was previously-broadcast.[58] These offerings, growing in popularity in the 1990s and

54 Picker, *supra* note 51 at 205 ("The continuing, dramatic drop in the cost of a gigabyte of storage makes it possible to switch from clunky tapes to smooth digital storage. Plus, the DVR comes with software to make it much easier to record your favorite shows: tell it to record *Friends* forever and it will").

55 *See id.*; *Fox*, 2012 WL 5938563, at *2-4. The effortlessness of skipping commercials in modern DVRs is an important emphasis of the *Fox* case and will be described in more detail below.

56 *See, e.g.*, XFINITY ON DEMAND, http://xfinitytv.comcast.net/ondemand (last visited Mar. 9, 2013); DIRECTTV ON DEMAND, http://www.directv.com/technology/on_demand (last visited Mar. 9, 2013); WIKIPEDIA, http://en.wikipedia.org/wiki/Television_on_demand (last visited Mar. 9, 2013).

57 "Pay-per-view" events include, for example, events such as boxing matches and other fights that occur and are telecast at a particular time, but that are only accessible to those who pay for them. *See* COMCAST PAY-PER-VIEW EVENTS, http://www.comcast.com/Corporate/Programming/Comingevents.ashx (last visited Mar. 9, 2013); WIKIPEDIA, http://en.wikipedia.org/wiki/Pay-per-view (last visited Mar. 9, 2013).

58 "On demand" programming includes, for example, movies and other content not comprising live events, television programs that were recently televised, and any content that may be telecast

2000s, further illustrate the consumer demand for control and technology's ability to provide that control.

C. Today's Technology—Revolutionary and Awaiting a Chance to Shine

Finally, the advent of the Internet, with its virtually limitless capability to distribute television offerings, completes the revolution of television technology. All broadcast networks and practically all cable networks today make at least some of their content available for online streaming. This may be through their own websites,[59] through an aggregator site such as Hulu.com, or both.[60] While online streaming may be less than ideal for live and time sensitive content,[61] and while difficulty in acquiring distribution rights to demanded content has so far prevented it from reaching its full potential,[62] Internet-streamed television otherwise seems to

---

individually at any time to a particular viewer willing to pay for it. *See* XFINITY ON DEMAND, *supra* note 56; DIRECTTV ON DEMAND, *supra* note 56.

59 For example, official content-streaming websites can be found for ABC, CBS, Fox, and NBC at, respectively, http://abc.go.com/watch, http://www.cbs.com/video, http://www.fox.com/full-episodes, http://www.nbc.com/video. Many cable networks similarly provide content streaming of their programs. For example, http://tbs.com/shows provides a portal for TBS programming and http://www.usanetwork.com/fullepisodes allows content streaming from the USA Network.

60 Fully-ad-supported Hulu and its for-pay counterpart Hulu Plus, for example, together provide content from all four major networks and from many cable networks. Ryan Lawler, *CBS Finally Does a Deal with Hulu*, TECHCRUNCH (Nov. 5, 2012), http://techcrunch.com/2012/11/05/cbs-hulu/.

61 Public service, emergency, and localized content, for example, are largely absent from online streaming offerings like Hulu at present. Indeed, the on-demand, non-live nature of streaming services itself may presently inhibit such content from comprising a significant part of online streaming services. This is not to say, however, that Internet-streaming technology could not ever respond to a demand for live or local content—it is just not a current focus of the most popular streaming sites today.

62 Services such as Netflix, Amazon Instant Video, Hulu Plus, and YouTube nicely supplement the recently broadcast programs typically available on network websites and through Hulu. However, while these services provide some older television content (e.g., all episodes from all

approach a perfect model of television.[63] It is able to support any business model that enterprising businesspeople may want to attempt.[64] It promises ultimate flexibility with its potential to make available unlimited content choices.[65] And it facilitates not only limitless time-shifting,[66] but also boundless space-shifting.[67]

---

past seasons of a series) and other content (e.g., movies, user-made content, etc.), few would argue that they sufficiently provide access to everything anyone would ever want to watch. These services are making an increasingly significant dent in the content for which there is consumer demand, but there remains much room to grow as rights are acquired for movies, television back catalogs, and other content not currently available.

63 The fact that online streaming has only been available on small computer screens in the past may be another limitation that many would point to. However, this problem has also been solved with the advent of "smart TVs" and "set top boxes" which act to stream content from the Internet onto a big screen in the living room.

64 Specifically, the distribution infrastructure made possible by the Internet allows for commercial interruptions reminiscent of the traditional ad-based television model discussed in Part III infra, other ad-based methodologies (see, for example, some of the methods discussed in notes 77 and 94, infra), subscriber-based or pay-per-view models (since, unlike over-the-air broadcasting, streaming allows for convenient tracking of who is watching what), or other new models that clever entrepreneurs may dream up.

65 As discussed in note 62, *supra*, the distribution infrastructure of the Internet provides an avenue for all content to be distributed, even if much content is, for business and licensing reasons, not currently available. In other words, the technology has the potential to distribute any content to anyone at any time. The limitation is that not all content is legally available to be sent to anyone at any time.

66 The nature of web streaming is time-flexible at its core. Everything is streamed when a viewer indicates that it should be. In fact, if there is any weak spot in the streaming business model, it is that such extreme catering to viewers' schedules makes live and time-sensitive content less natural candidates for streaming distribution.

67 A huge trend toward portable viewing on shrinking screens of computers, smart phones, and tablet computers has arisen as these devices have gained prominence. Space-shifting, or "place-shifting," as it is sometimes called, refers to the ability of users to watch television anywhere that they can appropriately use these devices. This is just one more way that consumers are demanding flexibility and receiving it from technology advances. *See* PLACESHIFTING, http://www.slingbox.com/get/placeshifting (last visited Dec. 12, 2013) (providing information about place-shifting technology and how place-shifting relates to time-shifting).

The technology is revolutionized. The limits and disadvantages that came along with television in its early days have been thoroughly exterminated from the medium. But the technology is only the first part of the story, the first obstacle the revolution faces en route to a better future. Spurred by consumer demand and the conspicuous existence of the sufficient technology, the television revolution will not spare the laws and the outdated business models that still stand in its way. I now examine these next obstacles the revolution faces and speculate on their fate.

III. Preparing For Revolution: The Business is Lagging the Technology

A. Traditional Ad-Based Television—The "Stool" Model and Three Assumptions on Which it is Built

In the early days of television, a small handful of television networks controlled both the creation of all program content as well as its distribution.[68] However, the networks could not profit from television the same way they had profited from visual entertainment in years past—by charging viewers directly for the content the viewers consumed.[69] The nature of early television—electronic boxes in millions of homes undetectably receiving over-the-air broadcast signals—precluded such a direct-billed model. As much demand as existed for the content they

68 Lisa Lapan, Note, *Network Television and the Digital Threat*, 16 UCLA ENT. L. REV. 343, 345 (2009). Today, as in the early days, the "Big Four" networks that rule the airwaves and enjoy the most influence in the industry are ABC, CBS, Fox, and NBC. *Id.*

69 Jesse Haskins, *Commercial Skipping Technology and the New Market Dynamic: The Relevance of Antitrust Law to an Emerging Technology*, 2009 DUKE L. & TECH. REV. 6 (2009).

controlled,[70] the networks seemingly had no way at all to charge viewers for only the content the viewers watched, or indeed to charge *directly* for anything at all.[71] Instead, the networks were forced to employ an advertisement-based ("ad-based") model relying on at least three principal assumptions that supported and stabilized the model like the three legs of a stool: 1) Big Media produces all content, 2) Big Media distributes all content, and 3) Big Media's stranglehold on production and distribution allows it to guarantee sponsors that viewers are watching the sponsor's advertisements.

This traditional model (the "stool model"[72]) worked well for decades. As imperceptible as they were irreplaceable, the assumptions upheld the stool model and provided avenues for the

70 *See*, *Television in the 50s and 60s*, RETROWOW, http://www.retrowow.co.uk/television/television.html (last visited Mar. 1, 2013). Today, the Bureau of Labor Statistics reports that the average television viewer watches 3.51 hours of television per day. *American Time Use Survey—2011 Results* (June 22, 2012, 10:00 AM), http://www.bls.gov/news.release/atus.t01.htm. Indeed, it is easy to understand how television advertising has grown into a nearly $70 billion industry. Meg James, *TV's ad revenue stream faces crosscurrents*, L.A. TIMES (Nov. 15, 2011), http://articles.latimes.com/2011/nov/15/business/fi-ct-tv-advertising-20111115.

71 While the government may be able to tax the entire population for a common good that it provides, private interests like this burgeoning television industry enjoy no such right. Being unable to meter the usage of the millions of individual citizens, including some that did not take advantage of the invisible broadcast signals at all, the industry had to find another way to bring in revenue.

72 Throughout this Comment, I will refer to the traditional model that requires the three assumptions described herein as the "stool model" to evoke the three legs, or assumptions, on which the model stands. While other names might have been more descriptive, I steered away from them because the names might have been misleading or unhelpful. For example, an "ad-based" model, while accurate, seemed to imply that advertisements were the problem, and they certainly are not. As I will discuss, advertisements may well play an important part in the television business models of the future. Likewise, the "traditional model" or the "old model" seemed too vague. I thus settled on the "stool model" because the three assumptions—the three "legs" on which the industry has traditionally rested—are precisely what define the problematic business model that I am referring to.

television industry to evolve and grow even in the face of tumultuous cultural,[73] technological,[74] economic,[75] political, and demographic shifts in the lives of its customers.[76] The networks were happy to create content and broadcast it free-of-charge for everyone to consume. Viewers were happy to receive entertainment that only cost them their initial investment in the television equipment and the electricity to run it. Advertisers were happy to act as the glue between the networks and the consumers, making television commercially possible by paying networks to broadcast the advertisers' commercials[77] and by receiving compensatory revenue from

73 For example, the culture has shifted from earlier generations of children who had just four channels of television broadcasts available only during particular parts of the day, to the "Baby Einstein" generation of today growing up from infancy in front of all types of screens (e.g., high-definition televisions, computers, tablets, mobile phones, digital readers, portable music players, etc.) and learning to do all types of activities on them (e.g., television, movies, video games, texting, social networking, web-surfing, etc.). *See supra* note 70 and accompanying text.

74 For example, the technology has shifted from the Big Four networks being all that was available in the early days to cable, VCRs, DVRs, on-demand programming, and the web-based content of today. *See infra* Part II(B).

75 For example, economics have shifted from a world where significant portions of the population could not afford any television set and practically no one was willing to pay for more than one, *see supra* note 70, to a world where each individual in a house may be able to afford multiple different screens packed with multiple content options.

76 In spite of all of the changes discussed *supra* in notes 73-75, television has continued to grow and now offers more options in more ways to more people than it ever has. *See supra* note 70.

77 It may be noted that advertising, at times, may comprise something more than watching a traditional 30-second spot. In the early days, "consumers had little choice but to watch advertisements, each lasting sixty seconds in length. Advertisers could also pay to place their name on the title of the television program, as was the case with NBC's 'Colgate Theatre' and 'Texaco Star Theater.'" *Id.* Further, advertising has become even more creative and subtle since then with the advent of "branded entertainment" or "product placement," wherein advertisers pay to have their products conspicuously displayed and used by characters in the programming the advertisers sponsor. WIKIPEDIA, http://en.wikipedia.org/wiki/Product_placement (last visited Mar. 1, 2013).

consumers who watched those commercials and consequently bought the advertised products.[78] The model was synergy at its best—networks, advertisers, and consumers all won.

Taking a closer look at the stool model, the first leg of the stool is the assumption that Big Media alone is capable of producing quality content.[79] As with all the assumptions, this first assumption was true for decades.[80] The phrase "content is king" became a mantra in Hollywood because, while content creation is the most difficult and unpredictable aspect of television, it is simultaneously the most valuable aspect, and the aspect most immune to technological change.[81] While millions of viewers in their living rooms at home may have had ideas for the next great television concept or innovative story arc for the characters in their favorite show, the cost of production equipment was prohibitive. Professional video cameras have always been well outside of the reach of average individuals,[82] while personal video recorders only appeared in the late 1970s and began to enjoy mainstream market penetration in the 1990s and 2000s. This is not to mention the high degree of experience and expertise that were required to make any type of video until the advent of mass market movie-making software in the 2000s.

---

78 Haskins, *supra* note 69 at *6.

79 As used herein, "content" or "programming" may refer to any creative product in which media companies traffic, including television shows and movies, as well as other types of media for which there is a demand such as music, video games, books and other textual materials, computer programs, and so forth.

80 Lapan, *supra* note 68 at 346-47.

81 *Id.*

82 Even today, professional video cameras continue to be so expensive that it rarely makes sense for anyone but a major movie or television studio to own one rather than rent it. For example, high-end, high-definition cameras may cost well over $1000/day to rent and even lower-end, standard-definition video cameras cost several hundred per day. *See* BUDGET VIDEO RENTALS, http://www.budgetvideo.com (last visited March 1, 2013).

The assumption rang true and, for decades, stabilized the industry.[83] Whatever competition the networks faced from each other and from all the other activities their viewers could spend time on other than watching television, the networks never had to face competition from the millions of viewers in their living rooms with the great ideas.[84] With this monopoly on content, the industry thrived and the networks grew as they reaped the benefits of increasingly high quality, diverse, and targeted content that delivered the attention of specific groups of people, effectively if imprecisely.[85]

The second leg of the stool model that has upheld the television industry is the assumption that Big Media alone is capable of suitably distributing the content that it creates. This second assumption has also served the industry well, though it has come into question more readily than the content assumption.[86] In this case, the model relied on the fact that television could exist only insofar as it could be broadcast by powerful transmitters and large antennas affordable only to major networks and their local affiliates.[87] Or, to put it more succinctly: "[Y]ou can make the most wonderful content in the world, [but] without a commitment from a distribution outlet, you have an audience of one."[88]

---

83 *See* Lapan, *supra* note 68 at 346-47.

84 *See Id*.

85 Picker, *supra* note 51 at 205.

86 *See* Lapan, *supra* note 68 at 346-47.

87 *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd. 380 F.3d 1154, 1167 (9th Cir. 2004), *rev'd*, 545 U.S. 913 (2005) ("The introduction of new technology is always disruptive to old markets, and particularly to those copyright owners whose works are sold through well-established distribution mechanisms").

88 Haskins, *supra* note 69 at *27 n.122 (quoting Frank Rose, *The Fast-Forward, On-Demand, Network-Smashing Future of Television*, WIRED, Oct. 2003, http://www.wired.com/wired/archive/11.10/tv.html).

The truth embedded in this assumption for so many years likewise served the industry well. The networks and their affiliates not only had the content that people wanted, they had it *exclusively.* Anyone who wanted to see the latest chapter in a favorite serial television show had but one option: to mark the calendar, to get home on time, to tune in to the right network, and to stay tuned throughout the program.

The third leg of the stool is closely related to the first two legs since it arises from them. This is the assumption that Big Media would have the tools and protection it needed to maintain the other assumptions forever. Put another way, the third assumption presumes that legal and technological limits would perpetually allow Big Media to guarantee advertisers the "eyeballs" they pay for without significant adaptation of the stool model.[89] In many ways, the third leg bears more of the load than any other leg because the assumption connects the business to the bottom line.[90] At the end of the day, money is at the root of the television industry just as it is at the root of any commercial industry in a free market.[91]

89 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 446 n.28 (1984) ("The traditional method by which copyright owners capitalize upon the television medium—commercially sponsored free public broadcast over the public airwaves—is predicated upon the assumption that compensation for the value of displaying the works will be received in the form of advertising revenues").

90 Ethan O. Notkin, Note, *Television Remixed: The Controversy over Commercial-Skipping*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 899, 908 (2006) ("Since the networks' free broadcasts continue today without the collection of subscription fees or other direct charges to viewers, the sale of advertising time has become the essential source of broadcast networks' revenue").

91 Randal Picker at the University of Chicago explains that "[w]e know the place of TV in the United States: other than sleep and work, Americans spend more time watching TV than doing anything else. TV is the main source of news and information, which magnifies its importance in a democracy. TV advertising is also a $54.4 billion-per-year industry, which puts it squarely in the middle of the wheels of commerce." Picker, *supra* note 51 at 206.

B. Advantages and Disadvantages—Whether the Stool Model is Worth Keeping

The makeup of the television industry and these assumptions on which the stool model is based may have been unavoidable.[92] Be that as it may, it is worth analyzing the advantages and disadvantages of the model today, even if the limits that necessarily commanded the decisions of the past have disintegrated. Because today there is a choice. Through legal and technological means, society may *choose* to attempt to maintain old business models if old business models are determined to be best. But, if those old models are no longer working, society is not circumstantially bound to them anymore. Today, technology offers the ability to shape the future of television to whatever models are best.[93]

Accordingly, I start with an examination of some advantages of the stool model. Surely the most obvious advantage is its monetary cost to viewers. The stool model provides premium content of all types—entertainment, news, informational programming, etc.—to *everyone* for *nothing.*[94] While many people have demonstrated a willingness to pay substantial monthly

92 Indeed, there may have been few other options for television at its advent, making these types of assumptions inevitable. Patrons were easily charged an entrance admission to watch a film or a play in a theater. Music fans paid good money to purchase a record or hear a live concert. But the nature of television and radio technology, where the entirety of the product's value was broadcasted indiscriminately over public airwaves, precluded television viewers and radio listeners from being billed for what they consumed by such simplistic and traditional business models. Short of reliance on the honor system in asking viewers to pay for time they spent watching television, it is difficult to conceive of a direct way that early television broadcasters could have billed viewers directly for the content those viewers consumed. Accordingly, selling advertisers an opportunity to sponsor content and billing them was a natural, seemingly inevitable, choice.

93 Granted, there may not be any one entity with an ability to unilaterally change the model. No individual person, company, court, or even Congress is likely to be able to steer the outcome of the television revolution singlehandedly. But societies have a way of inching towards policy goals that the societies deem best. If everyone—individuals, companies, courts, and Congresses—all agree on an ideal, that ideal will become a reality eventually.

94 An advertising-weary citizen of the modern world may be forgiven for disputing the assertion that the stool model provides content for "nothing." Though out-of-pocket costs for ad-sponsored

premiums for additional content available via cable, satellite, and Internet streaming services,[95] free over-the-air television is still vital to tens of millions of Americans.[96] Even households

goods and services may indeed be zero, that is not to say that intangible costs are not still exacted. As one ad executive explains it: "We never know where the consumer is going to be at any point in time, so we have to be everywhere. Ubiquity is the new exclusivity." Louise Story, *Anywhere the Eye Can See, It's Likely to See an Ad*, N.Y. TIMES, Jan. 15, 2007, http://www.nytimes.com/2007/01/15/business/media/15everywhere.html (quoting statement from Linda Kaplan Thaler, chief executive of New York ad agency Kaplan Thaler Group). Market research firms have estimated what this ubiquity looks like: while a person in a big city of 30 years ago might come across 2,000 advertisements per day, today that person will see 5,000. *Id.* (citing an estimate by market research firm Yankelovich). In the television ad context, content-creation budgets have grown while consumer attention to ads has diminished (in part because of the technology discussed above). This has forced advertisers to saturate markets with their ads—a tactic that may ensure the message gets across but that takes a toll on the many people forced to wade through those advertisements. This is true on television and off. For example, the New York Times article gives additional examples including school buses playing advertisements aimed at children, advertisements on examination tables in 2,000 pediatricians' offices, billboards at bus stops emitting odors, billboards large and small being converted to digital screens that can display multiple and more attention-grabbing advertisements, interactive floor displays where lights respond to user movements, images projected onto buildings and sidewalks, airline-sponsored pizza boxes, and ads on dry-cleaning boxes and bags, on pills, on eggs, and the list goes on. *Id.*

95 There are several forms of directly delivered content that consumers have shown a willingness to pay for. *See infra* Part II(B). Much paid content may be subsidized by various types of advertising or, in some cases, may be ad-free. In some cases, freedom from advertising is part of what the consumer is being charged for (e.g., for a consumer upgrading from Hulu to Hulu Plus).

96 The FCC recently noted that "[f]or many people, free, over-the-air television is their primary source of news, information and emergency alerts—not to mention entertainment." Press Release, FCC, Ten Days and Counting to DTV Transition (June 2, 2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-291141A1.pdf. Specifically, there are 20.7 million American households representing 53.8 million Americans that only receive free over-the-air television. Press Release, National Association of Broadcasters, Over-the-air TV Viewership Soars to 54 Million Americans (June 18, 2012), *available at* http://www.nab.org/documents/newsroom/pressRelease.asp?id=2761. And this reliance is particularly pronounced among minority and low-income Americans. *Id.* For example, 23 percent of African American households, 26 percent of Hispanic households, and 26 percent of households with incomes under $30,000 rely on free broadcast television exclusively. *Id.*

relying primarily on paid television often watch programming developed using funding derived from the stool model.[97]

Another advantage enabled by the traditional model of television is the relationship and natural interplay between large, national networks and their local affiliates.[98] Because different advertisers strive to reach national and local audiences, and because people benefit both from programming aimed at national audiences[99] as well as programming aimed at local audiences,[100] a model is needed to connect national and local advertisers to national and local audiences and to bring those audiences both national and local programming. The stool model has provided a network-affiliate relationship that has served nicely to meet these goals. Local advertisers sponsor local programming at certain times of the day when people tend to be interested in that local programming, and national advertisers can reach national audiences at times of the day when those same people want to watch national programming. Another significant advantage to

97 Stool-model-derived programming may take many forms including broadcast television stations retransmitted by cable or satellite companies, "re-run" episodes of syndicated television shows on cable networks, streamed television programming from online sources after the programming was broadcast over the air, etc.

98 *See generally* Brief of the ABC Television Affiliates Ass'n et al. as Amici Curiae in Support of Appellants, Fox Broadcasting Co. v. Dish Network, L.C.C., No. CV-12-4529 DMG, 2012 WL 5938563 (C.D. Cal. Nov. 7, 2012) (No. 12-57048), 2012 WL 6803504.

99 For example, sponsors paying for national audiences might be required to fund high-budget entertainment programming such as sitcoms, dramas, and reality shows. Informational programming such as national and world news would also be prohibitively expensive, impractical, and redundant to produce for each small market individually.

100 Localized news, weather, and investigative reporting, might never be produced or distributed if it had to compete with programming having a national appeal. These things bring real value to Americans as studies show that local news is more highly valued and trusted than any other source of news. *See, e.g.*, Pew Research Center for the People & the Press, Further Decline in Credibility Ratings for Most News Organizations, at 2 (Aug. 16, 2012), *available at* http://www.people-press.org/files/2012/08/8-16-2012-Media-Believability1.pdf ("Since 2002, every news outlet's believability rating has suffered a double-digit drop, except for local daily newspapers and local TV news").

the cooperative relationship between national networks and local affiliates is the ability of the local affiliates to take over the airwaves and reach large majorities of the population during emergency situations.[101]

While the advantages of the seasoned stool model are numerous and important, the disadvantages are also significant. In a world where saturated marketing exposes people to 150% more advertisements per day than they were exposed to thirty years ago,[102] many people view any institution exposing them to more advertising as a bad thing.[103] Perhaps even more significant, however, is the lack of control that the stool model provides viewers. Television viewers in the new millennium demand control over their media and they typically get it.[104] While new models of television provide time-shifted, space-shifted, on-demand, and even interactive programming,[105] the stool model requires viewers to be in their seat when broadcasters tell them to be. It requires viewers to watch what broadcasters tell them to watch. It requires[106] viewers to stay put while commercials—in many cases commercials irrelevant to the

101 *See* Brief of the ABC Television Affiliates Ass'n et al. as Amici Curiae in Support of Appellants, *supra* note 98, at *10-11 (discussing the role played by emergency broadcasts during Hurricane Sandy and quoting the FCC and FEMA's direction to the public to "[tune] into your local television or radio stations . . . for important news alerts").

102 While the average American was exposed to 2,000 advertisements per day thirty years ago, that person is exposed to 5,000 ads per day now. *See* Story, s*upra* note 94.

103 *See id.*

104 Consumer control arises, at least in part, from the advent of computers and the Internet in the last part of the Twentieth Century. Unlike television and technology from its era, the Internet functioned as an individualized, unicast medium from the beginning. The Internet eschews the very concept of "broadcasting" in favor of individual control—users requests information they want on their terms and that information is delivered.

105 *See infra* Part II(C).

106 Technically, users may not be *required* to stay put during commercials, although the networks and advertisers would greatly prefer it. As Jamie Kellner, then head of Turner

viewers or which they have seen so many times as to have practically memorized them[107]—are shown. Everything is done on the *broadcaster's* timetable, on the *broadcaster's* terms. The significance of this disadvantage in the modern world is difficult to overstate. As numerous and significant as the advantages of the traditional model are, these disadvantages overshadow and outweigh them significantly for many. Viewers today want TV on *their* terms.

C. The Stool Today—Technology's Devastation of the Three Legs and the Failure of the Business to Innovate

Today, the ground under each of the three traditional assumptions is shaky and getting shakier. Pressure put on the television industry by shifts in consumer demand and advances in technology have stressed each assumption to its limits. Indeed, as stable as the "stool" has been over the decades, today it seems poised to collapse under the weight of the rapidly transforming industry.

The first leg of the stool—the assumption that viewers are only willing to watch content produced with Big Media's resources—has clearly been weakened by the advent of the Internet and social networking. Quality content is cheaper than ever before to produce with today's

---

Broadcasting Systems, infamously asserted: "Your contract with the network when you get the show is you're going to watch the spots. Otherwise you couldn't get the show on an ad-supported basis. Any time you skip a commercial . . . you're actually *stealing* the programming." Interview of Jamie Kellner, in Staci D. Kramer, *Content's King*, CABLE WORLD 32 (Apr 29, 2002). To be fair, Kellner did begrudgingly allow, when pressed on the extremeness of this assertion, that "I guess there's a certain amount of tolerance for going to the bathroom." *Id.* Honest bathroom-goers everywhere may take a sigh of relief.

107 *See* Picker, *supra* note 51 at 205 ("Next time you turn on your television, actually watch the commercials and you will quickly see how poorly the economic model of TV is working. They put on a commercial for dog food, but you are allergic to dogs, a commercial for diapers, but, mercifully, your kids are old enough that you no longer need to decide whether Pampers are better than Huggies. Many of the commercials are for product categories that you do not purchase; others are for products, such as cars or computers, that you use constantly but purchase only sporadically. Most ads are targeted at no more than the broad side of the barn: Adults 18-49 or Women 25-54 or some other rough demographic segment").

technology.[108] Moore's law has provided powerful computers to the masses at prices that everyone can afford.[109] Affordable movie-making software runs on these computers, and inexpensive videography hardware further levels the playing field. Because of technology, average people no longer have to sit on the couch and watch content other people have made. More than ever before, a new option to grab a camera and a couple friends and to make a movie is presenting itself. And people are beginning to choose this option.[110] What is more, while most of this user-produced content still falls far short of the production standards that Big Media has consistently used, this content has proven capable of finding audiences,[111] and, in some cases, very significant audiences.[112]

---

108 For example, while "it wasn't until the late 80's that camcorders dipped below $1000," bohus, *1980's Toshiba IK-1850 Camera Teaches Today's Camcorders A Thing Or Two*, RETRO THING, http://www.retrothing.com/2008/11/before-camcorde.html (last visited Mar. 23, 2013), today, video cameras are available on cellphones, tablets, and other devices that have come to find themselves accompanying most people most of the time. Even if a person did not have access to a video camera on a device he or she already owned, cheap, personal video cameras are available for well under $50. *E.g.*, Cobra DVC955 Digital Video Camcorder, Black, STAPLES, http://www.staples.com/DVC955/directory_DVC955? (last visited Mar. 23, 2013) (listing portable video camera on a clearance sale for $19.90).

109 Named after Intel Corporation executive Gordon Moore, Moore's law refers to the observation, first described in a 1965 paper by Moore, that "over the history of computing hardware, the number of transistors on integrated circuits doubles approximately every two years." WIKIPEDIA, http://en.wikipedia.org/wiki/Moore's_law (last visited Mar. 23, 2013). Of course, as the number of transistors on a chip increases, those transistors get smaller, faster, and more tightly packed together. This has led to an exponential growth in computing power since the 1970s even as prices for computers have dramatically dropped. *See id.*

110 *See* Ben Rubenstein, *How to Make a Movie*, WIKIHOW, http://www.wikihow.com/Make-a-Movie (last visited Mar. 23, 2013) (presenting how-to steps "liked" and contributed to by hundreds of people for creating a movie aimed at hobbyists with simple equipment). *See also* YOUTUBE, http://www.youtube.com (last visited Mar. 23, 2013) (exhibiting millions of examples of such amateur moviemaking).

111 Indeed, the premise of Chris Anderson's book *The Long Tail* is that, while consumer demand has traditionally been for popular "hits" under the middle of a bell curve of popularity, the Internet has greatly enabled exploration of the "long tail" of that bell curve. *See generally*

The second leg of the stool—the assumption that Big Media has to distribute content for it to reach significant audiences—has also been undermined by cheap computers[113] and the advent of widespread broadband Internet access.[114] YouTube, in particular, has emerged as an extremely popular vehicle by which user-generated content can be stored and distributed.[115] Along with social networking websites, set-top boxes capable of streaming YouTube videos

---

ANDERSON, *supra* note 10. The Internet allows for easy distribution of content even if that content is only of interest to a very small, disparate audience. *Id.*

112 The number of views on the most popular YouTube videos, in fact, dwarfs the ratings of even the most popular television events. For example, while Nielsen Ratings reports average Super Bowl viewership in recent years to have been slightly above 100 million viewers, *see* NIELSON, *Super Bowl XLVII: How We Watch and Connect Across Screens* (Feb. 5, 2013), http://www.nielsen.com/us/en/newswire/2013/super-bowl-xlvii-draws-108-7-million-viewers-26-1-tweets.html, top YouTube videos have received views in the billions. Richard MacManus, *Top 10 YouTube Videos of All Time*, READWRITE (September 2, 2012), http://readwrite.com/2012/09/02/top_10_youtube_videos_of_all_time (recognizing PSY's "Gangham Style" music video as the top-viewed YouTube video of all time with 1.25 billion views). Indeed, even very amateur videos that strike a strong chord with viewers on YouTube have been rewarded with views in the hundred of millions. *See id.* (recognizing amateur video "Charlie Bit My Finger – Again!" as having over 510 million views).

113 Of course, along with what might be traditionally considered a "computer," I also include here the many new computing devices with which people access the Internet—smart phones, tablets, digital readers, etc.

114 Broadband Internet access has grown rapidly for in the last decade as dial-up Internet has decreased at about the same rate. Lance Whitney, *Broadband Growth Slows in the U.S.*, C|NET (Aug. 12, 2010, 9:13 AM), http://news.cnet.com/8301-1023_3-20013438-93.html. Though it appears that growth may be slowing as a saturation point is approached, over 66% of American adults now have access to broadband Internet, as compared to just 5% who still use dial-up. *Id.*

115 Founded in February 2005 after two founders had trouble sharing a video of themselves a dinner party that the third founder did not believe had occurred, YouTube was later bought by Google and rose to prominence by "allow[ing] billions of people to discover, watch and share originally-created videos. YouTube provides a forum for people to connect, inform, and inspire others across the globe and acts as a distribution platform for original content creators and advertisers large and small." YOUTUBE, *About YouTube*, http://www.youtube.com/t/about_youtube (last visited Mar. 23, 2013); WIKIPEDIA, http://en.wikipedia.org/wiki/Youtube (last visited Mar. 23, 2013).

straight to televisions in the living room,[116] and online communities fostering "viral videos" and other Internet memes,[117] YouTube and similar sites have proven that the Internet is fully capable distributing high-bandwidth content from one ordinary person to any number of other people interested in it.[118] Big Media and its networks of television antennas, cables, and satellites are not needed.[119]

---

116 Many devices capable of streaming YouTube videos to a big screen are now commonly found in the living room entertainment center: video games systems, DVD and Blu-Ray players, DVRs, other set-top boxes such as Roku and AppleTV, etc.

117 "An Internet meme is a concept that spreads from person to person via the Internet. . . . Fads and sensations tend to grow rapidly on the Internet, because the instant communication facilitates word of mouth transmission." WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_meme (last visited Mar. 23, 2013). Viral videos such as the "Charlie Bit My Finger" series are one example of an Internet meme. *See* MacManus, *supra* note 112.

118 This ease of distribution is memorably illustrated by an anecdote given in the Shirky article:

> Back in 1993, the Knight-Ridder newspaper chain began investigating piracy of Dave Barry's popular column, which was published by the Miami Herald and syndicated widely. In the course of tracking down the sources of unlicensed distribution, they found many things, including the copying of his column to alt.fan.dave_barry on usenet; a 2000-person strong mailing list also reading pirated versions; and a teenager in the Midwest who was doing some of the copying himself, because he loved Barry's work so much he wanted everybody to be able to read it.
>
> One of the people I was hanging around with online back then was Gordy Thompson, who managed internet services at the New York Times. I remember Thompson saying something to the effect of "When a 14 year old kid can blow up your business in his spare time, not because he hates you but because he loves you, then you got a problem." I think about that conversation a lot these days.

Shirky, *supra* note 9.

119 Admittedly, many companies that fall under the "Big Media" label defined in this Comment are the same companies that provide Internet access. Insofar as that Internet side of its business is implicated, Big Media will of course continue to be very relevant. It is only the legacy, stool-model media channels offered by Big Media companies, not necessarily the companies themselves, that I contend are losing their relevance.

With the impending failure of the first two legs of the stool, the third leg—the assumption that the other legs are stable enough to guarantee eyeballs for advertisers—is failing and doomed to fail as well. As viewers increasingly become siphoned off from watching traditional content through traditional channels, advertisers are forced to follow them—to innovate and move their money to the avenues where viewers are found.[120] And, what is more, no one seems to care. [121] As the established model that has been relied on for decades crumbles, television viewers are enthusiastically embracing new television models and purveyors of those models are reporting notable profits.[122] And, perhaps even more telling, a trend to use online-streaming models *exclusively* is growing as well.[123] While the advantages of the traditional model are significant,

120 For example, as viewership increases, YouTube is experimenting with new advertising models. *See* David Hancock, *Google Adds Commercials To YouTube Videos* (Feb. 11, 2009, 4:21 PM) http://www.cbsnews.com/8301-501203_162-3193449.html. *See also supra* text accompanying note 94 (discussing many of the other creative avenues advertisers have taken advantage of in an effort to follow viewers).

121 Surely, a recognition of this instability has caused great concern amongst the Big Media crowd and those financially tied to the success of the stool model, but the growing number of people who are "cutting the cable" and embracing online and other non-traditional televisions business models suggests that television viewers in the population at large stand ready to usher out the old and welcome new models. *See, e.g.*, Paul Bond, *Hulu Reports 65 Percent Revenue Growth in 2012*, THE HOLLYWOOD REPORTER (Dec. 17, 2012, 12:42 PM), http://www.hollywoodreporter.com/news/hulu-reports-65-percent-revenue-403362 (reporting 2012 year-end figures for Hulu, a company representative of the migration of viewers to online media, including Hulu's surging revenues—they quadrupled from $100 million to $400 million from 2009 to 2011—and the rapid growth of its subscriber base, content library, and advertising partners).

122 *Id.*

123 The trend to reject the stool model is exemplified by a movement to "cut the cord"—that is, to do away with the high fees of cable and satellite providers. According to one survey, nearly one tenth of Americans had "cut the cord" by 2011. Mike Flacy, *Survey: Nearly One Tenth of Americans Have "Cut the Cord" from Premium TV*, DIGITAL TRENDS (January 5, 2012), http://www.digitaltrends.com/home-theater/survey-nearly-one-tenth-of-americans-have-cut-the-cord-from-premium-tv (hereinafter "Cut the Cord Survey"). While people cutting the cord may not necessarily cut out all types of television incorporated in the stool model—for example, they may still receive over-the-air broadcasts from the major networks—the emphasis of cutting the

reluctance to lose them has not impeded the growth of the number of people willing to look beyond the traditional model and even desert it completely.[124]

In summary, the traditional stool model was extremely useful, and probably inevitable, for the first several decades of television. But it has served its purpose. While it offers some advantages even to modern viewers, the disadvantages of the model are far too great and the alternatives too enticing. Accordingly, the model is not merely unworthy of continued protection, but it is already on its way out the door. The assumptions that have upheld the model no longer ring true in the world of ubiquitous Internet access and cheap, portable screens. Advertisers are looking for more value than the model can offer them. In short, "the old stuff [is getting] broken faster than the new stuff is put in its place."[125] The revolution is happening, and, at least from the point of view of the stool model's advocates, things are going to get worse before they get better.

IV. Facilitating the Revolution: The Law Can Help Synchronize the Business and the Technology

A. The "Shake-It-Up Policy"—Rather Than Coddle Outmoded Business Models, the Law Should Encourage Innovation

With the reality of the television revolution as a backdrop, I consider a final question: What can the law do to help?

---

cord is a reliance on online content and modern technology such as that discussed above. *See*, Mike Flacy, *Cord Cutting 101: Four Easy Steps to Cut the Cord*, DIGITAL TRENDS (Jan. 2, 2013), http://www.digitaltrends.com/home-theater/cord-cutting-four-steps-to-cut-the-cord/.

124 *See* Flacy, *Cut the Cord Survey*, *supra* note 123.

125 Shirky, *supra* note 9.

It is not typically the place of the law to dictate or even influence the business models of companies in an industry of free enterprise.[126] Yet even in a capitalist economy such as that of the United States, nearly all industries are governed to at least some degree by the legal and regulatory environment in which they are built. Thus, even if the television industry has many hallmarks of free enterprise,[127] it is still driven both directly and indirectly by laws and policies that the government has built around it over the years.

For example, FCC regulations prohibiting obscene and indecent material[128] directly shape the way broadcast networks do business. The relative success of entertainment content embodying obscene and indecent material produced by entities not governed by these FCC regulations illustrates that there is a tolerance and often a demand for entertainment with such material.[129] Yet, due to these government regulations, broadcast television directors creatively cut away from obscene or indecent scenes to imply rather than show them while broadcast

126 The essence of the free enterprise characterizing capitalist societies is that business is "governed by the laws of supply and demand, not restrained by government interference, regulation, or subsidy." INVESTER WORDS, http://www.investorwords.com/2085/free_enterprise.html (last visited Mar. 23, 2013) (giving a dictionary definition of "free enterprise").

127 Unlike many other countries where governments own and operate television stations (e.g., the largest broadcaster in the world, the British Broadcasting System, is owned by The Crown), the American television industry is characterized by independent networks with independent affiliates all competing for a maximum share of the industry's currency—viewer attention to sell to advertisers.

128 47 C.F.R. § 73.3999 (2005) ("No licensee of a radio or television broadcast station shall broadcast any material which is obscene. . . . No licensee of a radio or television broadcast station shall broadcast on any day between 6 a.m. and 10 p.m. any material which is indecent").

129 *See* Todd Cunningham, *Glut of R-Rated Movies Putting Box Office on Overload*, THE WRAP (Jan. 30, 2013, 4:27 PM), http://movies.yahoo.com/news/glut-r-rated-movies-putting-box-office-overload-212714468.html.

television writers stretch their dialog in an attempt to make speech sound natural without the profanity that many of their characters might otherwise be expected to employ.[130]

Additionally, law also affects otherwise-"free" enterprise in less direct ways. For example, federal copyright laws[131] govern content distribution indirectly but to an enormous extent. Indeed, the entire entertainment industry is based on copyright law—if the three assumptions I have identified are the legs of the stool, copyright law might well be the floor on which the stool stands. Without copyright laws dictating that each network only distribute programming that, at great cost, it creates or licenses, every network may be expected to make drastic changes its programming schedule overnight.[132]

Accordingly, it is clear that law is very capable of *directing* an industry toward desirable behavior even without *forcing* such behavior. Just as copyright law provides an environment wherein a television industry can freely innovate and creatively chase the promise of capitalistic awards while simultaneously being encouraged and empowered to undergo the costly development of original content, the rule of law is similarly capable of directing old business

130 For a discussion among writers of how to deal with this issue, *see, e.g.*, WRITING FORUMS, *Thread: Swearing - can I get away without swearing?*, http://www.writingforums.org/showthread.php?t=59908 (last visited Mar. 23, 2013).

131 *See* Title 17 of the United States Code.

132 Of course, while the prospect of high-demand, premium content always being available on 100+ cable channels coming into the house seems like a good thing at the outset, the corollary to it is of course that there would be little incentive or capital with which to continue developing new quality content. As illustrated above in the context of user-generated content on YouTube, this does not necessarily mean that there would be *no* content worth watching. But few would dispute that an absence of copyright law would be accompanied by a significant detrimental effect on available content. *See generally* Sumner M. Redstone, Chairman and Founder, Viacom Inc. and CBS Corp., Copyright is Even More Right in the Digital Age (Aug. 22, 2006), *available at* http://www.pff.org/issues-pubs/pops/pop13.21_sumner_speech.pdf (rebutting anti-copyright arguments to show that strong intellectual property laws are more crucial in the digital age than ever).

models out and ushering new ones in. The challenge is in the identification of the new models worthy of encouragement and, then, in maintaining the balance between spurring these policy goals while leaving the business enterprise as "free" as possible.

I do not purport to know which new business models will be ideal in the post-revolution television industry. Indeed, beyond illustrating that other models exist and that they are already arising and starting to attain some degree of success,[133] I will not speculate at all on which direction television *should* go in the future or which business models *should* be encouraged. Indeed, my position is that *no one* can purport to know the future from the mid-revolution position vantage of the industry we currently have.[134] Rather, I merely assert that the traditional business models, and the stool model in particular, have largely reached the end of their usefulness, that new experiments can and are being carried out, and that the law should enable such experimentation.[135]

---

133 *See, e.g.*, *supra* Part II(C).

134 *See* Shirky, *supra* note 9 (discussing the arbitrariness of historical revolutions and the unpredictability of which experiments will stick and which will be rendered irrelevant: "During the wrenching transition to print, experiments were only revealed in retrospect to be turning points. . . .The importance of any given experiment isn't apparent at the moment it appears; big changes stall, small changes spread. Even the revolutionaries can't predict what will happen").

135 Though I do not support any single experiment above another or pretend to know which ones will prove successful, I do think it appropriate that I mention a few examples of the types of experimental business models to which I am referring. Some are currently being carried out while others may be carried out in the coming years. These examples include: subscription based models like Netflix and HuluPlus, dual revenue models that couple subscriptions with ad-based sponsorship, inbound advertising models comprising commercials people watch by choice, less disruptive advertising such as banners and product placement, hyper-personalized advertising allowing fewer commercials to be much more effective, state sponsored television like the BBC, donation-based television like PBS, more limited versions of the stool model for areas such as live sports and news where the three assumptions may still stand, any combination of the above, and many other models that neither I nor anyone else have yet thought of. Some of these business models may change the world while others may be complete failures. The point is that the law should help create an environment where all may be tested and tried. The essence of my thesis and the end result of the revolution is that if the law enables these experiments to be

A public policy naturally arises from my assertion that old models have run their course and that new models should be encouraged. I will refer to it as the "shake-it-up" policy. That is, while it would be a mistake for the law to force or even favor a particular business model for the future of television, the law may facilitate the television revolution by encouraging experimentation with new models. The law can help by making it as easy as possible for the industry to "shake it up," to sort out the disparity between the old business and the new technology, and to find a new status quo that will work for the coming decades. Of course, the policy has boundaries within which it is most likely to succeed. For example, no business model ought to be encouraged until there is good reason to believe that it is actually working,[136] and even then the law should only favor the merits of the business model insofar as they benefit the public.[137] But, within these boundaries, the law will best serve the public by helping the industry to shake it up and sort out the business/technology tensions that exist within it.

Make no mistake. The television revolution is unavoidable. Old, ineffective business models will continue to crumble while newer ones continue to encroach and find success no matter what the law does within reason. But the shake-it-up policy will speed the revolution along, and that is a good thing. The wisdom in comedian Jerry Seinfeld's suggestion for

---

conducted, something will eventually work. A model that begins as an experiment will ultimately reinvent television and, unlike the stool model, it will do so in a way that does not arbitrarily limit technology.

136 Determining what is "working" is, of course, a challenge in and of itself. Though the details of what might characterize a "working" model fall largely outside the scope of this Comment, a business model may be considered to be "working" if it does at least two things: 1) The business model respects and deals with copyrights so as to promote and enable the development of new, high-quality content, and 2) The business model does this without arbitrarily placing significant limits on what technology is allowed to do.

137 In other words, attainment of enormous financial benefits by leaders of the industry, while acceptable, should not in itself be considered a criterion of the success of the industry. The central question must only be how successful the industry is at serving the needs of the public.

minimizing the awkwardness arising from breaking off a relationship—"[J]ust do it like a Band-Aid. One motion, right off!"[138]—is very applicable to the television revolution. The sooner the television industry is "shaken up"—the sooner that old models lose their stranglehold to allow new experiments to flourish on their merits—the less painful the revolution will be for everyone,[139] and the sooner everyone will be able to enjoy the revolution's considerable benefits.[140]

B. An Illustrative Example—*Fox v. Dish Network*

Even if the shake-it-up policy makes sense in theory, a practical element remains for our consideration. What should the shake-it-up policy actually look like in practice? To address this, I first note that, while the shake-it-up policy might well be applied by lawmakers and policy-

138 *Seinfeld: The Ex-Girlfriend*, (NBC television broadcast Jan. 23, 1991), *available at* http://www.pkmeco.com/seinfeld/exgirl.htm.

139 Surely many industry leaders relying on the stool model would dispute the overarching term "everyone" as it is used here. However, while a literal interpretation of "everyone" may overstate the case somewhat, there is good historical evidence that even many defenders of the status quo will ultimately benefit from an upending of that status quo if it enables the industry to be restructured more sensibly. Mark A. Lemley, William H. Neukom Professor of Law at Stanford Law School, gives a speech in which he identifies numerous historical instances in which industries seemingly threatened by new technologies actually came away from rough patches stronger than ever, thanks to the technology. Mark A. Lemley, *Is the Sky Falling on the Content Industries?*, 9 J. TELECOMM. & HIGH TECH. L. 125 (2011). Among the examples Lemley includes are the artists threatened by photography which would render painting obsolete, the musicians threatened by the player piano and gramophone which would render live performances of music unnecessary, the music industry threatened by the advent of free radio which would eliminate the public's willingness to pay for music, the publishing industry threatened by the photocopier which would eliminate any need for published books, and the video content industry threatened by the VCR which would devastate the media content markets. *Id.* Of course, in all of these cases, the "threats" not only turned out to be overrated, but, in many cases, the industries were significantly bolstered by the threats in the end. *Id.* For example, the VCR did not hurt content producers but, rather, made possible the entire video market, which has become an extremely important part of the total content market that these producers serve. *Id.* Thus, it is not always just the consumers who benefit from technological revolutions, but often the companies within the industries as well. *See id.*

140 *See supra* Part II(C).

shapers in all branches of government, the judicial branch seems to be uniquely situated to promote the policy. This is because, of the three branches of government, the judicial branch is uniquely insulated from political concerns[141] and dedicated to nonpartisanship.[142] There is no doubt that money talks and that established industries wield influence as to every branch of government, but, while powerful lobbies and "revolving door" politics[143] may help protect entrenched parties from sweeping statutory and regulatory changes, the judiciary is more insulated from such politics. The judiciary is positioned to promote ideal public policy without regard for the demands of campaign donors, the consequences of upsetting special interest groups, or the threat of unemployment due to the discontentment of a constituency.

---

141 Unlike the President in the executive branch and members of Congress in the legislative branch, judges are given life terms "during good Behaviour," U.S. Const. art. III, § 1, and are appointed and confirmed rather than directly elected, *see* U.S. Const. art. II, § 2, cl. 2.

142 Indeed, the Supreme Court's legitimacy derives primarily through the public's perception of how well it maintains neutrality and fairly promotes justice. The judicial branch is not constitutionally endowed with power to the same degree that the executive and legislative branches are. In fact, the Court's most significant power today, "the notion of judicial review[,] was far from resolved during the first years of the republic. . . . [W]ith its undefined powers and lack of real leadership, the judicial branch was largely viewed as the junior partner among the three branches. That would soon change, however, with John Marshall's appointment by John Adams in 1801 [and Marshall's subsequent reforming of the way the Court operated and his important *Marbury v. Madison* decision implementing the power of judicial constitutional review]." Scott Regan, *The Great Decision: Jefferson, Adams, Marshall, and the Battle for the Supreme Court By Cliff Sloan and David McKean*, 83-MAY FL. B.J. 62 (2009) (book review). Though the political neutrality of the Supreme Court has increasingly come under scrutiny, the Supreme Court is at least sensitive to this issue. *See* Chief Justice Roberts, *2011 Year-End Report on the Federal Judiciary* (2011), *available at* http://www.supremecourt.gov/publicinfo/year-end/2011year-endreport.pdf (discussing the Court's self-imposed code of conduct and the importance of recusal when an appearance of neutrality is threatened).

143 "Revolving door politics" refers to the tendency for important players in high levels of government and industry to move between the state and private sectors and the problems it can pose for the public as incentives and allegiances become misaligned and "regulatory capture" occurs. WIKIPEDIA, http://en.wikipedia.org/wiki/Revolving_door_(politics) (last visited Mar. 25, 2013).

Accordingly, I examine a case currently before the judiciary to illustrate how decisions might immediately be made to further the aims of the shake-it-up policy and to thereby facilitate the television revolution. *Fox v. Dish Network*,[144] a case currently before the Ninth Circuit, serves as an example of a prime opportunity that courts currently have to choose to protect entrenched, ineffective business models, or to choose to "shake it up" and help the accelerate the revolution.

Fox brought a preliminary injunction action to enjoin Dish Network's PrimeTime Any Time ("PTAT") and "Auto Hop" technologies.[145] Fox's problem with these technologies is simple. The "Hopper"— a special DVR offered by Dish Network which embodies the PTAT and Auto Hop features that Fox opposes—allows users, as do most modern DVRs, to fast forward commercials,[146] to skip predetermined lengths of time, and to effortlessly select programming to record.[147] But the Hopper doesn't stop there. The Auto Hop feature goes beyond *automatic* commercial removal—the unspoken "line in the sand" that had implicitly existed in the tense

144 Fox Broadcasting Co. v. Dish Network, L.C.C., No. CV-12-4529 DMG, 2012 WL 5938563 (C.D. Cal. Nov. 7, 2012).

145 *Id*. at *1.

146 There seems to be little doubt after *Sony Corp. of Am. v. Universal City Studios, Inc.* that recording television broadcasts in order to "time-shift" the programs and watch them later is a copyright fair use. 464 U.S. 417, 447-56 (1984) ("it supports an interpretation of the concept of 'fair use' that requires the copyright holder to demonstrate some likelihood of harm before he may condemn a private act of time-shifting as a violation of federal law"). Once time-shifted, broadcasters may prefer that users keep their eyes glued to entire broadcasts, advertisements and all, *see* Kramer, *supra* note 106, but using the fast forward operation of the VCR has not been considered illegal. *See also infra* text accompanying note 148.

147 *See Fox*, 2012 WL 5938563, at *2-4. *See also* DISH NETWORK HOPPER FEATURES, *supra* note 53.

industry since the advent of the DVR[148]—to essentially provide a *manual* commercial removal service,[149] while the PTAT feature allows effortless recording of both programming *selected* by the user and programming that the user had *not* selected or even necessarily heard of.[150]

148 After "the networks' attempt to thwart the DVR's cousin, the videocassette recorder ("VCR"),

failed miserably in *Sony*," the networks proceeded cautiously in their litigation efforts to "curb the outer boundaries of DVR technology." Ned Snow, *The TiVo Question: Does Skipping Commercials Violate Copyright Law?*, 56 SYRACUSE L. REV. 27, 29 (2005). Specifically, they focused their energy toward defending a new line in the sand—that technology not allow commercials to be removed from recordings completely. Notkin, *supra* note 90 at 913-14. Notkin describes the line in the sand between fast-forwarding and automatically skipping commercials (embodied in a feature called "AutoSkip" that was offered by SONICblue in its ReplayTV DVR in the early 2000s):

> One might wonder why the media and broadcast companies sued SONICblue over AutoSkip when [competing DVR, TiVo,] also features a fast-forward button that allows commercials to be skipped over. The difference here was that ReplayTV's AutoSkip feature automatically deleted the commercials, so that viewers could not scan commercials at high speed like they do with TiVo. As a result, ReplayTV users would not even be aware of who is advertising during a program, preventing them from rewinding and viewing a commercial that might be relevant to them.
>
> In addition, the plaintiffs may also have been taking advantage of an opening proposed by the district court in Sony—that commercial-skipping in VCRs was "too tedious" an activity to truly pose a threat. By stressing that AutoSkip was a vastly easier way to allegedly infringe on programs, the plaintiffs sought to further differentiate their claims from the technology in Sony.

Id. Further, as it turns out, there is actually empirical evidence supporting this distinction between commercials flashing by and being removed completely. One study goes so far as to suggest that viewers actually get *more* out of advertising when they focus on it flashing by as they attempt to fast-forward through a commercial break without going too far. *See* Elizabeth A. Thomas, *Pilot Study: Measuring Uses and Gratifications of Digital Video Recorders in Modern Television Viewing*, 2 J. MASS COMM. & JOURNALISM 109 (2012) ("In the process of fast-forwarding, viewers must pay attention to passing images and are capable of not only recognizing advertisements but altering their viewing to incorporate DVR use. . . . Visual cues within advertising are often provocative enough to

The significance of these technological innovations must not be underestimated. While some may argue that Fox's injury is more imagined than real,[151] most would agree that Fox's claim for injury is legitimate. This time, it really hurts.[152] First, there is the shift from *automated* commercial removal to the *manual* ad-removal service offered by the Auto Hop feature. While automatic commercial removal has certainly proven to be a thorn in the side of the stool model,

---

stimulate action – stopping viewers from fast-forwarding through ads. Still, the idea persists that when viewers do fast-forward through television advertisements, the ads have a reduced effectiveness. This broad assumption ignores the fact the DVR owners report watching more television, using their DVRs for the primary benefit of time shifting – and not fast-forwarding through advertising. The central motivation for using DVR technology is the ability to watch programming at convenient times. In attempting to avoid advertising, most viewers do, in fact, pay attention to their TV screens. Doing so may result in viewers inadvertently paying even more attention to advertising messages").

149 *Fox*, 2012 WL 5938563, at *4 ("A technician views the recording, fast-forwarding through the program itself to the commercial breaks, to ensure that the marking announcement is accurate and no portion of the program is cut-off").

150 PTAT records what Dish Network configures it to record once the viewer merely turns it on. While users may choose to manually opt out of recording certain programming, "the default settings cause the Hopper to record the *entire primetime window* on all four of the major networks, including Fox, every day of the week." *Id.* at *3 (emphasis added).

151 *See*, *e.g.*, Brief of Law Scholars and Professors as Amici Curiae in Support of Defendants-Appellees at 33, *Fox*, WL 5938563 (2012) (No. 12-57048), 2013 WL 431699 (arguing that "[t]he fears raised by the copyright holders in *Sony* and echoed by Fox in this case are as unfounded today as they were then."); Lemley, *supra* note 139.

152 *See*, *e.g.*, Brief for Amicus Curiae Nat'l Ass'n of Broadcasters in Support of Appellants at 6, *Fox*, WL 5938563 (2012) (No. 12-57048), 2012 WL 6803505 (arguing that "[i]f not enjoined, the AutoHop service will cause irreparable injury to local broadcasters' ability to continue delivering valuable local and network programming to viewers free of charge. If advertising spots in broadcast programming—particularly the most popular network primetime programming—cannot reach viewers, broadcast programs will lose their value to advertisers, who will move their ads to competing platforms. Broadcasters, in turn, will have fewer financial resources to invest in producing and acquiring expensive local and network programming, including local news and critical emergency information. *Taken to its logical end, ad-stripped television could spell the end of free, over-the-air broadcast television and the important public interests it serves.*") (emphasis added); Brief of the ABC Television Affiliates Ass'n et al. as Amici Curiae in Support of Appellants, *supra* note 98 (arguing similar themes).

at least it was prone to error and was equally harmful to all of the networks. It had its upsides.[153] Dish Network's Auto Hop service, on the other hand, works differently. With Auto Hop, commercials from networks that Dish Network selects are manually analyzed by technicians to create a software filter that, uploaded to users' Hopper devices, enables virtually perfect commercial skipping.[154] This threatens both to be more effective[155] and more prone to unfair competition[156] than anything the industry has yet faced.

Next, PTAT effectively offers users a free service that is almost indistinguishable from a service that would otherwise cost money. That is, with a one time flip of a software setting on the Hopper device, users can direct the Hopper to record *all* primetime programming[157] from Dish-

153 *See* Thomas, *supra* note 148 at Abstract.

154 *Fox*, 2012 WL 5938563, at *4.

155 *See supra* text accompanying note 148.

156 Amici for Fox argue that the unbalanced targeting of the major broadcast networks as the only networks to bear Dish Network's commercial removal creates an anticompetitive scenario. *See* Brief of the ABC Television Affiliates Ass'n et al. as Amici Curiae in Support of Appellants, *supra* note 98, at *3 ("It inflicts this harm, moreover, on a *discriminatory and anticompetitive* basis, targeting the most popular programming on the channels most dependent on advertising.") (emphasis added); Brief for Amicus Curiae National Association of Broadcasters in Support of Appellants, *supra* note 152, at *3 ("Dish Network's PrimeTime Anytime with AutoHop . . . strips every advertisement from network affiliates' copyrighted primetime programming streams *but, tellingly, not from competing primetime cable programming streams*.") (emphasis added).

157 *See supra* text accompanying note 150. Importantly, what the Hopper considers "primetime" is also determined solely at Dish Network's discretion. As the case explains, "Dish determines the start- and end-time of the primetime block each night and, for certain types of programming, may alter the total length of the PTAT

recording." *Fox*, 2012 WL 5938563, at *3. The Court further notes that Dish Network has taken advantage of this sole discretion to ensure that the very best content will be available to its users: "For example, during the Olympics in July and August 2012, Dish altered the PTAT start- and end-times to accommodate certain Olympics programming on NBC. Additionally, Dish designates as primetime any program at least 50% of which falls within the prime time window, and that program is then included in that network's PTAT recording for that evening." *Id.* at *3 n.5 (citation omitted).

selected channels forever.[158] Once that setting is enabled,[159] the Hopper will record all programming that is broadcast from those selected channels during the hours that Dish Network designates. Practically, this provides users with access both to programming that they want to watch and would have selected to record regardless of the DVR they owned, as well as to programming that they did not select. Thus, without trying or even realizing it, the users may record programming that they would never choose to watch. This unrequested programming may likely just be recorded over after months of sitting unwatched on the DVR's hard drive.[160] But unrequested recordings may also comprise programming that the viewer had not heard of at the time of the recording but which he or she finds out about later, or programming that the viewer meant to record but forgot. Even if it can be argued that the never-viewed recordings do not hurt anyone, these latter examples threaten to steal real market share from an actual market important to the networks—video-on-demand.[161]

158 *Id.* at *3.

159 Notably, it turns out that the actor to configure this setting is of critical importance to the court, as minor an action as the one-time configuration of the setting may seem. *Id.* at *8-11. This is due to the court's reliance on the *Cablevision* case, Cartoon Network LP, v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008), wherein a "remote storage DVR system" was distinguished from video-on-demand systems, which similarly allow viewers to stream programming held on servers maintained by content providers, based on the fact that viewers had to perform an action prior to the original airing of the programming. *Fox*, 2012 WL 5938563, at *8-11. However, although the *Fox* court finds that "Dish exercises more control over the copies than did the defendant in *Cablevision*," still, "it is not clear to the Court that this control, being exercised after the creation of the copies, is relevant to whether Dish causes the copies to be made in the first place." *Id.* at *10. In other words, Dish Network can modify the "primetime" start- and end-times all it wants without exercising significant control as long as all of it is done after the *viewer* configures the setting to begin with.

160 Fox, *supra* note 151, at *4. This benign case would almost certainly invoke the fair use protections of *Sony*.

161 There is arguably a huge difference in the analysis of the fourth fair use factor between unknowingly recording and later watching (arguably indistinguishable from video-on-demand)

In consideration of these unprecedented injuries to Fox's business, one may almost be tempted to feel sorry for the Big Media giant in light of the district court's ruling. The Central District of California denied Fox's motion for preliminary judgment.[162] Specifically, the court analyzed the four traditional factors of preliminary injunction[163] to determine that Fox was unlikely to win on the merits of most of its claims,[164] that Fox had not sufficiently established that it would suffer irreparable harm without an injunction related to the claim that it *was* likely to win on the merits,[165] and that the remaining equitable factors were irrelevant in light of the

---

and unknowingly recording without ever watching (arguably harmless). *See Id.* at *13-14. Indeed this distinction could even be determinative in the court's overall fair use analysis. *Id.*

162 *Id.* at *19.

163 Specifically, the factors "[a] plaintiff seeking injunctive relief must show [are:] (1) it is likely to succeed on the merits; (2) it is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in its favor; and (4) that an injunction is in the public interest." *Id.* at *5 (citing Winter v. Natural Res. Def. Council, Inc., 55 U.S. 7, 20 (2008).

164 Fox, *supra* note 144, at *5-17. As can be inferred from the large number of pages in the range here, a large portion of the opinion focused on the analysis of this first crucial factor. While the court grapples with various unique claims asserted by Fox, duly running each through the intricacies of various important copyright law rules and principles, it suffices for my purposes here to say that the court ultimately concluded that Dish Network was most likely to succeed on the merits of all of the claims Fox could bring except one: Fox was considered likely to succeed on the merits of its claim that Quality Assurance copies of the programming that were created by the technicians as part of the ad-filter-making process were an infringement and not a fair use.

165 Specifically, the court determined that Fox would not suffer irreparable harm from the court allowing the Quality Assurance infringement referred to *supra* note 164 to continue. Fox, *supra* note 144, at *17-8.

court's conclusions on the first two factors.[166] Fox and Dish emerged from Round One and the Hopper is still on sale.[167]

A significant blow to Fox notwithstanding, the district court's ruling is probably a step in the right direction. Allowing the Hopper to exist—to painfully force some of the staunchest defenders of the stool model to rethink that model and to innovate—will surely have the effect of thrusting the industry deeper into the revolution. It is the very essence of "shaking it up." But, to be sure, while Fox loses this time, neither fairness nor public policy will favor Dish Network's emergence from the battle unscathed. Dish Network's stance may happen to promote innovation and revolution in this particular case, but that does not make Dish Network the "good guy" any more than Fox is a "bad guy." Indeed, this case is not about good guys and bad guys, but outdated business models and new experiments promising to nudge the industry toward a brighter future.

In this sense, *Fox v. Dish Network* is an ideal case for the illustrative purposes for which I use it. Both parties are significantly coupled with and dependent on the institution that has to go—the stool model. Clearly, Fox is fighting to keep the third leg of the stool alive—to force people to keep watching commercials so that it can keep charging advertisers as it always has. But while Dish Network may be content enough to kick that leg out from under Fox, it, too, continues to rely on that assumption for its own business.[168] The best way forward is not to

166 *Id.* at *19.

167 Indeed, it is promoted most prominently on Dish Network's website and may easily be purchased there as of this writing. DISH NETWORK, http://www.dish.com/ (last visited Mar. 25, 2013).

168 I argue that Dish Network is every bit the part of the Big Media establishment that would fight to maintain the status quo of the stool model that Fox is. This can be seen is part by Dish Network's failure to create a truly disruptive technology like, for example, the one that SONICblue created, *see supra* text accompanying note 148, but, rather, to create a technology

encourage one embodiment of the stool model to hobble another in an unending struggle to be "king of the mountain."[169] Rather, the industry will move forward by letting technology and new ideas for fully employing the technology *move* that mountain. Will there be casualties along the way? Will parties that made up an important part of the old establishment fall by the wayside while new parties make a name for themselves in the new establishment? Of course. But that is how it should be. That is business. That is revolution.[170]

Of course, Dish Network's victory of the district court battle for the preliminary injunction does not equate to the end of the war. Fox may be hurting now, but the threat to its business from upcoming appellate decisions far outweigh anything it has yet faced. Should the Ninth Circuit affirm the trial court's denial of preliminary injunction and if, eventually, the Hopper prevails on the merits against the many challenges it will face, the revolution will move forward significantly. With the legal path cleared, other competing technologies will follow the Hopper's lead.[171] With a solid affirmance of the *Sony* doctrine that has largely governed the

---

that merely gave it a anticompetitive advantage against other players in the environment of the stool model, *see supra* text accompanying note 156.

169 The childhood game of "King of the Mountain," wherein "children attempt[] to occupy the highest point on a raised platform or hill, while resisting attempts by other children to knock them off and replace them," *King of the Mountain*, WIKIPEDIA, http://en.wikipedia.org/wiki/King_of_the_Mountain (last visited Mar. 25, 2013), (last visited Mar. 25, 2013), is an apt analogy for what Dish Network seems to be trying to accomplish with its rollout of the Hopper. Dish Network has seemingly perched itself atop "the mountain" in relation to its competitors at the expense of the advertising ability of major networks such as Fox. Even as it enjoys its reign at the top, however, it is aware that similar technology and other backlash is likely to soon knock it off its perch to continue clawing its way to the top with the rest of the competitors.

170 Or, in Clay Shirky's words: "That is what real revolutions are like." Shirky, *supra* note 9.

171 *See, e.g.*, Brief of the ABC Television Affiliates Ass'n et al. as Amici Curiae in Support of Appellants, *supra* note 98, at *18 ("If Dish's gambit succeeds, its commercial-free television service is likely to be expanded, both to other [multichannel video programming distributors] and

industry for thirty years, technology is sure to advance quickly as the "shaken up" industry scrambles to come up with ways to make money in the brave new world. This scrambling will eventually lead to an industry that works. Some industry power may change hands as companies rise and fall, but, ultimately, the public will win.

C. Finding the Best Way Forward for the Courts

It is easy to make predictions, to paint pictures of a rosy future. It is easy to say what the law *should* do. But, of course, the rule of law demands that courts do much more than make sheer policy judgments. Even if it is good policy for the courts to shake things up and plunge the industry deeper into the revolution, the question remains as to *how* such judgments can legitimately be made. This question is clearly a more difficult one.

For the Ninth Circuit considering the preliminary injunction of *Fox v. Dish Network,* a good way forward has been proposed by the district court's decision[172] and by some of the amici.[173] For a future case that actually considers the merits of the Hopper or other similar technology, however, it may be more difficult to "shake it up" while also staying true to statutory mandates of Congress and giving due discretion to regulatory agencies. But, while the courts cannot implement the revolution alone—Congress and the relevant agencies have their parts to

---

beyond primetime. DIRECTV has already warned that it possesses similar commercial-skipping technology and is watching the outcome of this litigation").

172 *Fox Broad. Co. v. Dish Network, L.C.C.,* 905 F.Supp.2d 1088 (C.D. Cal. 2012).. Specifically, the court adheres strictly to traditional analyses of copyright fair use, the preliminary injunction factors, and stare decisis to consecutively eliminate the validity of each of Fox's claims.

173 *See, e.g.*, Brief of Law Scholars and Professors as Amici Curiae in Support of Defendants-Appellees, *supra* note 151 at *28-29 (offering spirited defenses for the traditional, broad application of the *Sony* and *Sega* cases and concluding that: "The *Sony* and *Sega* cases have been a fundamental part of this evolution in television and technology, and this Court should affirm their ongoing viability by rejecting Fox's attempt to narrow or eliminate their relevance").

do as well—the judiciary does have tools that it can use. Accordingly, I conclude with a brief look at three possible principles that courts may follow to continue shaking up the television industry and facilitating the revolution.

First, courts should use preliminary injunctions judiciously. That is, when it comes to equitable relief, courts should err on the side of permissiveness. This is typically considered good policy anyway—injunctions should always be reserved for extraordinary cases.[174] In *Fox v. Dish Network*, the Central District employed this principle[175] and the Ninth Circuit should affirm. For this case and cases like it that will arise in the future, this principle will bear great fruit as it is combined with the rapid-moving nature of the industry. As litigation stretches out over months and years and entrenched models become weakened, new, experimental models tend to encroach and force the Big Media establishment to rethink its strategies.[176] This is a good thing. Every little bit helps.

Second, courts should make liberal use of the copyright doctrine of fair use. This doctrine was the key to the Supreme Court's blessing of a similarly disruptive technology—the VCR—in the 1980s,[177] and a broad application of the statutory factors of fair use can go a long way toward encouraging technology and forcing new business models to revolutionize the industry. Along

174 Winter v. Natural Res. Def. Council, Inc., 55 U.S. 7, 24 (2008) ("A preliminary injunction is an extraordinary remedy never awarded as of right. In each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief.") (citation omitted).

175 *Fox*, 905 F.Supp.2d at 1096-97. ("An injunction is an exercise of a court's equitable authority, which should not be invoked as a matter of course, and only after taking into account all of the circumstances that bear on the need for prospective relief.") (citation omitted).

176 For example, competitors of Dish Network who have watched the litigation closely have used the time to prepare to take advantage of a potential holding that functionality such as Auto Hop is legal. *See supra* text accompanying note 171.

177 *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

these lines, the fair use principles laid out in *Sony* should be strengthened rather than hobbled when they come into play.[178] *Sony*, in many ways, is the seminal case for the "shake-it-up" policy. No doubt, the technology at play today is distinguishable from the technology at play in *Sony*,[179] but the high-level principle embodied by the *Sony* decision is as true today as it was then: Do not artificially stifle technology that improves lives. Disseminate the technology and let enterprising new business models make sense of it in the market place. Things worked out after *Sony*.[180] They will work out again as this principle is followed.

Finally, third, courts should apply stare decisis liberally. There is a rich tapestry of case law permissive to new technologies and innovative uses of copyrighted materials.[181] These

178 *See, e.g.*, Brief of Law Scholars and Professors as Amici Curiae in Support of Defendants-Appellees, *supra* note 151 at *28-29.

179 Indeed, it might be argued that the Hopper technology is much more threatening to the television industry than the VCR ever was. It should be noted, however, that, in its day, many believed that *Sony* would spell the end of the television industry. *See, e.g.*, *Home Recording of Copyrighted Works: Hearings on H.R. 4783, H.R. 4794, H.R. 4808, H.R. 5250, H.R. 5488, and H.R. 5705 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 97th Cong. 8 (1982) (testimony of Jack Valenti, President, Motion Picture Association of America, Inc.) ("I say to you that the VCR is to the American film producer and the American

public as the Boston strangler is to the woman home alone"). It was only in retrospect that it became obvious how benign and even helpful the *Sony* decision was to the entertainment industry. Lemley, *supra* note 139 at 128-29. While it may be difficult to believe now, history suggests that on the other side of the current revolution, cases like *Fox v. Dish Network* may appear similarly benign or helpful.

180 *See* Lemley, *supra* note 139 at 128-29.

181 *See, e.g.*, *Sony*, 464 U.S. at 417 (holding that time shifting is usually a fair use); *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994) (holding that parodies are presumptively fair use and that courts are not to consider the artistic merits of such parodies *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1993) (holding that "intermediate" copying as part of a process of reverse engineering may be a fair use if it is the only way that the information can reasonably be obtained); *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991) (holding that fact-intensive, non-creative works are likely to merit a thin copyright at best and only be protectable with very close copying).

permissive principles may be extracted from these cases and applied permissively to new technologies of today. For example, there is a question about how *Sega Enters. Ltd. v. Accolade, Inc.* should apply in *Fox v. Dish Network.*[182] There are good arguments on both sides as to whether and how a case like *Sega* should apply,[183] and the court might have been justified either in applying *Sega* to the benefit of Dish Network or in declining to find that it was relevant.[184] The court advanced the revolution by construing the *Sega* holding broadly, and following this pattern in the future may go a long way toward further implementing the revolution while appropriately maintaining the strictures of the rule of law.

V. Conclusion

A revolution is happening in the television industry. It is ongoing—it has been building for years as technology has advanced and consumer demand has evolved, and it will continue to build for years to come. At the end of the revolution, television will hardly be recognizable as the institution it once was. The assumptions upon which it was built—that Big Media was needed to

182 *Sega Enterprises Ltd. v. Accolade*, Inc., 977 F.2d 1510 (9th Cir. 1992)*Sega* was a case where the court found that intermediate copying of protected works in the process of reverse engineering could be construed as infringing even if the copies were not ultimately incorporated into an end product. However, the court concluded, in that case, that the intermediate copies at issue were a fair use since they were the only reasonable way that the information could be obtained that the defendants needed and the defendants actions were justifiable under public policy.

183 *See Fox Broad. Co. Inc. v. Dish Network, L.C.C.*, 905 F. Supp. 2d 1088, 1102 (C.D. Cal. 2012). (discussing the arguments for how *Sega* might be applied to settle the fair use question without a full-fledged analysis using the four fair use factors); Brief of Law Scholars and Professors as Amici Curiae in Support of Defendants-Appellees, *supra* note 151 at *28-29.

184 The district court ultimately declined to find that *Sega* was relevant, though it still declined to grant the preliminary injunction. *Fox*, 2012 WL 5938563, at *12 (following the discussion referred to *supra* note 183, the court concluded: “Therefore, the Court is not persuaded that Sega resolves the fair use inquiry. Accordingly it will examine the four factors set forth in 17 U.S.C. § 107”).

make good content and distribute it, and that doing so would allow Big Media to perpetually expose viewers to commercials that advertisers would be willing to pay for—are crumbling and will continue to crumble until they are another relic of the industry like the cathode ray tube. As technology continues to advance and old business models continue to deteriorate, the law should encourage experimentation in the industry. This may be done simply by declining to protect business models that no longer work—despite the money and power behind those models. Declining such protection will serve to "shake up" the industry in a way that will encourage experimentation, hard trade-offs, and innovation. These are good things. As experiments bear fruit and new business models that actually work emerge, the revolution will transpire more quickly and smoothly. At the end of it all, history suggests that both consumers and the industry will enjoy the benefit of a modern, revolutionized industry.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 2, PAGE 51

Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare

By Allison Gaul*

Table of Contents

Introduction	53
United States Defense Industry Infiltration	53
Stuxnet & the Iranian Nuclear Program	54
Estonia	56
The Georgian Conflict	58
1. Laws of Armed Conflict	62
2. The Principle of Neutrality	63
A. The Hague Convention	64
B. Privileges Afforded to neutrals	66
C. Duties and Obligations	66
i. Duty to Remain Impartial	67
ii. Duty to Intervene	68
iii. Duty to Repel Belligerent Forces	72
D. Right of Necessity	73
E. Conclusion	74
3. What is Information Warfare?	74
A. Armed Conflict, Espionage, or Criminal Activity?	76
i. Armed conflict	77
ii. Espionage and Military Intelligence Operations	79
iii. Criminal Activity	80
iv. Is Information Warfare Armed Conflict?	82
B. Types of Information Warfare	82
i. Exploitation	83
ii. Destruction	86
iii. Disruption	89
C. Conclusion	92
4. Analysis	93
A. How the Use of Information Warfare Affects the Privileges and Immunities of a Neutral State	93
B. What's a Neutral to do?	96
C. Applying The Hague Convention to Information Warfare Scenarios	106
5. Conclusion	110

* J.D. from Temple University Beasley School of Law. Patent Attorney with a background in Applied Mathematics & IT security. Special thanks to David Post for the many helpful reviews.

ABSTRACT

As technology develops, the spectrum of potential uses for information warfare will broaden. Creation of new applications for weaponized bits and bytes will inevitably result in the generation of new legal questions. The information warfare scenarios discussed in this article are a sample of the possible uses for digital attacks. It does not address every potential legal factor but instead examines the basis for applying the Law of Armed Conflict to information warfare that involves neutral states. Specifically, the article examines whether the Hague Convention of 1907 and subsequent Hague Rules Regarding Aerial Warfare, as pillars of the LoAC, can be reasonably applied to information warfare involving neutral states.

Introduction

The first decade of the 22nd century has seen the emergence of information warfare as a means of armed conflict that offers non-lethal, rapid strike capabilities. Many nations have military cyber divisions that employ information operations to supplement and support physical military operations. Non-state actors also utilize information warfare because of its low cost and low risk of loss to human life. There is currently no definitive legal framework in place to structure the meets and bounds of information warfare engagements. Complex legal questions arise and disappear within the blink of an eye as digital attacks travel through cyber space. Though this new mode of combat brings with it many nuanced tactical and legal considerations, it does not necessitate entirely new rules of engagement. Existing international laws, customs and norms addressing traditional modes of armed conflict are sufficient to guide information warfare practice. The international community has not formally embraced the application of existing law to information warfare, and until it does so, the digital battle space will remain a hi-tech free-for-all.

Over the last decade, the digital battle-space has become increasingly crowded as world superpowers; criminal organizations and terrorist groups develop offensive cyber capabilities. Networks are probed, data is stolen, military and civilian operations are compromised. The nature and extent of these actions varies as greatly as the groups perpetrating them. Some incidents are relatively benign episodes of experimentation, while others border on acts of war.

United States Defense Industry Infiltration

On July 14, 2011 the United States Department of Defense (DoD) publicly confirmed a

substantial breach of its digital security systems.[1] The DoD acknowledged that a digital assault in March of 2011 resulted in the theft of over 24,000 files from an unidentified defense contractor.[2] The content of the stolen files was not specifically revealed during the DoD's incident disclosure; but they did address defense intelligence thefts over the past few years, stating, "some of the stolen data is mundane, like the specifications for small parts of tanks, airplanes, and submarines. But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols[.]"[3] "Foreign intruders" were blamed for the attack, but fingers were not pointed at a particular nation or group.[4] The intrusion represents the largest publicly acknowledged cyber attack on U.S. defense intelligence to date.[5]

Stuxnet & the Iranian Nuclear Program

In July 2010 a covert and complex cyber attack struck Iran's nuclear enrichment program.[6] The attack, referred to as "Stuxnet," was a worm that monitored and subverted the operations of Iran's nuclear development facilities. Stuxnet was the first publicly known attack to

---

[1] *See* William J. Lynn, U.S. Deputy Secretary of Defense, *Remarks on the Department of Defense Cyber Strategy,* U.S. DEPT. OF DEFENSE (Jul. 14, 2011), http://www.defense.gov/speeches/speech.aspx?speechid=1593) [hereinafter Lynn's Remarks].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] William Broad J., John Markoff, David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay,* NEW YORK TIMES (Jan. 15 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all [hereinafter Broad].

not only spy on industrial facilities, but to also subvert control of their operations.[7]

The worm effected industrial machinery control computers used in Iranian uranium enrichment facilities.[8] These computers utilized Siemens software control packages to instruct centrifuge machinery to "'turn on and off motors, monitor temperature, [and] turn coolers on[.]'"[9] Once the worm infected an enrichment facility computer, Stuxnet would monitor and record files of normal plant activity.[10] These recordings were displayed to plant operators to create the illusion that machinery was operating normally.[11] At the same time, Stuxnet subverted instructions causing centrifuges to spin out of control.[12] The worm was programmed to propagate slowly, making it hard to diagnose infection because only a few computers were infected at any given time.[13] The difficulty of detection allowed Stuxnet to continue causing centrifuge malfunctions without the notice of plant operators.

Its likely target being Iranian nuclear facilities, the Stuxnet worm compromised five Iranian industrial processing organizations, including the Natanz nuclear research facility.[14] Iran

---

[7] Jonathan Fildes, *Stuxnet Virus Targets and Spread Revealed,* BBC NEWS (Feb. 17 2011), http://www.bbc.co.uk/news/technology-12465688 [hereinafter Fildes].

[8] *Id.*

[9] *See Stuxnet Worm Hits Iran Nuclear Plant Staff Computers,* BBC NEWS (Sep. 26, 2010), http://www.bbc.co.uk/news/world-middle-east-11414483 [hereinafter *Stuxnet Worm Hits Iran*]; *see also,* Fildes, *supra* note 7.

[10] *See* Broad, *supra* note 6.

[11] *Id.*

[12] *See* Broad, *supra* note 6.

[13] *See,* Fildes, *supra* note 7.

[14] *Id.*

initially denied that the attack had any impact, but later acknowledged that its uranium enrichment programs were disrupted.[15] There was much speculation that the attack was a joint effort between the United States and Israel.[16] Though these speculations were not publicly confirmed, Iran reacted with verbal hostility towards the suspected culprits.[17]

Estonia

In late April of 2007, Estonia was hit by the first of several waves of cyber attacks targeting Estonian infrastructure.[18] The attacks began on April 26th during a period of political upheaval prompted by the removal of a bronze soldier statue commemorating Russian military victory, from the center of the Estonian capital of Tallinn.[19] Cyber assaults on Estonian media, banking, and government services continued until shortly after May 9th, the Russian holiday celebrating victory over Nazi Germany.[20] After the digital dust settled, the list of affected targets

---

[15] John Markoff, *A Silent Attack, but not a Subtle One,* NEW YORK TIMES NEWS, (Sep. 26 2010), https://www.nytimes.com/2010/09/27/technology/27virus.html.

[16] Broad, *supra* note 6.

[17] Director of Information Technology Council at the Iranian Ministry of Industries and Mines, Mahmud Liaii, said: "An electronic war has been launched against Iran." Peter Beaumont, *Iran 'Detains Western Spies' After Cyber Attack on Nuclear Plant,* The Guardian, (October 2, 2010) *http://www.theguardian.com/*

world/2010/oct/02/iran-western-spies-cyber-attack .

[18] *See* Ian Tavnor, *Russia Accused of Unleashed Cyberwar to Disable Estonia,* The Guardian, (May 17, 2007) http://www.guardian.co.uk/world/2007/may/17/ topstories3.russia [hereinafter Tavnor]; *see also,* Mark Landler, John Markoff, *Digital Fears Emerge After Data Siege in Estonia,* N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted= all [hereinafter Landler].

[19] *See supra* note 18.

[20] *See id.*

included the websites, network resources, and e-mail servers of the Estonian Parliament, the Reform Party, the Prime Minister, a number of newspapers, and the largest bank in Estonia.[21]

The attackers utilized a large network of hijacked computers, called a botnet, to assault Estonian websites and networks with a large-scale, distributed denial-of-service attack.[22] This type of attack transmits a large volume of data at a victim computer system to overwhelm its resources and degrade its ability to operate normally.[23] This is analogous to opening a dam to destroy a town downriver by flood. If enough water is released, then the town may be unable to muster the resources to defend against the aquatic assault. By instructing the botnet to send large volumes of data at Estonian networks, the attackers were able to rally enough bandwidth resources to overcome the network resources of the defending country.[24] The technique was ultimately successful and forced several sectors of Estonian government and economy offline.[25]

Media perception focused on the Russian Government as the likely culprit.[26] Kremlin

---

[21] Landler, *supra* note 18.

[22] *E.g.* , *War in the Fifth Domain. Are the Mouse and Keyboard the New Weapons of Conflict?*, THE ECONOMIST (Jul. 1 2010), http://www.economist.com/node/16478792l [hereinafter War in the Fifth Domain]; Tavnor, *supra* note 18; John Schwartz, *When Computers Attack* N.Y. TIMES (Jun. 24, 2007), http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?pagewanted=all; Landler, *supra* note 18.

[23] Taynor, *supra*, note18.

[24] *See* Tavnor, *supra* note 18.

[25] *War in the Fifth Domain*, *supra* note 22.

[26] *See*, *e.g.*, Traynor, *supra* note 18; *War in the Fifth Domain*, *supra* note 22; Landler, *supra* note 18; *Cyberwarefare: Newly Nasty*, THE ECONOMIST (May 24, 2007), http://www.economist.com/node/9228757 [hereinafter *Newly Nasty*]; Steven Lee Myers, *'E-stonia' Accuses Russia of Computer Attacks*, N.Y. TIMES (May 18, 2007), *available at* http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html.

spokesman Dmitry Peskov ardently denied such allegations as being 'completely untrue."[27] Though the IP addresses of some attackers pointed to Russian involvement, NATO investigators did not report a conclusive link between the attacks and the Russian government.[28] A number of groups and individuals claimed responsibility including "hacktivists" (aggressive cyber activists), individual students of Russian background, the Kremlin backed youth group NAASHI (young democratic anti-fascist party), and even a Russian political party representative who jokingly claimed that his assistant had carried out the assault.[29] Some experts dismissed these claims due to the scale and complexity of the attacks, positing that it was highly improbable that such actions could be carried out without assistance from the Russian government.[30] Without publicly resolving these issues, NATO offered assistance to Estonia and in 2009 established a cyber warfare center in Tallinn to provide a base for response to future attacks in Europe.[31]

The Georgian Conflict

A year after cyber attacks assailed Estonian infrastructure, the country of Georgia became the target of a similar digital assault. In July 2008, a targeted DDOS attack was executed against the website of the Georgian president Mikhail Saakashvili.[32] The attack commenced a month

[27] *Estonia fines man for 'cyber war'*, BBC NEWS (Jan. 2852008), *available at* http://news.bbc.co.uk/2/hi/technology/7208511.stm [hereinafter Estonia Fines].

[28] *See id.; see also* Taynor, *supra* note 18.

[29] *See* Taynor, *supra* note 18; *see also, Estonia has no Evidence of Kremlin Involvement in CyberAttacks*, RIA NOVOSTi, (Sep. 6, 2007), *available at* http://en.rian.ru/world/20070906/76959190.html.

[30] Landler, *supra* note 18; Estonia Fines, *supra* note 27.

[31] *See* Newly Tasty, *supra* note 26.

[32] *See* Siobhan Gorman, *Hackers Stole IDs for Attacks*, WALL ST. JOURNAL (Aug. 17, 2009), *available at* http://online.wsj.com/article/SB125046431841935299.html; *see also* John Markoff,

prior to the Russian invasion of Georgia's Abkhazia and South Ossetia regions.[33] As the five-day Russia-Georgia conflict unfolded, a larger wave of cyber attacks hit Georgia.[34] Government and media websites were shut down, telephone and emergency services were crippled, and the web-based services of the largest bank in Georgia were disabled.[35] The resulting loss of communication capabilities impeded Georgia's ability to inform the outside world about the mounting casualties of the Russian conflict.[36]

Blame for the attacks was once again placed on the Russian government, but the obfuscated trail left by the attackers resulted in a lack of definite culpability. The bulk of the data traffic, much of which bore the pro-Russian message "win+love+in+Russa" was controlled and routed through a set of servers in the United States.[37] Combined with the timing of the cyber attacks, which closely coincided with Russian military movements into and around Georgia, these facts lead some analysts to suspect that the Kremlin was responsible.[38] Yevgeniy Khorishko, a spokesman for the Russian embassy in Washington, D.C. denied any involvement

---

Before the Gunfire, Cyberattacks, N.Y. TIMES (Aug. 12, 2008), *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html; *War in the Fifth Domain*, *supra* note 22.

http://online.wsj.com/article/SB125046431841935299.htmlhttp://www.nytimes.com/2008/08/13/technology/13cyber.html

[33] *See supra*, note 32.

[34] *See* Gorman, *supra* note 32.

[35] *Id.*

[36] *See id.*; *see also Marching off to Cyberwar*, THE ECONOMIST (Dec. 4, 2008), *available at* http:www.economist.com/node/12673385; *War in the Fifth Domain*, *supra* note 22.

[37] Tavnor, *supra* note 18.

[38] Markoff, *supra* note 32.

by the Russian government, stating, "Russian officials and the Russian military had nothing to do with the cyber attacks on the Georgian Web [.]"[39] Suspicion was later diverted from the Kremlin to the Russian Business Network (RBN), an organized crime ring known for taking part in cyber crime.[40] The RBN owned ten of the websites used to perform the attacks on Georgia, which were purchased using credit cards and identities stolen from Americans.[41] Though, American resources were used in the attack against Georgia, American servers were used to save the Georgian government's data.[42] A private company in the United States offered to host the Georgian government websites and provide data backup during the conflict.[43] Thus, Georgia was assailed by non-state actors from Russia and protected by non-state actors from the United States.

These scenarios provide chilling examples of how computers may be used to cause instability in various sectors of a country's infrastructure. One can easily imagine far more disastrous effects waiting on the horizon if appropriate deterrent measures are not developed. What legal framework should be applied in guiding the development of such measures?

Amidst the flurry of publications on information warfare printed in law reviews across

---

[39] *Id.*; see War in the Fifth Domain, supra note 22.

[40] *See* Gorman, *supra* note 32*; see also* War in the Fifth Domain, *supra* note 22; Markoff, *supra* note 32.

[41] *See* Gorman, *supra* note 32.

[42] Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN, Aug. 18, 2008, http://articles.cnn.com/2008-08-18/tech/cyber.warfare_1_hackers-internet-assault-web-sites?_s=PM:TECH; Peter Svensson, *Russian Hackers Continue Attacks on Georgian Sites*, AP NEWS, Aug. 12, 2008, http://www.usatoday .com/tech/products/2008-08-12-2416394828_x.htm.

[43] Svensson, *supra* note 42.

the United States, the topics of "general culpability" and "redefining warfare" are abundant; however, there is scant material addressing some of the less obvious problems presented by cyber conflicts. Should responsibility and liability change depending on whether the perpetrator is an individual, a company or a government entity? Is it legally and morally permissible to assign at least a portion of the blame for an information warfare attack to nations who were unaware of their participation? What if assigning such blame results in the nation's forced entry into an international armed conflict? These questions present legal issues for which there is little guiding precedent and a woefully incomplete framework for application. We are thus required to pursue applications of aging legal frameworks to modern dilemmas. To this end, I will examine a narrow set of legal issues posed by the onset of information warfare, and attempt to determine if the present legal framework can be equitably applied to the situations arising within that narrow set of questions.

In this paper I will examine the impact of information warfare operations on neutral states; those that have adopted a position of non-involvement with respect to international armed conflicts. While the law concerning the behavioral interaction between neutral and warring states is well established in physical settings, the application of this law to the digital battlefield is a complicated issue. What rights and duties does a neutral state have under current international neutrality law when information warfare is the modality of aggression? The following sections of this paper examine and analyze this difficult question. Section I discusses the fundamentals of the Law of Armed Conflict. Section II examines the framework of the principle of neutrality and addresses pertinent aspects of the Law of Armed Conflict. Specifically, it focuses on the Hague Conventions on neutrality as the basis for current neutrality law and the rights and duties of a neutral state. Section III assesses the definition of information warfare as it applies to the

determination of what actions may or may not be encompassed by international neutrality law. Lastly, Section IV analyzes the question of whether current international neutrality law can be reasonably applied to impose rights and duties on a neutral state in an information warfare setting.

1. The Law of Armed Conflict

The Law of Armed Conflict (LoAC) is a set of international rules and regulations that provide authorization for the military personnel of parties to an international armed conflict to engage in attacks on lawful military targets.[44] These rules and customs suggest specific behaviors that if adhered to, will limit the destructive toll exacted by international conflicts.[45] They apply equivalently to all parties to an international conflict. The LoAC comprises a multitude of treaties, conventions and international customs, but the primary sources are the Hague Convention of 1899, Hague Convention of 1907, Hague Rules of Aerial Warfare, the Geneva Conventions, and the Geneva Convention Protocols.[46] There are seven general principles established by the LoAC: 1) distinction (the differentiation of combatants from non-combatants); 2) military necessity (all enemy military personnel are automatically presumed to be hostile); 3) proportionality (military advantage to be gained by an attack must be greater than the resulting

---

[44] *See* DEP'T OF DEF. OFFICE OF GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADB257057[hereinafter Assessment of International Legal Issues].

[45] *See id*.; *see also* David L. Wilson, *An Army View of Neutrality in Space: Legal Options for Space Negation*, 50 A.F. L. REV. 175, 192-193 (2001).

[46] These sources are particularly significant due to the number of signatories and breadth of issues addressed therein. Subsequent treaties have expanded on the concepts set forth in the Hague and Geneva Conventions, but are largely specific to particular conflicts and/or signatories, making those treaties less relevant to the international community as a whole. *See generally* Assessment of International Legal Issues, *supra* note 44.

collateral damage); 4) superfluous injury (specific weapons that cause superfluous injury are disallowed); 5) indiscriminate injury (weapons causing indiscriminate damage, such as biological weapons, are disallowed); 6) perfidy (certain persons and property are immune from attack and are designated by visually recognizable symbols); and 7) neutrality (nations wishing to remain uninvolved in a conflict may declare themselves neutral).[47] In this paper I focus on the principle of neutrality and examine how this element of the LoAC can be applied to information warfare.[48]

2. The Principle of Neutrality

The principle of neutrality is established through a set of rules and customs that provide guidelines for interaction between parties to an international armed conflict. The 1899 Hague Convention, 1907 Hague Convention and 1923 Hague Rules regarding Aerial Warfare (hereinafter jointly referred to as "the Hague Conventions") established a framework for acceptable means of interaction between neutrals and belligerents. Subsequent agreements and treaties, such as the United Nations Charter, further addressed the proscribed interactions of neutrals and belligerents; however, these sources are not within the scope of this paper.[49] As the

[47] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS [ICRC], *Basic Rules of the Geneva Convention and their Additional Protocols,* Doc. Ref. 0365(1988) *available at*: http://www.icrc.org/eng/resources/documents/publication/p0365.html; *see also,* Assessment of International Legal Issues, *supra* note 44.

[48] More information on the application of other principles of the LoAC to information warfare is available through several excellent articles in the 64th Edition of the Air Force Law Review ("Cyber Edition"). *E.g., see generally* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121 (2009) [hereinafter Schaap]; Lieutenant Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyber Space: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009).

[49] While the Hague Convention and Laws of Armed Conflict are the primary sources of neutrality law, the United Nations also levies obligations on neutral states. Pursuant to the United Nations Charter, Article 51, member states may not commence the "use of force"

primary source for the principle of neutrality, the Hague Conventions are critical to understanding a neutral's obligations and immunities with respect to an international conflict. In this section, I discuss the background of the Hague Conventions, describe the privileges afforded to neutral states, and then categorize several articles of the Conventions that are potentially applicable to information warfare scenarios. These articles belong either to a duty to remain impartial, a duty to intervene, or a duty to repel. Lastly, I address a belligerent's right of necessity with respect to the duties and obligations associated with neutrality law.

A. The Hague Convention

The 1899 and 1907 Hague Conventions and subsequent Rules of Aerial Warfare established a behavioral mechanism for a state to maintain its rights as a neutral in exchange for

---

without authorization from the U.N. Security Council. U.N. CHARTER art. 39. Unauthorized use of force is only allowed when a member nation is attacked and lacks adequate time to consult the Security Council before defensive measures are taken. U.N. CHARTER art. 51. This provision is consistent with the right of necessity provided by the LoAC. The difference between the right of necessity and Article 51 of the U.N. Charter is the U.N. Security Council's ability to call upon member nations to assist in keeping the peace by peaceful means or by use of force. U.N. CHARTER arts. 41-2. Member nations are required to provide armed forces, facilities and rights of passage that the Security Council deems necessary for the maintenance of international peace. U.N. CHARTER art. 43. Thus, a neutral state belonging to the United Nations might be called upon to furnish troops or allow the troops of other nations to pass through its territory in order to bring resolution to an international armed conflict. Resources such as telecommunications facilities or satellite access can also be commandeered for U.N. peacekeeping missions. *See generally* Richard A. Morgan, *Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and Peaceful Purposes*, 60 J. AIR L. & COMM. 237, 239 (1994). Though these acts by a neutral would otherwise violate their duties under the LoAC, neutrals do not violate the principle of neutrality when they uphold their U.N. member obligations. *Id.* This is because Article 49 of the U.N. charter requires member states to cooperate with Security Council decisions, effectively absolving the neutral of fault for providing aid to peacekeeping forces. U.N. CHARTER art. 49; *see* Assessment of International Legal Issues, *supra* note 44. As a practical matter, belligerents opposing U.N. troops will likely see all neutrals participating in the mission as aligned with opposing belligerents, even if no such legal conclusion exists. Should the neutral choose not to obey the U.N. Security Council request, the neutral will suffer reproach and international relations deterioration. Neutrals would be wise to observe their duties and obligations under the LoAC and assist the U.N. as necessary, without fear of destroying their neutrality.

meeting certain obligations. The Hague Conventions were among the first international treaties to formally state the laws of war. The first convention, adopted at an international peace conference in 1899, focused primarily on structure of international arbitration, the basic laws of armed conflicts, and prohibitions on use of certain ultra-hazardous technologies such as: chemical warfare, hollow point bullets, and explosives dropped from air balloons.[50] In 1907, the peace conference met again to expand upon the principles outlined in the first Hague Convention and address emerging trends in the technology of war. Areas of major focus included large-scale naval warfare and the obligations on land and sea of neutral powers.[51] Changing trends in the modality of warfare were addressed once again at a 1923 peace conference where the Hague Rules of Aerial Warfare were drafted, further extending the rights and duties of a neutral power to cover aerial combat.[52] These rules were never officially codified as part of the Hague Convention; however, most of the international community has adopted them as custom.[53]

---

[50] *See* Convention Respecting the Pacific Settlement of International Disputes, July 29, 1899, 32 Stat. 1799; Convention with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803; Convention Respecting the Adaptation to Maritime Warfare of Principles of Geneva Convention of 1864, July 29, 1899, 32 Stat. 1827; Convention Respecting the Prohibiting Launching of Projectiles and Explosives from Balloons, July 29, 1899, 32 Stat. 1839.

[51] *See* Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), Oct. 18, 1907, 36 Stat. 2310[hereinafter Hague Convention V]; Convention Rights and Duties of Neutral Powers in Naval War(Hague XIII), Oct. 18, 1907, 6 Stat. 2415[hereinafter Hague Convention XIII].

[52] Hague Rules of Aerial Warfare, art. 40-2, Feb. 19, 1923, 32 AM. J. INT'L L. Supp. 12 (1938) (not in force) [hereinafter Hague Air Rules].

[53] George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1135 (2000) [hereinafter Walker].

B. Privileges Afforded to Neutrals

When a state formally declines to align with any party to an international conflict, the state becomes a "neutral" and gains privileges as outlined in the Hague Convention. Signatories to the Hague Conventions agree to abide by rules governing treatment of neutral states, and afford all due privileges to those states. The primary benefit of neutrality is inviolability of territory. Once a declaration of neutrality is made, it is a violation of the Hague Convention for belligerent agents to trespass on the neutral's territory.[54] This prohibition effectively removes the territory of the neutral state from the list of potential battlefields, thereby reducing the likelihood of damage to the territory during the conflict. Neutral states are allowed to maintain trade relations and formal communications with all belligerents. For non-neutral states, these acts could draw a state into the conflict and align the state with a belligerent power in the eyes of the international community.[55] Thus, neutral states are at least partially insulated from the economic distress and opportunity costs of breakdowns in communication resulting from participation in international armed conflicts.

C. Duties and Obligations

In exchange for the aforementioned privileges, a neutral state has a duty to perform or refrain from performing certain actions.[56] A neutral's failure to meet its duties and obligations can put its neutral status at risk. The Hague Conventions set forth scenarios in which a neutral

---

[54] Hague Convention V, *supra* note 51 at art. 1-5.

[55] *See* Hague Convention V, *supra* note 51 at art. 7-8; *see also* STEPHEN C. NEFF, THE RIGHTS AND DUTIES OF NEUTRALS, 1 (2000).

[56] *See generally* Hague Convention V, *supra* note 51; Hague Convention XIII, *supra* note 51; Hague Air Rules, *supra* note 52.

may act, not act, or act in response to the actions of a belligerent. A neutral is obligated to respond in the proscribed manner, though the manner of fulfilling the duty in question is generally left to the discretion of the neutral state. The type of duty imposed on the neutral state varies according to the modality of the conflict. For instance, a neutral must not allow a belligerent to move troops, munitions, or aircrafts over the neutral's land; however, a belligerent warship that is merely passing through a neutral's waters will not trigger any responsibility on the part of the neutral power.[57] Many of these duties and obligations may be classified as: a duty of impartiality, a duty to intervene, or a duty to repel**.**

i. *Duty to Remain Impartial*

Neutral nations must interact impartially with the belligerent states on all sides of an international conflict.[58] If a neutral provides the use of its services and resources to any belligerent state, then the neutral must make the same services or resources available to all belligerent states. A neutral power that allows belligerent owned vessels, whether military or civilian, to make use of the neutral's ports may not give preference to either belligerent.[59]

Generally, private companies within a neutral state are not subject to the same resource allocation restrictions as the state's government. A neutral state that maintains relations with warring nations may not show preference to one belligerent over another with regard to available resources.[60] Conversely, material resources sold by a private company can be sold to any party.[61]

---

[57] Hague Convention V, *supra* note 51 at art. 1; Hague Convention XIII, *supra* note 51 at art. 30; Hague Air Rules, *supra* note 52 at art. 35.

[58] *See* Major David L. Wilson, *An Army View of Neutrality in Space: Legal Options for Space Negation,* 50 A.F. L. REV. 175, 192 (2001).

[59] Hague Convention XIII, *supra* note 51 at art. 9.

[60] *See* Hague Convention XIII, *supra* note 51 at art. 19, 21; *see also,* Hague Convention V, *supra* note 51 at art. 4,7-8.

Thus, private companies may continue to sell and export goods to any and all belligerents.[62] This includes munitions, supplies of war and even aircraft.[63]

An exception to the freedom of a neutral state's private companies to contract with belligerent states focuses on access to communications services. Communications resources must also be offered or denied equally to all belligerents. Neutral states must insure that private companies providing telegraphy services do not offer services or resources to one party that are not available to all.[64] Belligerent forces and companies may not erect telegraphy towers on neutral territory unless the resulting telegraphy services are publicly available.[65] The precise meaning of "telegraphy services" is not legally well defined.[66] For the purposes of this paper, telegraphy is defined as "the practice of using or constructing communications systems for the transmission or reproduction of information."[67]

---

[61] Hague Convention V, *supra* note 51 at art. 9.

[62] *Id.* at art. 7.

[63] Hague Air Rules, *supra* note 52 at art. 45.

[64] Hague Convention V, *supra* note 51 at art. 8-9.

[65] *Id.* at Art, 3.

[66] Though not technically "telegraphy," erecting of website hosting facilities on neutral territory during the Georgian conflict was seen as a violation of the principle of neutrality. l Lieutenant Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyber Space: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009). *See* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV 1427, 1428 (2008) (citing Newly Nasty, THE ECONOMIST, May 26, 2007, at 63).

[67] A Google search of the terms "definition telegraphy" yields the definition: The "science or practice of using or constructing communications systems for the transmission or reproduction of information." http://www.google.com.

The term "telegraphy" may encompass more than the telephone line based communications available at the time the Hague Convention was drafted. The United States Department of Defense has stated that the plain language of articles eight and nine of the Hague Convention justifies an extension of these constraints to satellite communications as well as ground based communication relays.[68] It is not yet settled whether the language of the articles can be interpreted to extend to systems that generate communications such as global positioning systems, weather analysis satellites, or signal intelligence systems.[69] The emergence of the Internet as a viaduct for weapons of digital warfare further complicates the question because the Internet possesses both communication relay and data generation properties. Though the Hague Convention details specific instances in which a country may not show preference to any side of a conflict, the modern trend points to the conclusion that the duty of impartiality may extend to situations beyond the instances described in the Hague articles.[70]

ii. *Duty to Intervene*

Neutral states must act to prevent belligerent forces found within neutral territory from leaving in a battle-ready condition.[71] Neutrals are thus obliged to prevent belligerent action from originating within neutral territory. The means a neutral can employ to prevent belligerents from quitting neutral territory varies according to the potential harm presented. Once the belligerents are in custody, the method and duration of detention is determined by the neutral state. The potential for internment of troops and supplies diminishes the appeal to belligerents of

[68] Assessment of International Legal Issues, *supra* note 44.

[69] *Id.*

[70] Hague Convention V, *supra* note 51 at art. 8-9.

[71] Hague Convention V, *supra* note 51 at art. 11-15.

trespassing on neutral territory by reducing the likelihood of gaining an exploitable strategic advantage.

The Hague Conventions provide neutral states a good deal of latitude in determining the extent of intervention appropriate in a given scenario, but intervention measures are mandatory.[72] In the simplest case, belligerent forces, vessels, and craft are rescued by agents of a neutral state and brought within the jurisdiction of that neutral power. Rescue scenarios present only marginal belligerent malfeasance and thus the belligerent vessel or craft, and its crew must be interned in a manner determined by the neutral, but the neutral need not take further action.[73]

On the other hand, trespassing belligerents who refuse to comply with the neutral state's orders to leave may be deprived of their means of escape. A belligerent warship or aircraft that enters the territory of the neutral state will be asked to leave. If the belligerents refuse to quit the territory the neutrals must act decisively.[74] Presumably due to the belligerents' greater level of culpability for their predicament; the neutral state may utilize what measures it deems necessary to prevent warships from being sea-worthy, or the means at its disposal to ground aircraft refusing to leave neutral territory.[75] Both events require internment of the craft's crew.[76] Any

[72] *e.g.*, Hague Convention XIII, *supra* note 51 at art. 24; Hague Air Rules, *supra* note 52 at art. 46.

[73] Hague Convention XIII, *supra* note 51 at Art. 3; Hague Air Rules, *supra* note 521 at art. 43.

[74] Hague Convention XIII, *supra* note 51 at arts. 21 & 24; Hague Air Rules, *supra* note 52 at art. 42.

[75] *Id.*

[76] *Id.*

belligerent ground forces found trespassing in a neutral's territory must be interned as far from the theater of war as possible.[77]

The most interesting case arises when the neutral state knows an aircraft within its jurisdiction is outfitted for the purposes of offensive operations or intelligence gathering, and reasonably believes such operations are targeted at opposing belligerents. Under these circumstances a neutral power is instructed to use the means at its disposal to prevent the aircraft from leaving the neutral's territory.[78] It must also take action to prevent the crew from doing any work on the aircraft, or from departing the neutral territory.[79] Additionally, a neutral must use means at its disposal to prevent aircraft in the neutral's airspace or waterways from collecting surveillance of enemy forces.[80] These articles do not stipulate that the means of prevention are limited to internment.[81] Consequently, a neutral state may act forcefully to prevent the departure of the aircraft and its crew, without jeopardizing the state's neutral status.

The duty to intervene creates an active intermediary role for neutral states and imposes a policy of "non-origination". Belligerent vessels, aircraft and forces must be interned if there is any suspicion that they have been or intend to be involved in hostile actions.[82] If there is reason to believe that belligerents in neutral territory intend to engage in hostilities with opposing

---

[77] Hague Convention V, *supra* note 51 at art. 11.

[78] Hague Air Rules, *supra* note 52 at art. 46.

[79] *Id.*

[80] Hague Air Rules, *supra* note 52 at art. 47.

[81] *Id.*

[82] Hague Convention XIII, *supra* note 51, at Art. 3, 24; Hague Air Rules, *supra* note 52 at art. 42- 43.

belligerents, then the neutral state must take whatever action it can to prevent those hostilities.[83] An active role in preventing hostile operations from originating in its territory reinforces the neutral's refusal to be politically aligned with any belligerent. Thus a neutral state may not simply turn a blind eye to the actions of belligerent states, but must actively prevent potential acts of war from originating within the neutral state's jurisdiction.

iii. *Duty to Repel Belligerent Forces*

Neutral states have an affirmative duty to repel belligerent incursions into neutral territory.[84] Denying the use of transportation infrastructure as a conduit for warfare is essential to maintaining neutral status. By attempting to prohibit belligerent forces from moving through neutral territory, a neutral state effectively asserts that its modes of transportation are not a means for facilitating hostile activities against opposing belligerents. The extent of the action necessary to satisfy this duty depends on whether the mode of incursion is by land, sea, or air. While the level of deterrent measures required by a neutral state varies according to the situation, every neutral state has a duty to try to stop belligerents from violating the neutral's territory.

Conflicts on land present the simplest scenario for repelling invading forces. Internationally accepted borders of each state are well documented, making it simple for belligerents and neutrals to determine whether or not a movement constitutes trespass. Additionally, most countries have the resources to launch minimal deterrent measures against invaders. Due to the relative ease of putting up token resistance, the Hague Conventions' prohibition against belligerent incursions into neutral territory does not impose a complex burden

[83] Hague Air Rules, *supra* note 52 at art. 46.

[84] Hague Convention V, *supra* note 51 at art 1-3.

on most neutral states.

The situation becomes less clear when combatant incursions take place at sea or in the air. Water and air are fluid media without definite delineated boundaries, making it difficult for neutral states and belligerents alike to distinguish the territory to avoid. Not all countries have the technological capability of detecting trespass over such nondescript boundaries. Even those nations that can adequately monitor their air and sea borders do not necessarily have a standing navy or air force capable of intervening in belligerent actions. These resource discrepancies amongst nations create a dilemma with respect to enforcement: how can the international community reasonably expect a poor or small country with minimal maritime resources to repel an invasion it couldn't even detect? The drafters of the Hague articles were presumably sympathetic to these concerns and decided that the duty to repel aircraft and vessels should be proportional to the resources of the neutral state.[85] Neutral states must utilize the "means at their disposal" to conduct surveillance and prevent belligerent states from entering neutral airspace or utilizing neutral waters for hostile activities.[86]

D. The Right of Necessity

[85] "A neutral Power is bound to exercise such surveillance as the means at its disposal allowing it to prevent any violation of the provisions of the above Articles occurring in its ports or roadsteads or in its waters." Hague Convention XIII, *supra* note 51 at art. 25."A neutral Government is bound to use the means at its disposal to prevent belligerent military aircraft from entering its jurisdiction and to compel them to land or to alight on water if they have penetrated therein." Hague Air Rules, *supra* note 52 at art. 42.

[86] *See* Hague Convention XIII, *supra* note 51 at Art. 25; *see also* Hague Air Rules, supra note 51 at Art. 42. *But see* Hague Convention XIII, *supra* note 51 at Art 10 stating that mere passage of a warship through neutral waters does not violate the neutral state's territory; consequently no action is required by the neutral state as long as the belligerent warship is just passing through. This discrepancy is likely due to the fact that alternative routes through airspace and on land are generally available to belligerent forces, while there may only be one passable water route for belligerents to travel on.

If a neutral state is unable or unwilling to repel or detain belligerent forces within its territory, opposing belligerent states have the right to intervene. Under a theory of "right of necessity," a belligerent state may take action in self-defense against an opposing belligerent state that has violated neutral territory.[87] This right is particularly pertinent to naval and air incursions in which a neutral nation with fewer resources may have met its duty by attempting to repel or detain the belligerent craft, but may have been unable to effectuate such measures successfully. In these circumstances, opposing belligerents may utilize the neutral's territory to defend their own interests.

E. Conclusion

The Hague Convention requires signatory neutral nations to intervene and prevent belligerents from operating within the neutral's territory, treat all belligerents impartially and equally, and repel belligerent forces trespassing on neutral territory. In a practical sense, this means neutrals must act to prevent a belligerent from utilizing the neutral's resources to commence hostilities against an opposing belligerent. Resources such as land, sea, air, telegraphy, and commercial goods are addressed in the Hague Convention, but data networks were not available when the Convention was drafted. In the following sections, this paper will explore the extension of the Hague Convention to include modern data communications networks and the tools of information warfare

3. What is Information Warfare?

The scope and nature of information warfare are amorphous and difficult to constrain to a single definition. There is no generally accepted definition concerning the coverage of the term

[87] *See* Walker, *supra* note 43.

"Information Warfare." Indeed there does not seem to even be an agreement as to what term should be used. The terms "cyber warfare," "information warfare," "cyber assault," "C4I," and "I-War" are used interchangeably.[88] U.S. attempts to describe information warfare focus on the intended result of the action. The U.S. Air Force uses the term network warfare operations" defined to mean "integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battle space."[89] Another definition comes from a 2006 CRS report to Congress, which referred to cyber warfare as "operations to disrupt or destroy information resident in computers and computer networks.[90]

The DoD adopted a broader approach to defining information warfare. The DoD describes "information operations" as "he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.."[91] This definition is overly broad because it encompasses standard operating procedures, electronic security, military intelligence acquisition, and other non-adversarial actions taken using military information systems. Definitional clarity is provided by the Department of Defense's recent separation of offensive cyber operations or "cyber attacks" into

---

[88] *See* Dr. Ivan K. Goldberg, *Glossary of Information Warfare Terms*, http://www.psycom.net/iwar.2.html (April 24, 2012).

[89] U.S. Dept. of Air Force Policy Dir.10-7, Information Operations, 19 (Sep. 6 2006) *available at* http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf.

[90] CLAY WILSON, CONG. RES. SERVICE REP. FOR CONGRESS NO. RL31787, INFORMATION OPERATIONS AND CYBERWAR CAPABILITIES AND RELATED POLICY ISSUES 5 (Sep. 14, 2006), *available at* http://www.fas.org/irp/crs/RL31787.pdf.

[91] Joint Electronic Library, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Though 15 October 2013) http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

the categories of exploitation, disruption, and destruction.[92] For the purposes of providing a simple, working definition, this paper will adopt the Department of Defense's definition of information operations as limited by the categorization of cyber attack.[93] The terms information warfare and cyber warfare will be used interchangeably. In this section, I will discuss armed conflict as contrasted with espionage and cyber crime, the types of information attacks, and which of these attacks fall within the scope of armed conflict.

A. Armed Conflict, Espionage or Criminal Activity?

It is sometimes difficult to determine if a cyber attack constitutes armed conflict, covert intelligence gathering, or merely cybercrime, because many of the same techniques and weapons are used to perpetrate each type of action. The LoAC applies to armed conflicts, briefly addresses

---

[92] *See* John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort,* U.S. Department of Defense (Jun. 16, 2011), http://www.defense.gov/news/newsarticle.aspx?id=64349.

[93] Independent authors have posited definitions that segregate offensive acts from rudimentary operations. The term "offensive ruinous information warfare" was used by Dorothy Denning to describe "organized deliberate military effort to totally destroy the military information capabilities, industrial and manufacturing information infrastructure, and information technology-based civilian and government economic activities of a target nation, region, or population. *See* Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179 (2006) [hereinafter Brown]] (*Quoting* Michael Erbschloe, INFORMATION WARFARE: HOW TO SURVIVE CYBER ATTACKS 125 (2001). Ivan Goldberg proposed the nuanced definition of "information warfare" as "the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries. Dr. Ivan K. Goldberg, *Glossary of Information Warfare Terms,* http://www.psycom.net/iwar.2.html. Eric Jensen described "computer network attacks," as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." *See* Brown (*Quoting* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L. L. 208 (2002)). An important distinction is made in these definitions, which describes destructive acts rather than merely passive intrusion. Any operative definition of cyber warfare allows this distinction to necessarily be drawn.

espionage and does not apply to crime that does not rise to the level of war crime.[94] Therefore, the type of action commenced determines how the LoAC applies to parties involved in an information attack. Proper application of the LoAC to the digital battle space requires that participants are able to recognize the type of action in question. The following sections address what armed conflict, espionage, and crime look like in an information warfare setting.

i. *Armed Conflict*

The scope of armed conflict is reasonably extended to non-physical warfare through a results-based approach. The use of digital weapons to achieve military objectives does not comport with our traditional notions of "arms" as physical objects such as spears, guns, crossbows and tanks, making it difficult to conceptualize cyber attacks as armed conflict. This is not the first time that legal scholars and military lawyers have confronted the problem of the militarized use of non-physical weapons.[95] The advent of biological, chemical and electromagnetic pulse technologies also presented the question of whether or not a non-physical attack constitutes armed conflict. Enemy military personnel are presumed to be combatants, so attacks of any nature on military targets are, by default, conducted in the course of armed conflict.[96] But, a commonly held view is that armed conflict does not necessitate physical force. Non-physical attacks are conducted in the course of armed conflict if the resulting damage could

---

[94] *See* Brown, *supra* note 93, at 187-189.

[95] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, OPINION PAPER: HOW IS THE TERM "ARMED CONFLICT" DEFINED IN INTERNATIONAL HUMANITARIAN LAW?, International Committee of the Red Cross (Mar. 2008), available at: http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

[96] *See* Hague Convention IV Respecting the Laws and Customs of War on Land, and its annex: Regulation Concerning the Laws and Customs of War on Land, arts. 1-3, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague Convention IV].

have been produced with guns and bombs.[97] This is a results-based classification of offensive actions, and is thus consistent with the DoD approach to defining information warfare attacks.[98]

Another classification proposes an extension of the results based approach and particularly focuses on the effects a non-physical attack has on the civilian population or otherwise protected persons or property.[99] The expanded approach broadens the scope of armed conflict to include actions that have effects on civilian populations as well as military personnel, such as destruction of emergency services dispatch computers, reprogramming of traffic patterns and forced stock market crashes.[100] Though some scholars protest the expansion of the definition of armed conflict into this area, arguing that adoption of such liberal interpretations presents a slippery slope, the LoAC seems intrinsically protective of civilian populations, making an civilian-effects based approach consistent with the goals of the LoAC.[101] The United States DoD recognizes this expanded approach and states that the deliberate acts of a belligerent, which "cause injury, death, damage, and destruction to the military forces, citizens, and property of the

---

[97] *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES, 362-63 (1963).; Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STAN. J. INT'L. L. 208 (2002) [hereinafter Jensen].

[98] "DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems." U.S. DEPT. OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, (Jul. 2011) available at http://www.defense.gov/news/d20110714 cyber.pdf [hereinafter DoD Cyber Strategy].

[99] *See e.g.*, Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the* Jus in Bello, 76 INT'L L. STUD. 187, 196-197 (2002) [hereinafter Schmitt].

[100] *Id.*

[101] *See* Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter,* 76 INT'L. L. STUD. 73 (2002).

other belligerent . . . are likely to be judged by applying traditional law of war principles."[102] For the purposes of this paper, I adopt the extended definition of armed conflict used by the U.S. Department of Defense.

ii. *Espionage and Military Intelligence Operations*

International law and the LoAC do not prohibit intelligence gathering and espionage activities.[103] Intelligence gathering operations by means such as open disclosure, accessing public networks, signal processing, and satellite monitoring is internationally accepted as a necessary part of military operations.[104] Espionage, on the other hand, is the "covert collection of information about other nations," and is not limited to the use of internationally accepted methods of information acquisition.[105] Both approaches are encompassed in the Hague Convention, which states that "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country" are acceptable during armed conflict.[106] International law and the LoAC have not yet addressed the legality of espionage operations during peacetime.

The difference between intelligence gathering and espionage hinges on the status of the actor. A spy is one who, "acting clandestinely or on false pretenses . . . obtains or endeavors to obtain information in the zone of operations of a belligerent, with the intention of

---

[102] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] Hague Convention IV, *supra* note 96, at art. 24

communicating it to the hostile party."[107] But uniformed military personnel engaging in intelligence gathering in enemy territory do not commit espionage because they do not act clandestinely.[108] Many nations have domestic laws that permit the punishment and/or execution of captured spies. Conversely, the Hague Convention prohibits the execution of military personnel captured while gathering intelligence.[109] It is therefore imperative that there is a clear definitional difference between persons committing digital espionage versus military intelligence gathering.

Rules regarding the perpetration of espionage have limited application to information warfare scenarios. This is largely due to the requirements that the perpetrator acts clandestinely and within enemy territory. Primary advantages of information attacks are the range at which they can be commenced and the anonymity they provide. It would be rare for an attacker to be physically located within enemy territory and acting under subterfuge. Aside from the limited situation where an enemy operative, disguised as a worker, steals files off a computer in enemy territory, it is unlikely that digital intelligence gathering will commence behind enemy lines. Furthermore, information acquisition performed by uniformed military personnel cannot be construed as espionage; thus, an operation performed by such personnel that does not "influence, disrupt, corrupt, or usurp" a nation's decision-making is not accurately described as either espionage or an information attack. Operations of this nature are best construed as military intelligence gathering.

---

[107] Hague Convention IV, *supra* note 96, at art. 29.

[108] *See* Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, art. 52, para. 2, 1125 U.N.T.S. 3.

[109] *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

iii. *Criminal Activity*

Information attacks perpetrated by civilian actors are cyber crimes and do not fall within the purview of the LoAC. The national laws of each country address the scope of cyber crime and the punishments associated therewith. International efforts between the United States and Europe suggested norms and regulations for normalizing how cyber crime is addressed in individual countries but these suggestions have not been formally adopted in many nations.[110] The types of actions that constitute cyber crime vary greatly across the international community. In the United States, citizens are entitled to unfettered access to Internet websites but engaging in unauthorized access to networks is a crime.[111] By contrast, Chinese citizens must access the Internet through elaborate content filtering systems and accessing unapproved websites is a crime.[112] The commission of a cyber attack by an individual or group of individuals in one nation against a target in an enemy country will likely be construed as cyber crime. It is conceivable that such attacks could rise to the level of war crimes by causing widespread damage or death. In

[110] "In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law[.]" BARACK OBAMA, PRES. OF THE U.S., INTERNATIONAL POLICY FOR CYBERSPACE: PROSPERITY, SECURITY AND OPENNESS IN A NETWORKED WORLD, 13 (May 2011) available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter White House Cyberspace Policy]; *see also* Council of Europe, Convention on Cybercrime, arts. 2-6, Nov. 23, 2001, E.T.S. No. 18.

[111] Computer Fraud and Abuse Act, 18 USC § 1030 (a)(2)-(3) (1996) (last amended 2004).

[112] S*ee* Congressional - Executive Commission of China, I*nternational Agreements and Domestic Legislation Affecting Freedom of Expression*, Congressional - Executive Commission of China Virtual Academy (Apr. 5, 2006); *contra* Jack L. Qiu, *Virtual Censorship in China: Keeping the Gate Between the Cyberspaces*. INT'L. J. COMM. L. & POL., 4.(Winter 1999).

such cases the LoAC would apply and the civilian actor tried by military tribunal instead of by domestic courts.

iv. Is Information Warfare Armed Conflict?

Whether information warfare constitutes armed conflict is a threshold question for determining the applicability of the LoAC to various information attack scenarios. Only attacks committed in the course of armed conflict are subject to the rules, regulations and norms embodied in the LoAC.[113] As discussed above, attacks that "cause injury, death, damage, and destruction to the military forces, citizens, and property of a belligerent" are committed in the course of armed conflict.[114] Some information attacks are easily described as armed conflict, while others are better classified as espionage, intelligence gathering, or cyber crime.

B. Types of Information Warfare

Traditional attacks based on physical force are often described according to their origin and/or associated weaponry (i.e. a U.S. Air strike on Afghanistan), because these factors are descriptive and easily determinable. This approach is problematic in information warfare because conventional weapons such as guns and bombs are replaced with computers and data streams, and the attackers are often unknown.[115] Due to the complexity of modern cyber attacks, it is easiest to characterize types of cyber attacks according to the result of the attack. This section discusses the results-oriented approach employed by the U.S. DoD for categorizing types of information warfare attacks, breaking them down into attacks that are primarily exploitative,

[113] *See generally* Walker, *supra* note 53.

[114] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

[115] *See* Jensen, *supra* note 97, at 222.

destructive or disruptive.[116]

i. *Exploitation*

At present, the largest threat to American cyber security comes from exploitation attacks resulting in the theft of information and intellectual property from government and commercial networks.[117] The list of private sector victims of exploitation attacks includes Lockheed Martin, Google, Citibank, the International Monetary Fund, NASDAQ, and members of the oil and gas industries.[118] The government sector has suffered an alarming number of intrusions to agencies such as the Department of Defense, NASA, the Department of Energy, and Army Aviation and Missile command.[119]

---

[116] DoD Cyber Strategy, *supra* note 98.

[117] Lynn's Remarks, *supra* note 1.

[118] John D. Banusiewicz, *Lynn Outlines New Cyber Security Effort*, U.S. Dep't of Def. (June 16, 2011), http://www.defense.gov/news/newsarticle.aspx?id=6434964349 [hereinafter Banusiewicz].

[119] The "Moonlight Maze" attack involved Russian hackers who probed networks at NASA, the Department of Energy, the Department of Defense and others starting in 1998. Intelligence stolen may have included Navy passcodes and missile guidance data. Though the attack seemed to stem from the Russian Academy of Sciences, the Department of Defense suspected a state sponsored effort to obtain classified U.S. defense technology secrets. *See* Gregory Vistica, *We're in the middle of a Cyber War!*, NEWSWEEK, (Sept. 19,1999)*; see also* Schaap, *supra* note 48, at 134; *see also* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L. L. 825, 840 (2001). In the "Titan Rain" incident Chinese hackers broke into U.S. defense systems starting in 2003. The hackers are thought to have stolen U.S. military secrets from the Redstone Arsenal, home to the Army Aviation and Missile Command, including aviation specifications and flight-planning software. The methodologies used by the attackers lead experts to suspect that the attacks had military origins. *See* Schaap, *supra* note 48, at 134; *see also* Tom Espiner, *Security experts Lift Lid on Chinese hack attacks*, ZDNET.COM (Nov. 23, 2005), http://news.zdnet.com/2100-1009_22-145763.html.

Exploitation attacks primarily utilize flaws in software design or implementation to gain access to restricted data. When software is written, the code defines specific steps that a computer must execute to obtain a desired result. If these steps are not well defined or specific enough, attackers may be able to skip the step and obtain unauthorized access. In a simple example, a piece of software may be designed to restrict access to tank blueprints to only those users having IP addresses between 12.34.567.005 and 12.34.567.009. If the software programmer code included a step to check that the last three digits of the IP address are greater than five, but forgot to include a step that checks if the last three digits are less than nine, then anyone with the IP address 12.34.567.005 to 12.34.567.999 can access the restricted tank blueprints.

In complicated real world settings, vulnerabilities in government and commercial networks are difficult for attackers to casually manipulate. Attackers must utilize additional tools referred to as "exploits." These are chunks of software code, data, or data sequences that cause unintended results to occur when the legitimate software is executed. Other methods of obtaining access to restricted data such as "IP spoofing" involve exploiting the ignorance of a legitimate user by tricking them into divulging information.[120] Once an attacker can control legitimate software or access information, he or she can obtain files such as engineering schematics, passcodes, research data, and the like.

The "theft of intellectual property threatens national competitiveness and the innovation

[120] IP Spoofing involves an attacker who masquerades as a trusted host computer to hide his identity. The method can be used to hijack networks, web browsers, and web pages themselves, thereby providing the attacker with access to potentially restricted content. "When IP spoofing is used to hijack a browser, a visitor who types in the uniform resource locator (URL) of a legitimate site is taken to a fraudulent web page created by the hijacker. If the user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. *See* Schaap, *supra* note 48, at 134.

that drives it."[121] The estimated economic loss due to exploitation attacks is over a trillion dollars in the United States alone.[122] This number does not contemplate the threat to national security posed by loss of intelligence, weapons schematics and defense strategy. There is no way of knowing how information gleaned through an exploitative attack will be disseminated and utilized. Hostile nations may use such information to gain competitive edge in defense industry markets or financial sectors. Weapons technology information may be used to develop counter-measures, thereby reducing the effectiveness of the victim nation's offensive military technology. Unlike conventional weapon attacks, the deleterious effects of exploitative information warfare may be long lasting, unpredictable, and widespread, making these attacks exceptionally dangerous to a nation's military operations.

Though dangerous to national security and economic prosperity, exploitative attacks will not generally fall within the scope of armed conflict. The exploitation of computer software and hardware vulnerabilities to gain access to restricted information and computer systems is not likely to cause injury, death, or damage akin to attacks using bombs and guns. It is feasible that an armed combatant could enter a military complex and demand tank blueprints or military intelligence at gunpoint, but such an operation would not be covert and thus the intelligence obtained necessarily limited. It is a stretch of the imagination to assume that exploitation attacks are an equivalent substitute for guns and bombs in information gathering operations. Any attempt at classifying exploitative attacks as armed conflict would thus depend on the attack causing damage to the military or civilian population, protected persons or property. Theft of military secrets could have direct repercussions on military and civilian populations alike, but exigency is

[121] White House Cyberspace Policy, *supra* note 111, at 4.

[122] Lynn's Remarks, *supra* note 1.

a problem. Even though the loss of military weapons schematics could potentially cause economic losses to civilian contractors and allow enemy militaries to gain competitive advantage, these effects are not immediately and directly deleterious to the civilian population. Thus, there is a causality problem that arises from the indirect nature of the damage of an exploitation attack. Whether an effect is adequately immediate and direct may depend on the lapse of time between the attack and the resulting harm and whether the attack directly affects the protected target(s). It is highly unlikely that the bulk of exploitation attacks will rise above the level of intelligence gathering or espionage, so the LoAC will apply minimally.[123]

ii. *Destruction*

The most fear-inspiring cyber assault scenarios arise from attacks that result in serious physical damage, known as destructive attacks.[124] These attacks use digital tools to cause physical destruction of control system equipment, network infrastructure, and in extreme cases the destruction may target geographical locations and the local human population. It is this type of strategy that Stuxnet attackers utilized when they corrupted the orders given to control system software, making the uranium centrifuges spin out of control.[125] Depending on the function of the target computer the damage caused could range from the simple cost of replacement to widespread casualties.

To cause physical damage to property with digital weapons, attackers must either alter the operation or cause the self-destruction of a computer. A particularly effective destructive attack might use exploitative methods to gain restricted access to the operations control system of a

[123] *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

[124] Banusiewicz, *supra* note 119.

[125] Fildes, *supra* note 7.

computer responsible for the cooling system at a nuclear power plant. A communications link between the control system computer and the outside world could be opened to allow remote users to access the machine. A remote attacker could then disable the cooling system, resulting in a nuclear meltdown that devastates the surrounding environment.[126] The Department of Energy attempted to simulate the effects of this type of attack by executing a control hacking incident on a nuclear power plant.[127] The ease with which the hackers were able to throw the generator's control system out of control alarmed intelligence and defense agencies across the United States.[128]

Alternatively, attackers can destroy a control system computer rather than manipulate its standard function. This can be accomplished through a variety of methods, one of which is referred to as a "permanent denial of service" (PDoS) attack.[129] Such attacks target the computer's hardware in an attempt to overload that hardware until it shuts down. Unlike methods that force manual reboot of a computer, PDoS attacks result in destruction of the host computer that requires replacement of the equipment.[130] The end result of an attack on computer hardware may be the same as one that subverts system software to cause destruction, but the victim's ability to recover may differ according to the methods used. If only the system software has been

---

[126] *See generally* Jensen, *supra* note 97, at 222; *see also* Brown, *supra* note 93, at 186.

[127] *See* Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/pow er.at.risk/index.html [hereinafter Meserve].

[128] *Id.*

[129] *See* Schaap, *supra* note 48, at 134.

[130] *Id.*

tampered with, personnel may be able to restart the affected computer or shut down a specific function. In the case of a permanent hardware disablement that destroys the host computer, the victims may be left with little or no recourse for stopping the resulting damage.

The potential for abuse of destructive information attacks is increasing. Though destructive attacks have been simulated, the U.S. Department of Defense asserts that, to date, no destructive cyber attacks have been used by military powers.[131] The current balance of cyber power lies primarily within the militaries of nation states and "the most malicious actors have not yet obtained the most harmful capabilities[.]"[132] This balance of power is unlikely to last forever due to the shrinking cost of computer systems and the increasing influence of the Internet in countries that harbor terrorist groups. As cyber weapons continue to develop in strength and ease of use, the danger to populations around the world will continue to escalate.

Destructive attacks are best classified as part of armed conflict. By definition, destructive attacks cause destruction of computer systems, infrastructure and even physical property. A properly executed destructive attack could destroy or permanently disable military systems, power plants and dam lock controls. The targeted application of small bombs or men with assault rifles could also take out these targets. A computer system destroyed by a deliberately instigated electrical short is just as useless as guns or bombs used to physically destroy the system. Destructive attacks are armed conflict because they cause injury, death, or damage to military forces, citizens, or property of a belligerent and thus fall within the purview of the LoAC.[133]

---

[131] Lynn's Remarks, *supra* note 1.

[132] *Id.*

[133] *See* Assessment of International Legal Issues, *supra* note 44, at 6.

iii. *Disruption*

Disruptive attacks deny or degrade the functioning of government or commercial networks.[134] Potential targets may include essential infrastructure such as, public utilities, financial services, defense operations, and communications networks. The disruption of any of these services can trigger a detrimental domino effect to military and civilian communities alike. It was this type of attack that hackers used to disrupt infrastructure accessibility in the Estonia and Georgia incidents.

The most common method used to execute a disruptive attack is the aptly named "denial of service" attack.[135] The term "denial of service" (DoS) refers to a family of offensive methodologies that attempt to overwhelm a target computer system to prevent it from operating normally. An attacker utilizing the DoS method sends a flood of fake communications requests, in the form of digital packets, to a server on a target network. The target system uses its resources to process the data as though it were received during the normal course of operations. Eventually, the server becomes overloaded with the effort to receive and respond to the phony messages, no longer being able to handle legitimate requests from others. If too much traffic is directed at the server, it may crash and remain inoperable until manually restarted.

The effectiveness of the method is increased with the use of botnets, or collections of

---

[134] Banusiewicz, *supra* note 119.

[135] *See* Mindi McDowell, *Understanding Denial-of-Service Attacks*, US-CERT (November 04, 2009), http://www.us-cert.gov/ncas/tips/st04-015. http://www.us-cert.gov/cas/tips/ST04-015.html

numerous computers to execute multiple DoS attacks on the same server.[136] Computers in a botnet are compromised through exploitative methods to allow a remote operator to control some of the computer's resources**.** Using a botnet, an attacker can flood a target system with many times the amount of data communications requests that could be sent with just a single computer. This type of concentrated effort is known as a "distributed denial of service attack" (DDos) and is used against large targets with robust networks such as those employed by commercial Internet websites, government agencies, and emergency services.

A preemptive disruptive attack against an enemy's critical service infrastructure could drastically reduce their ability to effectively respond to subsequent physical attacks. If the dispatch routing servers for 911 emergency calls were shut down in a disruptive attack, local civilian and military personnel would be unable to receive and respond to calls for help. Attackers could execute disruptive attacks against traffic signal control systems responsible for signal timing, equipment diagnostics, and traffic system performance. Without an operable signal control, system traffic lights would perform erratically causing serious problems in metropolitan areas. Air traffic control systems could be disrupted, preventing aircrafts from landing for dangerously lengthy periods. Many of these services can be remotely managed, making them vulnerable to offensive attempts to subvert control systems.[137]

Disruptive attacks can also target the flow of information rather than services. Attackers

[136] A remote attacker can control compromised computers from a distance. To compromise the computers, viruses may be used to open up connection points (backdoors) on a user's computer that would otherwise be closed. An attacker may then connect to the compromised computer through the open connection and launch DoS attacks at the target server. Many viruses are self-replicating and can spread to other computers, further increasing an attacker's arsenal. *See Id.*; *see also* Schaap, *supra* note 48, at 134.

[137] *Se* Meserve, *supra* note 128.

can shutdown media and government websites or hijack those websites for the purposes of disseminating the attackers' own information.[138] Television and radio signals can also be hijacked and supplanted with a phony signal. By taking over the news media and Internet press, an enemy military can make false statements about the status of fighting, the whereabouts of government officials, culpability for attacks, and whatever propaganda the attackers choose to spread.[139] Such information disruption can result in reduced awareness of the civilian population and increased disorganization during a physical assault. The LoAC prohibits the hijacking of telecommunications signals, but the prohibition is unlikely to stop terrorist groups from utilizing the tactic. [140]

Strategic use and timing of a disruptive attack can mitigate the loss of human life or increase the destructive toll. A disruptive attack's range of effects may vary from public confusion and disorientation, to numerous casualties due to loss of power, water, and access to first responders. Preemptive cyber strikes could reduce casualties by impairing a defender's ability to exert resistance to physical attacks, making it easy for invaders to seize control. On the other hand, these reduced response capabilities could open the door for malicious attackers to commit acts of mass slaughter. Whether or not disruptive cyber attacks are more humane than physical actions lies in the hands of an attacker.

Disruptive attacks are difficult to characterize because their results vary, but they will

---

[138] *See e.g.*, Rob Taylor, Reuters, *Hackers Take Over Taliban Website*, London Free Press (Apr. 27, 2012), http://www.lfpress.com/news/world/2012/ 04/27/ 19686051.html.

[139] *Id.*

[140] Passing yourself off as a government entity and alluding to armistices or ceasefires that have not actually occurred have been determined by US DoD to be a war crime. *See* Assessment of International Legal Issues, *supra* note 44.

generally be classified as armed conflict. A disruptive attack that degrades or disrupts services of critical infrastructure like air traffic control systems, utilities accessibility or first responder dispatches could have disastrous effects on both military and civilian populations. In one situation, first responders could be technologically cut off and unable to address distress calls. Alternatively, the attack might only stymie the flow of service just enough to cause a distraction that facilitates an easy ground invasion. In such a situation, Emergency calls may experience excessive disconnections or improper addresses transmitted to first responder vehicles. In the first scenario, it is fairly easy to imagine that injury, death or damage could result from the disruption. The second scenario, however, is not easily analogized to conventional arms. It seems farfetched that armed military personnel would invade a first responder dispatch without killing anyone and instruct the operators to arbitrarily send callers away. Guns and bombs are not reasonable means of obtaining these objectives; therefore, injury or death are not inevitable results. Thus, disruptive attacks at this end of the spectrum must be considered in view of the resulting damage to military or civilian populations, protected persons or property.[141] More often than not, attacks perpetrated by a state actor that degrade or disrupt services in another state will cause damage to protected persons or property. These attacks are therefore conducted in the course of armed conflict and the LoAC applies to their commission.

C. Conclusion

As I have discussed above, information warfare is an effective and rapidly evolving means of commencing armed conflict. Whether or not an action is committed in the course of armed conflict is dependent on the status of the actor, the place of the action, and the nature of the action. Information attacks conducted in the course of armed conflict should be subject to

[141] *Id.*

the LoAC in the same manner as other forms of armed conflict. In the subsequent section I will analyze the application of the LoAC to issues arising from information warfare scenarios that involve neutral nations.

4. Analysis

The Hague Conventions are applicable to digital armed conflict in much the same way as they apply to physical conflicts. Some of the rules and regulations set forth in the Hague Conventions are easily extended to the digital battlefield, while others require adjustment and adaptation. Neutral states must act as designated by the duties and obligations assigned to them by the LoAC, even when the modality of war is the digital battle space. All belligerents must respect the inviolability of the land, property and citizens of a neutral state, regardless of whether the weapons used are physical or digital. In this section, I will discuss and analyze the duties and obligations of neutral states in information warfare and apply them to the information attacks discussed at the beginning of this paper.

A. How Information Warfare Affects the Privileges and Immunities of a Neutral State

Digital communications by a belligerent that utilize a neutral state's Internet infrastructure will potentially violate the principle of neutrality. Users of the Internet cannot control the paths that their information takes before reaching the intended destination.[142] Data sent from a single source may be broken up into smaller groups and sent along different paths

[142] The Defense Advanced Research Projects Agency ("DARPA") is developing Internet modifications in the form of "active networks." Active networks can permit users more choice in the routing of their data by supplying their own instructions and requirements for path selection. *See Active Networks*, LINKTIONARY.COM (2001), http://www.linktionary.com/a/active_network.html.

before being reassembled at the end of the journey.[143] The data transmissions of a belligerent state could travel through many states, including the Internet infrastructure of a neutral state, thereby trespassing on the neutral's territory.

Unaggressive transmissions such as correspondence of information and intelligence transmitted from a belligerent state will not violate the principle of neutrality. This is because the Hague Convention provides that neutrals may allow use of their telegraphy systems by all belligerents.[144] The analogy between transmitting telegraphs over wire is easily extended to sending emails over fiber-optic cable. Indeed, the United States DoD has already adopted the extension of the telegraphy provision to modern communications systems.[145] Thus, a belligerent's Internet transmission of an informative nature will not violate the principles of neutrality if it crosses the boundaries of a neutral's territory.

Conversely, information attacks that utilize the Internet infrastructure of a neutral state violate the principle of neutrality. The primary privilege of neutrality is inviolability of territory.[146] A strict interpretation of this rule indicates that belligerents may not move munitions or troops of any kind, across the territory of a neutral state.[147] Cyber weapons are small and digital, but they can be used to destroy infrastructure, property and even cause death.[148] If a

---

[143] *See* George K. Walker, *Information Warfare and Neutrality,* 33 VAND. J. TRANSNAT'L L. 1079, 1199 (2000).

[144] Hague Convention V, *supra* note 51, at art. 8.

[145] Assessment of International Legal Issues, *supra* note 44.

[146] Hague Convention V, *supra* note 51, at art. 2.

[147] *See* Hague Convention V, *supra* note 50, at art. 2; *see also* Brown, *supra* note 93.

[148] Weapons are "devices designed to kill, injure, or disable people, or to damage or destroy property," U.S. Dept. of Air Force Policy Dir. 51-54, *Compliance with the Law of Armed*

belligerent state launches an information attack that moves cyber weapons across a neutral's Internet infrastructure, then the belligerent violates Article Two of the 1907 Hague Convention V. The violation occurs regardless of the belligerent's inability to control the transmission pathway of the attack. As a result of the current scheme for Internet traffic routing, belligerent states may inadvertently violate the principle of neutrality when using information warfare.

Like offensive information attacks, a belligerent's espionage and military intelligence gathering operations may not utilize neutral communications infrastructure. Exploitative attacks, best characterized as military intelligence gathering, or espionage, do not generally rise to the level of armed conflict.[149] Even so, the Hague Convention does provide some guidance to signatory nations on how to treat belligerent intelligence gathering activities. The Hague Convention states that such activities are "necessary" aspects of warfare, and prohibits a neutral from allowing belligerents to make aerial or sea-based observations of enemy forces, from within the neutral's territory.[150] This suggests that neutrals should not allow belligerent forces to utilize a neutral's territory even for non-offensive purposes. The premise is easily extended to the digital battlefield. If physical weapons are disallowed, then digital weapons are disallowed. If physical surveillance is disallowed, so too is digital surveillance. Therefore, a belligerent's use of neutral Internet infrastructure to conduct intelligence gathering on enemy forces will violate the principle of neutrality.

Conflict, 6.5 (Aug. 4 2011), available at: http://www.e-publishing.af.mil/shared/media/epubs/afpd51 -4.pdf.

[149] The provisions of the Hague Convention addressing espionage are more applicable to exploitative attacks than provisions addressing armed conflict. *See* Hague Convention IV, *supra* note 100, at arts. 30-31.

[150] *See* Hague Convention IV, *supra* note 100 at art. 24; Hague Air Rules, *supra* note 51 at Art. 47.

B. **What's a Neutral to Do?**

A neutral's duty to respond to information attacks that utilize the neutral's computer systems and Internet pathways is dependent on the situation. Unlike ground invasion, digital invasion presents a number of issues that would make a bright line "duty to repel" impracticable. The breakdown in real-world practicality of applying the most applicable Hague provision should not prohibit the application of other provisions that are better suited to the digital battlefield. Analogies can be drawn between information attack scenarios and situations in the physical realm that provoke a duty to remain impartial, intervene, or repel. Utilizing these analogies to adapt the existing framework of the LoAC to information warfare provides a means for addressing the potential problem of neutrality violations. In the rapidly developing arena of information warfare, it will be far more cost effective and time efficient to adapt existing frameworks rather than developing entirely new approaches, as the slow pace of international law development is likely to render treaties on information warfare obsolete before signing is complete.

There are multiple logistical issues that make digital violations different from physical violations of a neutral's territory. The problems of notification and attribution must be addressed before a neutral state can decide on the proper response to a violation of its neutrality. As a practical matter, for a neutral state to respond according to its duty under the Hague Conventions, it must be aware that an event is occurring that necessitates action by the neutral and it must know that the perpetrator of the event is a belligerent state. If a neutral state does not have notice that an attack is occurring or know the identity of the attacker, the neutral cannot be certain that an obligation to act exists.

The complexity of data routing through the Internet and the speed at which data travels

make real-time assessment of information attacks nearly impossible. Files are split up into small data packets that can travel a multitude of different paths on their way to their intended target.[151] Data packets travel at blinding speeds through a vast web of interconnections, existing in each location for portions of a second. By the time an information attack occurs, the digital weapons have already transited intermediate territories. Consequently, countries caught in the middle of an information attack are advised of their unwitting participation well after the attack is over. A middleman country rarely receives notice that it is being victimized while an attack is occurring. To find both the responsible and unaffiliated participants of an attack, computer forensics experts carefully trace the route of the attack backwards by examining data traffic at each stopping point in succession. This process can take months depending on the complexity of the attack and the routes used. Thus, significant lapses in time can occur between the actual violation of a neutral's digital territory and the time at which the neutral becomes aware of the violation.

Likewise, it may take a substantial portion of time before the perpetrator of the attack is discovered. The process of tracing the attack backwards along its path is time consuming at best. At worst, the trail is so obscured that no discernible initiation point is found. It could take days, weeks, months or even years to discover the location of computers used to initiate an attack. The location of an attack's starting point does not necessarily mean that the attacker is from that location or that the actor is a state rather than an individual or group. Perpetrating computers located on military bases are obvious indicia of state action, but computers belonging to administrative agencies or state-run businesses will not provide a firm connection between the state and the action because a private individual could access the computers without state authorization. Neutral states caught in the middle of a cyber attack may wait lengthy periods of

[151] Walker, *supra* note 53, at 1098.

time before discovering which belligerent(s) initiated the attack. In some cases the neutral state may never know the perpetrator's identity. Without attributing the attack to a specific belligerent, the neutral may be unable to effectively execute its duty to act.

A neutral's first duty is to remain impartial to all belligerents, particularly with respect to telecommunications and e-commerce. Belligerents using a neutral state's Internet infrastructure for unaggressive telecommunications purposes do not violate the principle of neutrality. Consequently, neutrals do not have a sufficient legal reason for denying specific belligerents access to Internet infrastructure and telecommunications means. Access to the neutral's telecommunications means must be available to or denied to all belligerents.[152] If preference is given to one belligerent over another, the neutral state violates its duty to remain impartial. To avoid neglecting this duty, the neutral must take steps to ensure that Internet Service Providers (ISPs) and telecommunications companies within the state do not filter, block or degrade bandwidth availability to belligerents individually.[153] This can be accomplished by a state-issued notice or temporary regulation prohibiting discriminatory behaviors during the course of the conflict.[154] Any Internet infrastructure located within a neutral's territory but owned by a belligerent must be shut down unless the owners agree to make the service available publicly and impartially.[155] Similarly, private companies in the neutral state can export arms, munitions, and

[152] *See* Hague Convention V, *supra* note 50, at art. 3, 8.

[153] *See id.* at art. 8-9.

[154] I find it highly unlikely that the duty extends to making the neutral government "hand check" each ISP on a regular basis to ensure compliance. The resulting administrative burden would be unreasonable and I was unable to find a single example of such behavior with respect to the telegraphy lines described in the Hague Convention.

[155] Hague Convention V, *supra* note 50, at art. 3.

supplies to belligerent forces as long as the goods are equally available to all belligerents.[156] On the digital battlefield, such trade goods could comprise network defense software and code for digital weapons. The sale of these items can be physical or completed over the Internet, with the goods themselves available for download by belligerents. Restriction of a belligerent's access to the neutral state's Internet infrastructure would make online purchases of digital defensive and offensive goods difficult, resulting in the violation of the neutral's duty to remain impartial with respect to export of goods of war. The best way for a neutral state to reduce the risk of inadvertent violation of its duty to remain impartial is for the state to provide actual notice to ISPs, telecommunications companies, and private businesses dealing in software or network services, communicating that all belligerents must be treated equally and without preference for the duration of the conflict. It is unreasonable to require that a neutral perform regular monitoring of each of these sectors for impartiality, but if a belligerent asserts that other belligerents receive preferential treatment with respect to Internet infrastructure access, the neutral state must act decisively to correct the error.

The next duty, the duty to intervene in belligerent operations on neutral territory, imposes an active intermediary role on a neutral state. A neutral must intern ships, planes and ground forces found within its borders to prevent belligerent attacks from originating within the neutral's territory.[157] Digital weapons, like their physical counterparts, must not be allowed to leave the neutral's territory once the weapons are discovered. Similarly, any attacks on belligerents that originate from within a neutral's borders must be disrupted immediately.

Information attacks that involve the use of a neutral's computer systems to launch

[156] Id. at art. 7, 9.

[157] *Supra* §2.c.ii.

offensive operations against a belligerent may be construed as originating from within the neutral's territory. Because neutrals are unlikely to declare neutrality and then deliberately launch attacks against belligerents, it is likely that computer systems used in the attack are compromised to allow remote control by belligerent attackers.[158] Once an attack commences, it may be discovered by an administrator of the compromised computer system or after the attack is over, during an investigation. These are the most probable scenarios for discovering the digital arms and munitions of belligerents within a neutral's territory. As discussed above, attacks merely "passing through" the neutral's Internet infrastructure are moving too fast and erratically to permit detection. In some rare cases, digital weapons such as those triggered to execute at a particular time or in parallel with a trigger event, may be discovered before an attack occurs by a computer system administrator who observes the system's odd behavior.

Intervening in belligerent information operations entails preventing operation of computer systems that would permit attacks or surveillance to commence, continue, or reoccur. The Hague Conventions stipulate that belligerent forces found within a neutral's borders must be interned as far from the theater of war as possible, thereby preventing belligerents from utilizing neutral ground to launch attacks on opposing forces.[159] At sea, neutrals may do what they believe is necessary to prevent belligerent vessels from leaving the neutral's territory in a battle-ready state.[160] With respect to belligerent aircraft on neutral ground, the neutral must use whatever

[158] It is unlikely that states that declare their official neutrality will then, of their own free will, attack belligerent states. This would destroy their neutrality and bring the state into the armed conflict. I therefore assume for the purposes of this analysis that attacks made from within neutral territory are actually perpetrated by outside attackers utilizing remote access to the neutral's computer systems.

[159] *See* Hague Convention V, *supra* note 51, at art. 11.

[160] *See* Hague Convention XIII, *supra* note 51, at art. 24.

means are at its disposal to prevent the aircraft from leaving to execute offensive operations or to obtain surveillance of opposing belligerent forces.[161] The fluid nature of the Internet and its lack of recognizable borders make the digital battle space more like air and sea warfare than traditional land based combat. Standards for aerial and naval warfare are therefore the most appropriate for application to information warfare. Applying these standards to the digital battlefield, a neutral may take actions it deems necessary to stop a potential attack from occurring, but it must use the means at its disposal to prevent an attack that is occurring or is certain to occur without intervention.

In many situations, affected computers can be quarantined and disconnected from the Internet and other computers on its network, thereby removing the computer's ability to transmit and receive data packets. A computer system that cannot transmit data is unable to participate in information attacks. Quarantine of critical computer systems can be tricky and time consuming because system administrators must attempt to prevent the system from engaging in malicious communications while maintaining its ability to engage in vital aspects of its normal operation.

Presently occurring or immediately imminent attacks are matters of exigency that may necessitate immediate intervention. Timely quarantine of affected computer systems is not always sufficient. The fastest way for a neutral to intervene is to shut down computer systems and Internet infrastructure suspected of harboring a belligerent's digital weapons or surveillance. This approach presents serious practicality problems for the neutral because it could mean shutting down systems critical to the operation of the economy, government, and general communication. It is analogous to requiring a neutral to shut down its seaport or blow up its airport to prevent belligerent ships and aircraft from quitting the neutral's supervision. Common

[161] *See also* Hague Air Rules, *supra* note 52, at art. 47.

sense suggests that it would be easier and less costly to the neutral to simply smash a hole in the side of the warship or aircraft and intern the crew. A physical aircraft or ship belonging to a belligerent can be shot down or otherwise damaged, but damaging digital weapons may be difficult or impossible without crippling the neutral's own property. Furthermore, the shutdown of telecommunications systems or Internet infrastructure can create ripple effects that cause service interruptions for countries far removed from the armed conflict.[162]

I propose the more reasonable interpretation of the disposal test to require that a neutral use the means at its disposal to intervene in an ongoing or immediately imminent attack so long as the damage to the neutral would not outweigh the harm to the belligerent. Neutrals are thus obliged to redirect manpower and system capabilities into the effort to quarantine an attacking computer system, but will only be required to shut the system down when timely quarantine is impossible and the harm to the victim belligerent of allowing the attack to continue outweighs the harm to the neutral of shutting the computer system down. A balancing test might seem unwieldy, but situations involving damage to civilian population or loss of human life will clearly outweigh most other interests. Such situations could arise during disruptive or destructive attacks, which can result in severe consequences to the human population of a belligerent state. If a neutral state learns that vital computer systems are being used by a belligerent to obtain intelligence about an opposing belligerent, the neutral would simply need to quarantine the system to the best of its ability, regardless of whether the quarantine is 100% successful. But, if the attack causes loss of human life, the neutral certainly has to shut down the offending computer systems to avoid violating its duty to intervene. By adopting a modified interpretation of the current duty, Hague Convention signatories could provide neutral states with some

[162] *See* Lynn, *supra* note 1.

flexibility in safeguarding their own interest while still meeting their duties under the Hague Conventions.

The final duty, the duty to repel, requires the employment of primarily proactive measures to prevent digital incursions onto a neutral's territory. When belligerent troops trespass on neutral land, the neutral is obligated to repel the trespassers.[163] Belligerent incursions into a neutral's airspace or waterways must be repelled using the means at a neutral's disposal.[164] The Hague Conventions do not specify whether the duty is proactive, reactive, or both. Proactive measures include barricades, sea gates, land and sea mines, and any other measures put in place to prevent a trespass from occurring. Once a trespass occurs, reactive measures using force of arms are employed. In information warfare, proactive measures take the form of firewalls, security software, closing network ports, disabling file sharing, and implementing personnel security measures. These measures are relatively inexpensive when compared to the cost of building barricades. Government agencies and military installations can easily implement such reasonable means of protecting themselves from information attacks and repel some belligerent incursions. Well-trained attackers will thwart even the best security systems, so a neutral's duty to repel cannot be absolute; nor can it end at the installation of security software and firewalls. If a neutral becomes aware of an ongoing attack that utilizes the neutral's Internet infrastructure, it should increase security measures in an attempt to block data traffic coming from the belligerent state. Attacks that continue despite an increase in security measures will trigger the neutral's duty to intervene in the attack. Consequently, the duty to repel requires mostly proactive measures by a neutral, and in the event that such actions fail, the neutral may be forced to intervene in the

[163] *See* Hague Convention V, *supra* note 51, at arts. 1-2, 5.

[164] Hague Convention XIII, *supra* note 51, at Art. 24; Hague Air Rules, *supra* note 52, at Art. 42.

attack with more aggressive measures such as quarantining or shutting down computer systems.

These duties collectively require that neutral states take an active role in preventing their inadvertent participation in an armed conflict. States cannot absolve themselves of liability by declaring neutrality. Where information warfare is concerned, neutrals must preemptively act to protect their Internet infrastructure and telecommunications highways. Neutrals must provide notice to telecommunications companies that their services shall be equally available to all belligerents and the public. The neutral must also adopt security measures to block information attacks from accessing the neutral's communications pathways. In addition to preemptive measures, neutrals must react as expeditiously as possible to intervene in information attacks originating within the neutral's territory.

If the neutral is unable or unwilling to fulfill these duties, belligerents may act in self-defense even if that action involves violating the principle of neutrality.[165] The "right of necessity" permits belligerents to protect themselves from harm when a neutral state is incapable of stopping an opposing belligerent from violating the neutral's territory. Ongoing information attacks that utilize a neutral's Internet infrastructure, computer systems, and telecommunications resources will trigger the neutral's duty to intervene, but the neutral may be unable to effectively quarantine affected services and unwilling to shut them down. The neutral acts appropriately within its duty to intervene if it deems that the harm to the neutral of shutting the systems down outweighs the harm to the belligerent of letting the attack continue. Understandably, the target belligerent's opinion may differ from that of the neutral state. If the belligerent feels that its interest strongly outweighs the neutral's interest and the neutral has not succeeded in repelling

[165] *See* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,* 106 MICH. L. REV. 1427-35 (2008).

the attacks or intervention therein, then the belligerent can take steps to stop the attackers from utilizing neutral resources. Such steps may include blocking Internet traffic from the neutral territory, digital sabotage of affected neutral systems and even physical invasion of the neutral's territory to shut down or destroy the offending systems.

The defensive right of necessity should be used sparingly by belligerents and only in times of exigency. On land, the invasion of neutral territory involves the rerouting of troops and supplies to cut off opposing belligerents on neutral ground. There is an opportunity cost as well as real cost associated with moving armed forces around and engaging the enemy in combat. These costs are drastically reduced in a cyber setting because effective defensive measures may be enacted from afar. The ease of affecting defensive capabilities obscures the danger associated with forcible shut down of potentially critical computer systems without warning. Unanticipated disruption in essential network infrastructure may have disastrous effects on a neutral's economy, utilities, first responder systems, and more. These effects may extend beyond the neutral's borders into other countries, some of which may not be involved in the armed conflict in any way. While belligerents are free to take measures to protect their citizens and their interests, they should think carefully before invoking the right of necessity to shut down neutral systems because the results may be significantly deleterious to the international community.[166]

[166] The United States recently asserted its right of self-defense in cyberspace, stating, "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking

C. Applying The Hague Conventions to Information Warfare Scenarios

Applying a neutral's duties and obligations to real-world scenarios involves subjective decision-making. There are many shades of grey regarding a belligerent's culpability for violating the principle of neutrality that can make it difficult to rationalize harsh intervention or repellant actions in some situations. More importantly, harsh actions responses can cause a degradation of Internet accessibility of countries not involved in the conflict. Neutrals must carefully consider the potential outcomes of their actions and be prepared for the possibility of international outcry arising over the results of a decision. In this section, I examine how a neutral state should act to meet its duties and obligations if involved in the scenarios described in the introduction to this paper. For the purposes of providing uniformity and simplicity, I impose a recognized international armed conflict on each scenario wherein the target state and the proposed actor are belligerents in the armed conflict. In each case, the duties and obligations of a hypothetical neutral state are discussed.

What should a neutral do if its Internet infrastructure was used to perpetrate an exploitative attack on the U.S. Department of Defense that resulted in the theft of a substantial quantity of electronic files? Exploitative attacks are espionage or military intelligence gathering, not armed conflict. If the attacker is a belligerent clandestine agency or military, then the neutral must take action to prevent further incidents of espionage or intelligence gathering. But, if the actor is a private group or individual and the state does not exert "effective control" over the actor, then the attack is merely cyber crime and the LoAC does not dictate the neutral's behavior.[167] Attribution is necessary before determining a proper course of action. This case

broad international support whenever possible." White House Cyberspace Policy, *supra* note 111, at 14.

[167] *See* Hague Convention V, *supra* note 51, at arts. 2-3.

presents a prime example of the problems that attribution can cause. No single state has been blamed for the theft and no evidence has been published that suggests specific actors. The neutral state cannot accurately gauge the extent of its obligation without knowledge of the actor's status as a belligerent. Still, it is best to err on the side of caution and assume that the actor is a belligerent military and a duty exists. The duty requires active participation by the neutral, because the attack has already taken place and proactive measures were ineffective. Was the information attack "just passing through," invoking a duty to repel, or was it utilizing the neutral's computer resources to assist in the execution of the attack, invoking the duty to intervene? The neutral should conduct its own inquiry if possible to determine the answer to this question. If a duty to repel exists, then the neutral must increase security measures and attempt to block traffic from the offending belligerent. If a duty to intervene exists, then the offending computer must be removed from the belligerent's arsenal if reasonably possible.

Because the attack is unknown in this case, repellant measures will be ineffective, making intervention necessary. A neutral state cannot repel attacks by blocking data traffic from a specific country, if the identity of the attacker is unknown. Neutrals cannot arbitrarily block traffic from all potential attackers because doing so denies telecommunications infrastructure to individual belligerents, violating the neutral's duty to remain impartial. The ineffectiveness of repellant measures gives rise to the duty to intervene. Here, the distinction between whether an information attack is passing through or originating within neutral territory is rendered moot by the lack of proper attribution. The neutral is therefore obligated to use the means at its disposal to intervene, so long as the damage to the neutral would not outweigh the harm to the belligerent.

The neutral should balance the cost to both parties of the neutral's intervention in the attack. While the neutral is required to conduct a reasonable investigation to discover computer

systems used in the attack, it does not need to exhaustively scour the digital landscape. Any computer systems identified as facilitating the attack must be shut down or quarantined. The neutral should determine whether systems can be effectively quarantined and, if this is not possible, whether the harm of shutting the systems down outweighs the harm of allowing ongoing theft of U.S. Department of Defense files. Systems vital to the neutral's critical infrastructure should not be shut down because the harm to the neutral would likely outweigh the harm to the United States. The neutral will successfully meet its duty to intervene by performing a reasonable search for participating computer systems and quarantining or disabling those systems to the best of its ability.

What should a neutral do when a belligerent actor employs a destructive information attack to destroy an opposing belligerent's non-critical resources, as in the Stuxnet attack? The Stuxnet worm was directly installed on target computer systems by an undercover operative, making this attack an act of espionage/sabotage rather than armed conflict. Whether the worm was electronically transmitted to or manually carried by the undercover operative, a neutral's territory could be violated during transit.

Once again, attribution is problematic for the neutral. The United States and Israel are suspected culprits but the suspicion is unconfirmed. In the previous example, meeting the duty to repel was impracticable given the lack of attribution, but in this case the neutral can choose to "repel" the U.S. and Israel based on the suspicion that these belligerents are responsible for the attack. Denying Internet accessibility to the U.S. or Israel would likely create the international perception that the neutral chose to side with Iran. Although the neutral would meet its duty under the Hague Conventions, the neutral could suffer serious international relations detriment. Alternatively, the neutral can choose to skip attempts at repelling and move to intervene in the

attack. A reasonable attempt at identifying and quarantining or disabling affected computer systems in accordance with the modified disposal standard will satisfy the neutral's duty to intervene. If intervention is not successful and more worms cross the neutral's borders, the neutral will be forced to repel the U.S. and Israel or risk losing its neutral status.

Lastly, what should a neutral do when its computer systems are used to disrupt essential infrastructure services of a belligerent, as in the Georgia/Estonia conflicts? The attack was attributed to Russia but the actor might be the state or a private group. Private group actors should be dealt with according to international cyber crime treaties, while state actors are addressed in the LoAC. The neutral here is the United States, whose servers were absconded and used in the botnet that launched numerous assaults on Estonian and Georgian network infrastructure. American computers, controlled by Russian attackers, executed repeated disruptive attacks, thereby triggering the U.S.'s duty to intervene and stop attacks from originating within U.S. territory. All involved states are known in this scenario and the neutral's obligation is clear, but this situation displays the problem associated with the timing of notification. The time at which the U.S. became aware of its involvement in the attacks is unclear from public reports. If it knew that its computer systems were compromised while the attack was occurring, the U.S. would be required to quarantine or disable those systems. But, if the U.S. did not receive notice of its involvement until the attacks were over, it would only need to remove remote control capabilities from the affected computers and take proactive measures to prevent attacks from reoccurring. Taking the proscribed action in either circumstance would satisfy the obligations of the U.S., but the extent of required action varies because of the differing levels of exigency.

The U.S. private company's storage of Georgian government data backups during the

Georgian conflict does not violate the U.S.'s neutrality, so long as no digital weapons were stored. The Hague Conventions prohibits belligerents from moving weapons and munitions onto neutral territory but does not restrict the movement of general resources.[168] Belligerents are thus free to store goods on neutral land that are not weapons or munitions of war. Georgian government websites are not digital weapons or munitions. Accordingly, private companies within a neutral state may offer to buy/sell or store belligerent goods without risking the violation of the principle of neutrality.

The application of the Hague Convention's duties and obligations to real world information warfare scenarios illustrates the many nuances of this mode of combat. Neutrals face problems with notice of attacks, attribution of attacks to a particular belligerent, potential damage to the neutral's digital resources, and damage to the neutral's international relations. Often, neutrals will be forced to make decisions on how to respond to an attack within a short period and without all necessary information. The positive side to this form of warfare is the potential for decreased loss of human life; so, even if neutrals suffer a greater rate of error, they may be less likely to make errors that result in loss of human life.

5. Conclusion

The ever-increasing utilization of information warfare will continue to pose a variety of complex legal problems. As technology develops, the spectrum of potential uses for information warfare will broaden. Creation of new applications for weaponized bits and bytes will inevitably result in the generation of new legal questions. The information warfare scenarios discussed in this article are a sample of the possible uses for digital attacks. It does not address every potential

[168] A non-state actor must be "effectively control[led]" by a state actor in order for the actions to be attributed to the state. *Nicaragua v. U.S.,* 1986 I.C.J. 14, (June 27, 1986).

legal factor but instead examines the basis for applying the Law of Armed Conflict to information warfare that involves neutral states. Can the Hague Convention of 1907 and subsequent Hague Rules Regarding Aerial Warfare, as pillars of the LoAC, be reasonably applied to information warfare involving neutral states? Yes. The duties and obligations imposed on neutral states by the Hague Conventions extend to the digital battle space. Information warfare will generally be construed as a form of armed conflict because it can result in injury, death, or damage to military, civilians, and protected property. Some information attacks, such as data theft, will be best categorized as espionage or cyber crime, but most information attacks pose serious physical threats. Information warfare, therefore, will generally fall within the purview of the LoAC. Neutrals thus have a duty to remain impartial, a duty to intervene in harm originating from within their borders, and a duty to repel belligerent forces in any form. Telecommunications services must be offered impartially, compromised computers within the neutral state must not be allowed to contribute to attacks on belligerent states, and pre-emptive measures must be taken to prevent information attacks from utilizing neutral telecommunications infrastructure. If neutrals cannot or will not meet these duties, then belligerents may exercise their right of necessity and take action to shut down neutral telecommunications resources that are used against the belligerent.

Though the LoAC applies to current methods of information warfare, the international community will have to work together to stay abreast of emerging trends in the use of digital weapons. Modification to the existing law of neutrality could be used to guide the actions of neutrals during armed conflicts involving information warfare. Norms that encourage neutral states to consider the legal and social consequences prior to choosing a course of action, will be far more beneficial to the rapidly developing area of warfare than new treaties that cannot fully

contemplate the extent of information warfare's future applications. Indeed, U.S. President Barack Obama stated that existing norms of international conduct in war and peacetime still apply in cyber space, making the re-invention of existing law unnecessary.[169] Nations must collaborate to develop new technologies that improve early warning capabilities and deterrent measures on the Internet.[170] By working together to adjust existing norms and create new technologies, the international community can shape the scope of information warfare, taking advantage of its non-lethal potential to mold a more humane form of war.

[169] White House Cyberspace Policy, *supra* note 111, at 9.

[170] *Id.* at 13.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 3, PAGE 113

Artificial Intelligence and the Patent System: Can a New Tool Render a Once Patentable Idea Obvious?

William Samore

I. Introduction

In the summer of 1956, leaders in the field of computer science met at Dartmouth College and founded the field of Artificial Intelligence.[1] Since then, one branch of Artificial Intelligence—Genetic Programming—has progressed to the point where it could drastically change the way that inventors design and create. Genetic programs (described in more detail in section III.B of this paper) operate by mimicking the biological evolutionary process[2] and have a wide variety of applications.[3] Antenna design, for example, is a field where genetic programming could radically change the nature and pace of innovation.[4] The first antennas were built in the late 1800's by Heinrich Hertz,[5] and an antenna with a specific shape can be designed

[1] *Dartmouth Conferences*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Dartmouth_conference (last visited Oct.23, 2013) (the founders proposed a study which was "to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.").

[2] Anne Eisenberg, What's Next; *When a Gizmo Can Invent a Gizmo*, N.Y. TIMES Nov. 25, 1999 at G9 *available at* http://www.nytimes.com/1999/11/25/technology/what-s-next-when-a-gizmo-can-invent-a-gizmo.html (Stating that genetic programs "solve problems by mimicking the principles of natural biological selection." *Id.*).

[3] *See id.* (listing genetic programming applications such as gas turbine, integrated circuit, and antenna design).

[4] Antenna technology is a good example here not only because of the dramatic ways that the tools that inventors have available to them have changed the way antennas can be designed, but because many antennas are patentable. In fact, the United States Patent and Trademark Office (hereinafter "the PTO"), in its classification system has a class for this: class 343 Communication: Radio Wave Antenna.

[5] *Antenna (radio)*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Antenna(radio) (last visited Oct. 24, 2013).

to emit a desired radiation pattern.[6] As technology progressed, computer programs were designed where an antenna's characteristics could be inputted to the computer program, and the radiation pattern would be calculated and displayed to the user.[7] Now, computer programs have gone one step further, making it possible to do the reverse: input a desired radiation pattern and have the computer program itself design the antenna.[8] The question that this note asks is, can changes in the tools available to inventors render previously patentable ideas obvious and therefore unpatentable?[9] In other words, should an antenna, which could only have been designed by a human at one point but now can be designed by a computer, be patentable?[10]

Part II introduces the reader to patent law. Part II.A discusses patent law in general, and includes an explanation of the derivation of patent rights. Part II.B then explains the legal concept of obviousness—the most relevant concept to patenting a device designed by a genetic program. Part III discusses relevant technological advances, particularly genetic programming. Next, Part IV argues that when genetic programming becomes widespread in a particular field, advances that could be created by the program should be deemed obvious. To provide a practical

---

[6] *Id.*

[7] A quick Google search of "antenna radiation pattern calculator" reveals a multitude of computer programs which can calculate radiation patterns for antennas.

[8] Anne Eisenberg, *What's Next; When a Gizmo Can Invent a Gizmo*, N.Y. TIMES Nov. 25, 1999 at G9 (satellite communications antenna designed).

[9] A separate very interesting question is: should the program itself, which designed the antenna, be patentable? *See* Peter M. Kohlhepp, *When the Invention Is an Inventor: Revitalizing Patentable Subject Matter to Exclude Unpredictable Processes*, 93 MINN. L. REV. 779 (2008) (arguing that a process, such as the computer program that designed the antenna, which produces unpredictable results, is not a process under the meaning of 35 U.S.C. § 101, and therefore is unpatentable.).

[10] It should be noted that genetic programs apply to far more than just antenna technology. *See infra* Part III.B.

application for this argument, Part IV.B sets forth a widespread use test. Part V addresses anticipated contra.

II. Patent Law & Obviousness

A. Patent Law Fundamentals

The United States Constitution grants Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[11] Congress has exercised this power, with respect to technological advances, by enacting patent laws.[12] A patent does not give its owner the right to make or use the patented invention; rather, the patent gives its owner the right to exclude others from making or using the patented invention.[13] This right to exclude provides incentive for inventors to innovate and disclose their ideas to the public.[14]

Bringing ideas to the public domain is patent law's underlying purpose.[15] After an inventor has disclosed his idea to the public in exchange for the right to exclude for a limited time,[16] the patent expires and the public enjoys the benefit of unlimited use of the idea.[17]

---

[11] U.S. CONST. art. I, § 8, cl. 8.

[12] Patent law is governed by Title 35 of The United States Code.

[13] CRAIG A. NARD, THE LAW OF PATENTS 1-2 (2011).

[14] *Id*. at 3 ("[P]atent law can be viewed as a system of laws that offer a potential financial reward as an inducement to invent, to disclose technical information, to invest capital in the innovation process, and to facilitate efficient use and manufacturing of invention through licensing.").

[15] Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 151 (1989) ("The ultimate goal of the patent system is to bring new designs and technologies into the public domain through disclosure"); Nard, *supra* note 13, at 3.

[16] Nard, *supra* note 13, at 3.

[17] *Bonito Boats*, 489 U.S. at 153 ("[A]n article on which the patent has expired[] is in the public domain and may be made and sold by whoever chooses to do so.").

To be patentable, an invention must be novel,[18] useful,[19] and nonobvious.[20] The novelty requirement precludes patentability when the invention is not new.[21] The utility requirement simply "mandates that the invention be operable to achieve useful results."[22] The nonobviousness requirement prohibits patentability when the "claimed invention as a whole would have been obvious."[23] Nonobviousness is explained in more detail in the following section as this requirement is the primary concern of this paper.[24]

B. § 103 obviousness

Even if an invention is novel, an inventor may not obtain a patent if the invention is obvious.[25] While the obviousness requirement was originally created at common law,[26] it was

---

[18] 35 U.S.C. § 102 (2006).

[19] 35 U.S.C. § 101 (2006).

[20] 35 U.S.C. § 103 (2006).

[21] 35 U.S.C. § 102 (2006); *In re* Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently.").

[22] *In re Swartz*, 232 F.3d 862, 863 (Fed. Cir. 2000).

[23] Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 1537 (Fed. Cir. 1983).

[24] Before leaving this section, it would be a mistake not to note that on September 16, 2011 the Leahy-Smith America Invents Act (hereinafter "the AIA") passed into law. *See* Leahy-Smith America Invents Act, H.R. 1249, 112th Cong. (2011) (enacted). While the AIA brought sweeping changes to many areas of patent law (*see Leahy-Smith America Invents Act*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Leahy-Smith_America_Invents_Act (last modified Sept. 22, 2013) (stating that the AIA, among other things, switches the patent system from a "first to invent" system to a "first to file" system, and "revises and expands post-grant procedures")), these changes do not substantially effect this note's topic. The main change from the AIA that does effect this note's topic is that obviousness under 35 U.S.C. § 103 is now determined at the time of filing rather than at the time of invention. This timeframe for obviousness determination will be discussed later in this paper.

[25] 35 U.S.C. § 103 (2006).

eventually codified in 35 U.S.C. § 103 by Congress in 1952.[27] The Supreme Court has expressed the opinion that the statute was intended to codify the existing case law.[28] 35 U.S.C. § 103 governs obviousness, stating:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.[29]

Importantly, the invention as a whole is evaluated for obviousness, not each individual element.

1. Basic Application of Obviousness

The Supreme Court established a framework for analyzing obviousness in *Graham v. John Deere Co*.[30] Under this framework, courts are to consider "the scope and content of the prior art,"[31] the "differences between the prior art and the claims at issue,"[32] and "the level of

---

[26] Hotchkiss v. Greenwood, 52 U.S. 248 (1851); *See* CRAIG A. NARD, THE LAW OF PATENTS 307 (2011) ("The *Hotchkiss* case is widely regarded as creating an additional patentability hurdle, above and beyond novelty and utility. This common law development . . . ").

[27] *See* Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 3 (1966) ("the Congress has for the first time expressly added a third statutory dimension to the two requirements of novelty and utility that had been the sole statutory test since the Patent Act of 1793. This is the test of obviousness . . . ").

[28] *Id*. at 3-4 ("We have concluded that the 1952 Act was intended to codify judicial precedents embracing the principle long ago announced by this Court in *Hotchkiss v. Greenwood* . . . ").

[29] 35 U.S.C. § 103 (1964).

[30] Graham v. John Deere Co. of Kansas City, 383 U.S. at 17 (1966); John F. Duffy, *Inventing Invention: A Case Study of Legal Innovation*, 86 TEX. L. REV. 1, 61 (2007) (Stating that a "significant development in the Graham opinion was the establishment of a four-step framework for analyzing the obviousness question.").

[31] *Graham*, 383 U.S. at 17.

[32] *Id*.

ordinary skill in the pertinent art."[33] Further, the Court stated, "[s]uch secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented."[34] In terms of when to measure obviousness, it is important to note that obviousness is measured "before the effective filing date of the claimed invention."[35] In asking the question of how the tools of invention can affect patentability, the level of ordinary skill is by far the most important component of this analysis, and this will be discussed more fully in the following section. Secondary considerations are also pertinent and will be discussed below in Part II.B.3.

2. Person Having Ordinary Skill in the Art (hereinafter "PHOSITA")

Critical to the question of obviousness is how the PHOSITA is construed. There is a true paucity of case law on the topic of how to determine the PHOSITA. Nevertheless, construing the PHOSITA is essential to the question as to whether genetic algorithms can render an invention obvious.

In the 1983 case *Environmental Designs, Ltd. v. Union Oil Co. of California*, the Court of Appeals for the Federal Circuit (hereinafter "the Federal Circuit")[36] stated:

> Factors that may be considered in determining level of ordinary skill in the art include: (1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with

[33] *Graham*, 383 U.S. at 17.

[34] *Id*. at 17-18.

[35] 35 U.S.C. § 103 (2011).

[36] In patent cases, appeals go to the Federal Circuit rather than the regional circuit courts. *See Court Jurisdiction*, U.S FED. CIR., http://www.cafc.uscourts.gov/the-court/court-jurisdiction.html (last visited Jan. 8, 2013).

> which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field.[37]

However, the Federal Circuit in *Environmental Designs* did not apply these factors since the parties did not dispute the PHOSITA's construction.[38] Other Federal Circuit cases mention the importance of determining the level of ordinary skill yet do not shed much light on how to interpret the PHOSITA.[39]

One of the only on-point cases that reasons through its PHOSITA analysis is *Daiichi Sankyo Co., Ltd. v. Apotex, Inc.*[40] In *Apotex*, the plaintiff's patent was "drawn to a method for treating bacterial ear infections by topically administering the antibiotic ofloxacin into the ear."[41] The district court had held that the PHOSITA would have a medical degree and would be either a pediatrician or a general practitioner.[42] However, the Federal Circuit reasoned that none of the

---

[37] Envtl. Designs, Ltd. v. Union Oil Co. of Cal., 713 F.2d 693, 696 (Fed. Cir. 1983) (Citing Orthopedic Equip.Co. v. All Orthopedic Appliances, Inc., 707 F.2d 1376, 1381–82 (Fed.Cir.1983)).

[38] Envtl. Designs, **7**13 F.2d at 697.

[39] *See, e.g.*, Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc., 707 F.2d at 1382 (Upholding the district courts finding that the PHOSITA was "an engineer having at least a few years of design experience working in the field of developing orthopedic soft goods," but not providing any evidence from the particular situation presented why the PHOSITA should be constructed this way.); Orthopedic Equip. Co. v. United States, 702 F.2d 1005 (Fed. Cir. 1983) (Not shedding much light on how to construct the PHOSITA besides listing some of the factors subsequently cited in *Environmental. Designs*, and stating, "[t]he individuals working in the art were of above average intelligence and educational training. Many possessed advanced university degrees."); Jacobson Bros., Inc. v. United States, 512 F.2d. 1065, 1070 (Ct. Cl. Nov. 6, 1974) (Listing some of the factors recited in *Environmental Designs* and stating, "[a] finite quantitative definition of this ordinarily skilled person is difficult at best.").

[40] Daiichi Sanko Co. v. Apotex, Inc., 501 F.3d 1254 (Fed. Cir. 2007).

[41] *Id*. at 1255.

[42] *Id.* at 1256.

inventors of the challenged patent had medical degrees.[43] Instead, they "were specialists in drug and ear treatments"—a research scientist and a university professor.[44] Further, the written description of the patent detailed the inventors' testing of their treatment on guinea pigs, which is not something a pediatrician or general practitioner would do.[45] Therefore, the Federal Circuit found that the district court had committed an error in construing the PHOSITA to be a general practitioner or pediatrician,[46] and instead construed the PHOSITA to be "a person engaged in developing pharmaceutical formulations and treatment methods for the ear."[47] The Federal Circuit found that the district court's use of the incorrect PHOSITA "tainted its obviousness analysis."[48] Based on the new PHOSITA, the Federal Circuit held that the patent was obvious.[49]

The search for additional precedent in constructing the PHOSITA turns up precious little. In *Ex Parte Hiyamizu*, the Board of Patent Appeals and Interferences (hereinafter "the BPAI") reviewed an Examiner's decision to construct a PHOSITA, in relation to a patent application for a semiconductor device, to be a person with a doctoral level degree.[50] The BPAI rejected the use of a degree in constructing the PHOSITA, stating, "[i]t is our view that such a hypothetical person is no more definable by way of credentials than is the hypothetical 'reasonably prudent

---

[43] *Id.* at 1257.

[44] *Id*.

[45] *Id*.

[46] Daiichi Sanko Co. v. Apotex, Inc., 501 F.3d 1254, 1257 (Fed. Cir. 2007).

[47] *Id.* at 1254.

[48] *Id*.

[49] *Id*. at 1259.

[50] Ex Parte Hiyamizu, 10 U.S.P.Q.2d 1393, 1394 (Bd. Pat. App. & Inter. 1988).

man' standard found in laws pertaining to negligence."[51] However, the BPAI did not go on to provide a framework on how to determine the PHOSITA.[52]

In sum, PHOSITA construction is a topic upon which there is a scarcity of case law. However, among what is available, *Apotex* provides the most complete analysis of the *Environmental Designs* factors. Therefore, the PHOSITA for this note's question will be constructed under the *Apotex* and *Environmental Designs* framework. Once the PHOSITA has been constructed, courts proceed to evaluate secondary considerations.

3. Secondary Considerations

In determining obviousness, the Supreme Court assesses several secondary considerations such "as commercial success, long felt but unsolved needs, failure of others, etc."[53] Further, courts consider unexpected results as a secondary consideration.[54] Secondary consideration arguments will often be raised in close cases of issues regarding obviousness.

Regarding commercial success, the Federal Circuit has explained: "Commercial success is relevant because the law presumes an idea would successfully have been brought to market sooner, in response to market forces, had the idea been obvious to persons skilled in the art."[55] In other words, if it was obvious, someone else would have already been in the market selling it, and it would have been harder to turn such a profit. However, commercial success may also be

---

[51] *Id*. at 1394.

[52] *See Id.*

[53] Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 17-18 (1966).

[54] *In re* Dillon, 919 F.2d 688, 692-93 (Fed. Cir. 1990) (Stating that the applicants "argument can consist of a comparison of test data showing that the claimed compositions possess unexpectedly improved properties or properties that the prior art does not have").

[55] Merck & Co., Inc. v. Teva Pharmaceuticals USA, Inc., 395 F.3d 1364, 1376 (Fed. Cir. 2005).

the product of advertising and marketing.[56] Therefore, for commercial success to count as evidence of nonobviousness there must be a nexus between the commercial success and the technical merits of the patented invention.[57] This battle to show a nexus was demonstrated in *J.T. Eaton & Co., Inc. v. Atlantic Paste & Glue Co.*[58] In this case, a patent for a "Stick-Em" glue mousetrap was challenged as obvious.[59] The patentee argued that the patent was not obvious because of commercial success.[60] The Federal Circuit ruled that the patentee had failed to establish the nexus between the patent and the commercial success because the sales data submitted was for a slightly different product than what the patent was directed to.[61] The Federal Circuit remanded the case to the district court to consider only sales data associated with the exact patented product.[62]

Courts also consider "long felt but unsolved needs [and the] failure of others."[63] Courts consider this because "[i]f people are clamoring for a solution, and the best minds do not find it

[56] Nard, *supra* note 13, at 375.

[57] *Id.*

[58] J.T. Eaton & Co., Inc. v. Atlantic Paste & Glue Co. 106 F.3d 1563 (Fed. Cir. 1997).

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.* (the Federal Circuit further stated, "[i]f a patentee makes the requisite showing of nexus between commercial success and the patented invention, the burden shifts to the challenger to prove that the commercial success is instead due to other factors extraneous to the patented invention, such as advertising or superior workmanship.").

[63] Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 17 (1966).

for years, that is practical evidence…of the state of knowledge."[64] In other words, if it was obvious, someone would have already tried it. However, this secondary consideration must be viewed bearing in mind that the failure of others may simply have been due to other research priorities.[65] From a policy perspective, granting a patent for an idea that the marketplace needs furthers patent law's goal of bringing ideas to the marketplace. An example of the long felt need was shown in *Environmental Designs*.[66] In that case, the Federal Circuit considered legislative regulation controlling sulfur dioxide emissions as evidence of a long felt need for technology with reduced sulfur dioxide emissions.[67]

A final secondary consideration is unexpected results.[68] For example, the Federal Circuit considered unexpected results in the case *In re* Merck & Co.[69] There, a patent application for an antidepressant drug with sedative properties had been rejected as obvious by the PTO.[70] The prior art the PTO cited was another antidepressant drug with sedative properties and with only a slight chemical structural difference to the drug in the patent application.[71] The patent applicant argued that even though the chemical difference in the drugs was small, the patent should be

---

[64] *In re* Mahurkar Double Lumen Hemodialysis Catheter Patent Litig., 831 F. Supp. 1354, 1378 (N.D. Ill. 1993).

[65] NARD, *supra* note 13, at 376.

[66] 713 F.2d at 697-98.

[67] *Id.* (stating "the desire of governmental bodies to mandate higher purity standards was frustrated by lack of technology thus dramatizes the need.").

[68] *In re* Dillon, 919 F.2d at 692-93; *In re* Merck & Co., Inc., 800 F.2d 1091, 1098 (Fed. Cir. 1986) ("A prima facie case of obviousness can be rebutted by evidence of unexpected results.").

[69] 800 F.2d at 1098-99.

[70] *Id.* at 1092.

[71] *Id.* at 1096.

granted because there was a difference in sedative properties.[72] As evidence of this, the applicant submitted an article which compared the sedative properties of the two drugs.[73] In weighing all the evidence, the Federal Circuit rejected the applicant's argument because the article characterized the difference as only "somewhat less" sedative.[74]

III. The Tools of Invention and Genetic Programs

A. The Increasing Prevalence of Computers in Research

Computer programs simulate, among many other things, electronic circuits,[75] rocket propulsion,[76] and reactions in nuclear physics.[77] Scientists and inventors use computers more and more in their research.[78] But thus far, computers have mostly been used only to augment human ingenuity. Genetic programming (described in the following section), a branch of artificial

---

[72] *Id.* at 1098 ("In rebuttal of the PTO's prima facie case appellant has asserted that, as compared to [the prior art drug], [the present invention drug] unexpectedly has a more potent sedative and a stronger anticholingeric effect.").

[73] *In re* Merck Co., Inc., supra note 68, at 1098-99.

[74] *Id.* at 1099.

[75] *See, e.g.*, PARTSIM.COM, http:// www.partsim.com/ (last visited Dec. 7, 2013) (website providing a free circuit simulator).

[76] *See*, Balachandar Ramamurthy, Eliyahu Horowitz & Joseph R. Fragola, *Physical Simulation in Space Launcher Engine Risk Assessment*, Reliability and Maintainability Symposium (RAMS), 2010 Proceedings - Annual, vol., no., pp.1-6, 25-28 Jan. 2010.

[77] *See*, INTERACTIVE SIMULATIONS UNIVERSITY OF COLORADO AT BOULDER, http://phet.colorado.edu/en/simulation/nuclear-fission (last visited Jan. 8, 2013).

[78] George Johnson, *The World: In Silica Fertilization; All Science Is Computer Science*, N.Y. TIMES, Mar. 25 2001, (quoting a Dr. at a research institute as saying, "'Physics is almost entirely computational now.…Nobody would dream of doing these big accelerator experiments without a tremendous amount of computer power to analyze the data.'" And, "'Ten years ago biologists were very dismissive of the need for computation…Now they are aware that you can't really do biology without it.'").

intelligence, brings computers to the next level— one where computers may supplant human creativity and reduce the role that humans play in the invention process.[79]

B. Genetic Programs

Genetic programming brings major changes to the future of invention.[80] Genetic programs operate by mimicking the evolutionary process.[81] For a simple genetic program, a user inputs a set of desired criteria. The genetic program then generates a random population of samples and selects some of the samples with criteria closest to the user's criteria. The program then randomly generates changes to these samples to create a new population and further selects the samples from the new population that are closest to the user's criteria. The procedure iterates until the desired criteria is reached.[82] To illustrate, if a genetic program is designing an antenna, the user would input a desired radiation pattern. The genetic program would then randomly generate ten antennas and select the antenna with the radiation pattern closest to the desired pattern. Using this antenna, the program would randomly generate slight changes in the antenna's shape and size to create a new population of ten antennas. From this new population, the

---

[79] *See, e.g.*, Liza Vertinsky & Todd M. Rice, *Thinking About Thinking Machines: Implications Of Machine Inventors For Patent Law*, 8 B.U. J. SCI. & TECH L. 574, 587 (2002) (Stating "the human role will increasingly be limited to identifying basic problem structures and evaluation criteria for results, and thinking machines will dominate the rest of the invention process.").

[80] *See* Kenneth Chang, *Hal, Call Your Office: Computers that Act Like Physicists*, N.Y. TIMES, Apr. 7, 2009, at D4; Eisenberg, *supra* note 2.

[81] *Genetic programming*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Genetic_programming (last visited Jan. 8, 2013).

[82] Method & Apparatus For Chem. Genetic Programming, U.S. Patent No. 7,610,154 (filed Jan. 27, 2005) (issued Oct. 27, 2009) ("The conventional genetic programming starts from a program consisting of randomly generated prescribed programming elements, and reproduces over generations a best fit program of each generation through genetic operations, so as to evolve the population."); *see also Genetic programming*, *supra* note 81.

program would then select the next antenna with a radiation pattern closest to the desired radiation pattern and repeat the process until it found an antenna with the desired pattern.

More advanced genetic programs may mimic additional aspects of the evolutionary process.[83] For example, in biological evolution, a newborn will have characteristics of both parents.[84] This is caused by a process called chromosomal crossover.[85] More advanced genetic programs can mimic this process.[86] Some genetic programs even generate populations with "offspring" based on three "parents."[87] Further, there are other biological evolutionary processes that genetic programs have imitated.[88] It is important to note that since genetic programs use random process (e.g. in selecting a first population and in mutating subsequent populations) the genetic program could make different designs using the same inputs each time it is run.[89]

---

[83] *See Genetic programming*, *supra* note 81.

[84] *See Chromosomal crossover*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Chromosomal_crossover (last visited Jan. 8, 2013).

[85] *Id.*

[86] *E.g.*, Zakir H. Ahmed, *Genetic Algorithm for the Traveling Salesman Problem Using Sequential Constructive Crossover Operator*, 3.6 International Journal of Biometric and Bioinformatics 96 (2010).

[87] *Crossover (genetic algorithm)*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Crossover_%28genetic_algorithm%29 (last visited Dec. 7, 2013).

[88] *See* Method and Apparatus for Automatic Synthesis, Placement & Routing of Complex Structures, U.S. Patent No. 6,424,959 (filed June 17, 1999)(a program mimicking s biological process that performs genetic operations on DNA) ("The present invention uses a population of entities which are evolved over a series of generations by an iterative process involving the application of operations, such as mutation, crossover, reproduction, and architecture-altering operations."); *Genetic programming*, *supra* note 81.

[89] *See* Kohlhepp, *supra* note 9, at 812 (Noting that when a genetic algorithm is used, for example to design a roof truss, that "[i]f the algorithm is run ten times, however, it will yield ten different roof truss designs.").

Genetic programming has been applied to solve many different kinds of problems. Jet engines[90] and antennas[91] have been designed by genetic programs. Fuel emissions for diesel engines have been optimized with genetic programming.[92] Classical music has been composed by a genetic program.[93] On the more theoretical side, scientists are using genetic programs to sift through data to discover fundamental laws of nature.[94]

The functionality of patented devices has been duplicated by devices designed by genetic programs.[95] For instance, a team lead by John Koza browsed patents and selected five patents on various electronic circuits issued after January 1, 2000.[96] They then used genetic programming to

[90] Ray Kurzweil, *The Virtual Thomas Edison*, TIME, Dec. 4, 2000, at 114.

[91] Anne Eisenberg, *What's Next*; *When a Gizmo Can Invent a Gizmo*, N.Y. TIMES, Nov. 25, 1999, at G9 (satellite communications antenna designed); Jonathon Keats, *John Koza Has Built an Invention Machine*, POPULAR SCI., May 1, 2006, at 72, 92 (antenna designed that looked like "bent paperclip").

[92] *Diesel Breeding: Looking Into Engines Helps Cross the Best with the Best*, 124 MECHANICAL ENGINEERING 53, Sept. 1, 2002, at 53 (Stating that using a genetic program to optimize engine design "resulted in a design that consumed 15 percent less fuel than a standard diesel engine while producing one-third the amount of nitrogen oxide and half the soot.").

[93] *See* Alasdair Wilkins, *This Classical Music was Created by a Supercomputer in Less than a second*, IO9.COM (Jan. 6, 2013, 3:00 PM), http://io9.com/5973551/this-classical-music-was-created-by-a-supercomputer-in-less-than-a-second.

[94] Kenneth Chang, *Hal, Call Your Office: Computers that Act Like Physicists*, N.Y. TIMES, Apr. 7, 2009, at D4.

[95] J. R. Koza et al., *Routine Automated Synthesis of Five Patented Analog Circuits Using Genetic Programming,* 8 SOFT COMPUTING 318, 318 (2004).

[96] *Id.* at 318-19.

successfully design circuits which duplicated the functionality of the patented circuits.[97] John Koza has also received a patent on a circuit designed by his genetic program.[98]

This rise of genetic programs illustrates that the way many inventors do their work may change as genetic programs become more widespread. Because a genetic program may simply be able to design what an inventor tells it to, the role of the inventor will change once genetic programs are brought to that inventor's field. In the view of one scientist, people will "become managers, directing the machines toward interesting problems and opportunities . . . . The creative act will be in mentioning the right problems."[99] As developed in Part IV, this major change in the inventor's role leads to some situations where widespread use of genetic programs should render some ideas obvious.

IV. The Situation Where Genetic Programming Should Render an Idea Obvious

The remainder of this paper argues that before genetic programming becomes widespread in its application to the design of a particular device, designs that could be created by the genetic program should be patentable. However, once genetic programming becomes widespread in its application to the design of a particular device, designs that could be created by the genetic

---

[97] *Id*. at 322-24.

[98] Kohlhepp, *supra* note 9, at 786; Keats, *supra* note 91, at 68 ("An invention-machine creation has earned a patent; the examiner did not know it was the work of a computer."); *see also* Apparatus For Improved General-Purpose PID and Non-PID Controllers, U.S. Patent No. 6,847,851 (filed July 12, 2002) (issued Jan. 25, 2005).

[99] Eisenberg, *supra* note 2. Further, although not within the scope of this note's topic, the above quote raises another separate and interesting question: if a device designed by a genetic program is patentable, *who* should get the patent on the device? Is it the person who coded the genetic program, the person who "mentioned the right problems" to the genetic program, or the person who built the device?

program should be held to be obvious because it would be obvious to an inventor to simply use a genetic program to design the device in question.

Let us return to the example of an antenna. In constructing the PHOSITA for this example, the factors from *Environmental Designs*[100] would be considered. First, the educational level of the inventor varies widely in antenna design. One inventor might be a professor with a Ph.D., while the next might be an undergraduate student. This criterion is not particularly useful here. Second, the type of problem encountered in the art is how to design an antenna that emits a desired radiation pattern.[101] Third, the prior art solution to this problem would be to design an antenna and then use a computer program to simulate the antenna design to determine if the antenna produced the desired radiation pattern. Fourth, the rapidity with which innovations are made in this field is directly linked to how antennas are designed, and is therefore linked to whether genetic programs are in widespread use in antenna design. Fifth, antenna technology and the tools used to design antennas can range from very basic to very sophisticated; so, this factor is also not very helpful. Sixth, the educational level of active workers in the field would likely be deemed to be an engineer with a few years of antenna design experience.

In view of the above, the question the court should ask is: would an engineer with a few years of experience, who sought to design an antenna emitting a particular radiation pattern, use a genetic program to design the antenna?

---

[100] Environmental Designs, LTD. And The Trentham Corp. v. Union Oil Co. of Cal. And Ralph M. Parsons Co., 713 F.2d 693, 696 (Fed. Cir. 1983); *see* discussion *supra* Part II.B.2.

[101] *See, e.g.*, U.S. Patent Appl. Pub. No. 2011/0276519 (filed July 22, 2011) (Describing an antenna in a parking meter, used e.g. to communicate with law enforcement officers or to provide credit card information, and showing the radiation patterns that will be emitted from the parking meter when different kinds of antennas are used).

Central to this question is whether the PHOSITA would have access to a genetic program. To illustrate, when John Koza used a genetic program to design an antenna he ran the program on his "invention machine," which is 1000 computers networked together[102]—hardly a tool that an ordinary antenna designer would have access to. The PTO should consider that even if an ordinary antenna designer knew that it was possible to design an antenna with a genetic program, he may not have access to a genetic program in his work. This leads to the conclusion that it would not be obvious to a PHOSITA to use the genetic program since he would not have access to it.

Further, 35 U.S.C. § 103 commands that obviousness be measured "before the effective filing date of the claimed invention."[103] This is important because the tools that the PHOSITA has available can easily change with time. It could be, for example, that at one point in time no antenna designers use genetic programs; yet, in the future, genetic programs become widespread in antenna design. In this situation, we must re-ask the question: would an engineer with a few years of experience, who sought to design an antenna emitting a particular radiation pattern, use a genetic program to design the antenna? At this later point in time, the answer is different than before—now a PHOSITA would use a genetic program to design the antenna.

In this post-spread of genetic programming situation, an antenna that could be designed by a genetic program should be held obvious. This is because any PHOSITA could easily plug the parameters into a genetic program, read the antenna design from the program, and bring the antenna into the public sphere. The public, in this situation, would gain nothing by this disclosure, since any PHOSITA could simply run the genetic program to design the antenna at

[102] Keats, s*upra* note 91, at 68-70.

[103] 35 U.S.C. § 103 (2013).

any time. Further, granting a patent on a particular antenna design would be useless for the inventor because the genetic program could potentially design a different antenna that emits the same radiation pattern the next time the genetic program is run.[104]

The above argument logically demonstrates why developments designed by genetic programs in fields where genetic programming is widespread should be held obvious. Nevertheless, just because something is logical does not make it good law or policy. Would holding such developments obvious make good policy? The following section explores this question.

A. Policy

Part II.A states patent law's goals of providing incentive for innovation and disclosure of ideas to the public.[105] Still, patents are not granted if an idea is obvious.[106] One reason for this is that obvious inventions may be brought into the public sphere without the incentive of a reward by a patent.[107] Once genetic programming has become widespread in a field, inventors working in the field can easily use a genetic program to design a device. Since the device may be developed and brought to the marketplace with such little cost, there is no need for the grant of a patent to incentivize an inventor to bring the device to the marketplace.[108] Another reason for not

---

[104] *See supra* note 89 and accompanying text.

[105] NARD, *supra* note 13, at 3 ("[P]atent law can be viewed as a system of laws that offer a potential financial reward as an inducement to invent, to disclose technical information, to invest capital in the innovation process . . . .").

[106] 35 U.S.C. § 103 (2013).

[107] *See* Duffy, *supra* note 30, at 11 ("For these [obvious] inventions, the rewards of the patent system are assumed to be largely unnecessary.").

[108] *Id.* (Stating that for obvious developments "enough incentive to create them is provided even by being the first to market the innovation . . . .").

granting a patent to an obvious development is to avoid granting a patent to a development "achieved through some cause not attributable to the patent applicant's efforts."[109] Once a genetic program has become widespread in a field, the advances created by a genetic program are not achieved through the patent applicant's efforts—the advances are instead created by the "efforts" of the genetic program.

Further, as a practical matter, let us return to the example of a genetic program designing an antenna, and let us assume that genetic programming has become widespread in this field. Allowing patents for antennas designed by genetic programs would allow companies to build a thicket of patents by repeatedly patenting designs created by the genetic program. Each time the genetic program is run, it would design a different antenna, since the program uses random processes.[110] If a company ran the program ten times, it could patent ten different antenna designs. If it did so, a competing company would have to go through the costly process of searching through the thicket of trivial patents. This competing company would have to shift investment dollars away from antenna research to searching though the thicket of patents.

Simply obtaining such a thicket of trivial patents would be very costly for a company. Therefore, it could be argued that companies would likely not pursue obtaining this thicket of trivial patents because of the high cost.[111] However, this high cost is much more of a burden to smaller companies than to large ones. In other words, a large, well-funded corporation could still obtain a thicket of patents and use it effectively against a smaller company that could not afford

[109] Duffy, *supra* note 30, at 12.

[110] Kohlhepp, *supra* note 9, at 812.

[111] *See* Duffy, *supra* note 30, at 12 (trivial patents can be discouraged by charging sufficient fees for obtaining or maintaining each patent).

the cost of sifting through a forest of patents. Holding devices obvious in fields where the use of genetic programs is widespread would disallow a large corporation from simply paying money to obtain a thicket of patents and using it to crush smaller, less well-funded companies.

Still, it is not enough to reach the conclusion that once genetic programming is widespread in a particular field, designs created by genetic programs should be held obvious. In order to have practical application, courts must know how to determine when genetic programming has become widespread in a field.

B. A Widespread Use Test Proposal

This note proposes a four-factor test to determine if genetic programming is widespread in a field, which evaluates: 1) whether the invention was actually designed with a genetic program, 2) the proportion of PHOSITAs in the field having access to genetic programs, 3) the cost associated with the use of a genetic program for this type of design, and 4) the amount of time and effort required to operate the necessary genetic program.

Because of the dynamic nature of genetic programming and artificial intelligence, the approach taken in applying the widespread use test must be flexible. In some situations, one or more factors may predominate; in others, all factors may apply equally. This flexible approach is in accordance with factor tests for other legal concepts.[112]

[112] *See, e.g.*, Playboy Enters., Inc. v. Netscape Commc'nsCorp., 354 F.3d 1020, 1026 (9th Cir. 2004) (analyzing, in a trademark dispute, likelihood of confusion factors and stating "courts must be flexible in applying the factors, as some may not apply. Moreover, some factors are more important than others.").

It is important to bear in mind that 35 U.S.C. § 103 orders that obviousness is measured "before the effective filing date of the claimed invention."[113] Therefore, the widespread use test would be applied at different times for different inventions.

1. Factor One: If the Invention was Actually Designed by a Genetic Program

At the onset, it is important to know if the invention was designed with the use of a genetic program. At a minimum, if the invention was designed by a genetic program, it shows that the technology exists and is available to at least one inventor in the field. Further, it shows that the inventor chose to design with a genetic program, which is evidence that genetic programming simplifies the task in this context.

One may question how the PTO or court is to know if an invention has been designed with a genetic program. However, "[e]ach individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the [PTO], which *includes a duty to disclose to the [PTO] all information known to that individual to be material to patentability . . . .*"[114] Therefore, the inventor and the attorney prosecuting the patent application both have a duty to disclose whether the invention was designed with a genetic program.

But, showing that the inventor alone had access to a genetic program is not sufficient to show widespread use. Therefore, we must look to see if other inventors in the field had access to applicable genetic programs.

---

[113] 35 U.S.C. § 103.

[114] 37 C.F.R. § 1.56 (emphasis added).

2. Factor Two: The Proportion of PHOSITAs in the Field Having Access to Genetic Programs

The proportion of PHOSITAs in the field having access to genetic programs is arguably the most important factor. If a high proportion of PHOSITAs have access to genetic programs, it demonstrates that more inventors are able to implement genetic programs to bring new designs to the market place. This in itself is evidence that patent law's goal of bringing new ideas to the market place[115] is being facilitated.

One issue in analyzing this factor will be how to determine the relevant market. For example, in the domestic market for diesel powered locomotive engines, there are only two major manufacturers—General Electric Co., and Electro-Motive Diesel Inc. (now owned by Caterpillar Inc.).[116] Therefore, when analyzing this market, courts will have to determine whether to limit the market to diesel powered locomotive engines (effectively only two companies), or whether to expand the analysis to related fields (e.g. truck diesel powered engines). In this example, it is better to limit the analysis to the exact problem to be solved. This is because even though truck engines and locomotive engines may have much in common, there are enough differences that a completely different genetic program would be required to design each. In selecting fields for determining the proportion of PHOSITAs having access to genetic programs, only fields where the same genetic program could in fact be used to design the invention in question should be considered. This ensures that a PHOSITA would actually be able to use the genetic program to design the invention in question. It may seem, in the diesel

[115] Nard, *supra* note 13, at 3.

[116] Bob Tita, *Caterpillar expected to make Electro-Motive more competitive* (June 4, 2010), http://www.webcitation.org/5trEL4dsG.

powered locomotive example, that this produces a bizarre outcome—that use by only two companies is "widespread." However, this is the correct conclusion. If only two companies produce a product, and both of these companies have access to a genetic program, then by definition every company producing this product has access to a genetic program.

3. Factor Three: The Financial Cost Associated with Using a Genetic Program for this Type of Design

In designing his antenna with a genetic program, John Koza ran the genetic program on his "invention machine," which is 1000 computers networked together.[117] The electric bill alone was $3,000 a month.[118] The high cost of gathering and assembling 1000 computers may provide deterrence for many inventors and companies from adopting genetic programs. Therefore, a high cost of running a genetic program would be evidence that genetic programming was not widespread in a field. Alternatively, if a genetic program could be run cheaply, this would show that companies could easily adopt them and that use was becoming widespread.

4. Factor Four: The Amount of Time and Effort Required to Operate the Necessary Genetic Program

Along with financial cost, the time and effort required to operate the genetic program should also be considered.[119] The time and effort necessary to network enough computers together to provide the computing capability needed to run some genetic programs could

[117] Keats, s*upra* note 91, at 68-70.

[118] *Id.* at 69.

[119] Although a high financial cost of running a genetic program will often go hand in hand with a large requirement of time and effort to run a genetic program, this is not always the case. The two could become especially separated in the future as computer processors improve. For example, if improved computer processors allow a genetic program to run on a PC, but a genetic program software licensor still charges a very high fee for using the genetic program.

preclude some inventors from using genetic programs. Further, at the point in time when John Koza designed his antenna, his system took from one day to one month to create a new invention.[120] A month is quite a long time for a computer program to run. Alternatively, if a genetic program could be run as quickly as an iPhone app, this would be evidence that genetic programming is widespread in a field.

V. Contra

Above, I argue that when genetic programming becomes widespread with regard to designing a particular product, designs that the genetic program could produce should be obvious and therefore unpatentable. Yet, there are multiple potential counter arguments to this proposal in different directions. It is possible to argue that anything created by a genetic program should be obvious, even before genetic programming has become widespread in a field. Conversely, it is possible to argue that even widespread use of genetic programming should not render an idea obvious. Finally, there is an argument that widespread use of genetic programming should create only a prima facie case of obviousness. The strongest contra is discussed below.

A. Argument that Nothing Designed by a Genetic Program Should be Patentable Because it was Designed by a Process of Trial and Error

One argument is that everything designed by a genetic program should be held obvious because genetic programs (it appears) operate by a process of trial and error. The trial and error argument assumes that if something can be discovered through a simple process of trial and error, it must be obvious.[121] But, genetic programs do not in fact operate by a process of trial and

[120] Keats, s*upra* note 91, at 68.

[121] *See* Cal Crary, *Impact of KSR v. Teleflex on Pharmaceutical Industry*, PATENTLYO.COM (May 3, 2007), http://www.patentlyo.com/patent/2007/05/impact_of_ksr_v.html (commenting that a

error. A process of trial and error would be, for example: ten antennas are created, one antenna with the best radiation pattern is selected, *and the process stops there*. Genetic programs do not stop there. A genetic program would then take the best one, two, or three antennas and merge or mutate them.[122] From this, a new generation of antennas would be created.[123] The additional step of merging and/or mutating removes genetic programs from the category of pure trial and error.

Furthermore, from a policy perspective, it may seem that if all that is required to reach a solution is a process of trial and error, then the solution should be obvious. However, in Canadian patent law for instance, trial and error actually counts as evidence of nonobviousness.[124] This is because "[i]f something requires this kind of research, then it is not obvious because it is not 'plain as day' or 'crystal clear.'"[125] Therefore, even as a policy matter, it is not clear that the use of trial and error should render an idea obvious.

Federal Circuit Judge's belief was that "an approach that is obvious to try is also obvious where normal trial and error procedures will lead to the result").

[122] *Crossover (genetic algorithm)*, *supra* note 86.

[123] *Id.*

[124] Donald M. Cameron, *Chapter 7 Obviousness*, 7-27 (May 17, 2010), http://www.jurisdiction.com/patweb07.pdf (Stating "If trial and error are required, it can't be obvious." And "[f]urthermore, it is not directly leading to the solution; instead it leads to intermediate failures.").

[125] *Id.*

B. Argument that Genetic Programming use should not Effect Patentability

When John Koza designed his five circuits, which mimicked the functionality of recently patented circuits, he expressed the view that the use of a genetic program will not affect an invention's patentability.[126] Further, John Koza received a patent on a circuit designed by his genetic program.[127] Yet, genetic programming is still in its infancy. Because the construction of the PHOSITA can change over time, what satisfied the PTO's requirements at one point in time may not satisfy it at a later point in time. 35 U.S.C. §103 itself addresses this by stating that obviousness is measured "before the effective filing date of the claimed invention."[128] Therefore, it makes perfect sense that before genetic programs became widespread in his field, Koza would be granted a patent on his device. Likewise, it makes perfect sense that after genetic programs became widespread in his field, Koza would be denied a patent on his device.

C. Should Widespread use Create only a Prima Facie Case of Obviousness?

An alternative proposal to the one in this note is that a finding of widespread use should create only a prima facie case of obviousness. The idea is that the prima facie case of obviousness could be rebutted using secondary considerations. As discussed in Part II.B.3, courts

---

[126] Koza, *supra* note 95, at 324 ("If an automated method were able to duplicate a previously patented human-created invention, the fact that the original human-designed version satisfied the Patent Office’s criteria of patent-worthiness means that the automatically created duplicate would also have satisfied the Patent Office’s criteria.").

[127] Kohlhepp, *supra* note 9, at 786; Keats, *supra* note 91, at 68 ("An invention-machine creation has earned a patent; the examiner did not know it was the work of a computer."); *see also* U.S. Patent No. 6,847,851 (filed July 12, 2002).

[128] 35 U.S.C. § 103 (2013).

analyze secondary considerations when determining obviousness.[129] However, for the reasons that follow, secondary considerations are not very useful to the question of genetic programming.

The secondary consideration of unexpected results is not very relevant here, although it does take a moment to understand why. Unexpected results come into play when a slight difference in design leads to a drastic difference in results. Genetic programs do the opposite of this—genetic programs produce designs that are very different from existing human-created designs.[130] As Popular Science Magazine stated, "[e]very day now, genetic programs continue to create the unexpected, the counterintuitive or the just plain weird."[131] In the antenna context, the antenna that John Koza designed "looks like a mistake, works like a charm."[132] In other words, unexpected results would come into play if the antenna was designed only slightly differently but produced a vastly different radiation pattern. Instead, the antenna's design was not slightly different—it was drastically different.

Further, a long felt need is not particularly relevant here either. The idea behind the long felt need consideration is: if it was obvious, someone would have created it earlier; since no one created it earlier, it must not be obvious.[133] However, in a field with widespread genetic programming, it becomes obvious to use a genetic program to solve a problem even if the problem has been long felt. For example, for an antenna with a particular radiation pattern when

---

[129] Graham v. John Deere Co. of Kansas City, 383 U.S. 1, 27-28 (1966).

[130] Keats, *supra* note 91, at 72 ("Koza's leap in genetic programming allowed for open-ended evolutions of basic structure and so produced more novel and sophisticated designs").

[131] *Id.*

[132] *Id.* at 70.

[133] Matter of Mahurkar Double Lumen Hemodialysis Catheter Patent Litig., 831 F. Supp. 1354, 1378 (N.D. Ill. 1993).

genetic programming becomes widespread, a PHOSITA would simply use a genetic program to create an antenna with the desired radiation pattern.

Commercial success is also not relevant in the context of widespread genetic programming. The Federal Circuit explains that commercial success "presumes an idea would successfully have been brought to market sooner, in response to market forces, had the idea been obvious to persons skilled in the art."[134] This is less applicable to our question because once genetic programming has become widespread in a field, it becomes obvious for a PHOSITA to use a genetic program to bring a product to market. Therefore, the presumption that a product would have been brought to the market sooner no longer makes any sense where genetic programming has become widespread. A presumption that the product will be designed using a genetic program, and immediately brought to the market makes more sense in this context.

None of the secondary considerations are relevant to the problems posed by widespread genetic programming. Therefore, after finding widespread use, creating a prima facie case of obviousness instead of simply finding obviousness would not be advisable.

VI. Conclusion

No one knows how genetic programming will affect the future of invention and the patentability of devices designed by genetic programs. Thus far, at least one device that was designed by a genetic program has been patented.[135] This is fine for now, as use of genetic programming is not widespread. In the future, however, as engineers begin to make common use of genetic programming, many designs that were once difficult to create will become trivially

[134] Merck & Co., Inc. v. Teva Pharmaceuticals USA, Inc., 395 F.3d 1364, 1376 (Fed. Cir. 2005).

[135] Kohlhepp, *supra* note 9, at 786; Keats, *supra* note 91, at 68, 72; *see also* U.S. Patent No. 6,847,851 (filed July 12, 2002).

simple. Once this happens, designs for a particular device that a genetic program could create should be deemed obvious, and therefore unpatentable.[136] If patents were granted on these designs, the public would gain nothing from these patent grants because a PHOSITA could already easily bring this technology to the marketplace. Because this situation only occurs after genetic program use becomes widespread in a particular field, finding a method to determine widespread use is critically important. This note has proposed a four-factor widespread use test to make this determination. There is no doubt that genetic programs have the potential to change invention and creative thinking as we know it.[137] As this sea change arrives, we must be ready to adapt our patent laws to maintain their underlying purpose.

[136] 35 U.S.C. § 103 (2013).

[137] Chang, *supra* note 80; Eisenberg, *supra* note 2.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 4, PAGE 143

The Usefulness of the International Trade Commission as a Patent Forum in the Wake of *Certain Personal Data and Mobile Communications Devices and Related Software* (Apple v. HTC)

Stephen Burke

I. Introduction 144

II. Brief History of the International Trade Commission 145

III. The ITC as a Patent Forum 147
- i. Obtaining Injunction and the Public Interest 148
- ii. Available Remedies 150

IV. Apple v. HTC 152
- i. Apple's Complaint 152
- ii. Initial Determination and Commission Decision 153
- iii. Third Party Submissions as to the Public Interest 153
- iv. The Commission's Analysis of §337 Public Interest Factors 155
- v. The Commission's Modified Exclusion Order 156

V. Previous Instances of Public Interest Outweighing Injunction 157
- i. Certain Automatic Crankpin Grinders 157
- ii. Certain Inclined-Field Acceleration 157
- iii. Certain Fluidized Supporting Apparatus and Components Thereof 158

VI. ITC Investigations Since Apple v. HTC 159
- i. Microsoft v. Motorola 159

VII. Policy Implications 163

VIII. Conclusion 169

I. Introduction

The United States International Trade Commission (hereinafter the "ITC") is a government agency with statutory power to control matters of trade.[1] As a part of this power, the ITC may investigate claims of patent infringement and ban infringing products from being imported into and/or sold in the country.[2] The patent investigation power of the ITC was seldom utilized by litigants before the turn of the 21st century, who instead preferred to file complaints in federal court.[3] With the technology boom of the 1990s and the mounting international competition into the new millennium, the ITC has seen a steadily increasing volume of patent claims.[4]

In 2010, the now deceased Apple co-founder Steve Jobs, released an aggressive intellectual property policy statement:

> "We can sit by and watch competitors steal our patented inventions, or we can do something about it. We've decided to do something about it. We think competition is healthy, but competitors should create their own original technology, not steal ours."[5]

Following this statement, Apple filed suit against High Tech Computer Corporation (hereinafter "HTC") in both the ITC and federal district court.[6] The complaint alleged that HTC smartphones

---

[1] UNITED STATES INTERNATIONAL TRADE COMMISSION, *About the USITC*, http://www.usitc.gov/press_room/about_usitc.htm (last visited Sept. 11, 2013).
[2] *Id.*
[3] Robert W. Hahn & Hal J. Singer, *Assessing Bias in Patent Infringement Cases: A Review of International Trade Commission Decisions*, 21 HARV. J.L. & TECH. 457, 460 (2008).
[4] *Id.*
[5] Philip Elmer-DeWitt, *Apple v. HTC: What's the deal with Delaware?*, FORTUNE (Oct. 2, 2012, 2:37 PM), http://tech.fortune.cnn.com/2012/10/02/apple-v-htc-whats-the-deal-with-delaware/.
[6] *Id.*

such as the Nexis 1 and the Droid Eris contained software that infringed Apple patents.[7] The ITC has regularly stopped the importation of such products even when the infringement concerns only a tiny aspect of the imported product.[8] After just over a year of investigation, the ITC found many HTC smartphones infringed the Apple patents and issued an unusual order. Instead of immediately barring importation of the HTC products, the ITC gave HTC four months to design around the patent before enjoining importation.[9] Business and patent experts are concerned that this unusual determination is the beginning of a more lenient approach by the ITC that would significantly weaken patentees' ability to stop competitors from getting their products into the U.S. market.[10]

This note examines the reasons behind the ITC's unusual holding and also looks at ITC investigations before and after Apple v. HTC to determine whether this type of holding is becoming commonplace or was simply an outlier.

II. Brief History of the International Trade Commission

Before the International Trade Commission, there was the United States Tariff Commission.[11] The Tariff Commission was established by Congress under the Revenue Act of

[7] Complaint, Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, Doc. ID 419917 (accessed by logging into the Electronic Document Information System at www.usitc.gov.).
[8] Steven Seidenberg, *The Year Ahead 2012: Top IP Legal Issues in the United States*, INTELLECTUAL PROPERTY WATCH (Jan. 13, 2012, 4:38 PM), http://www.ip-watch.org/2012/01/13/the-year-ahead-2012-top-ip-legal-issues-in-the-united-states.
[9] Dennis Crouch, *Injunctive Relief and the Public Interest at the ITC*, PATENTLY-O BLOG (Dec. 20, 2011), http://www.patentlyo.com/patent/2011/12/injunctive-relief-and-the-public-interest-at-the-itc.html
[10] *Id.*
[11] United States Government Manual, 1945 at 578, *available at* http://ibiblio.org/hyperwar/ATO/USGM/USTC.html.

1916.[12]. The primary function of the Commission was that of a fact-finding body; the Commission was to act as a nonpartisan investigative body that produced accurate information with which Congress could make an informed decision.[13] The Act of 1916 gave the Commission very broad investigative powers, but no power to actually change tariffs.[14] The Commission's powers changed with the passage of the Tariff Act of 1922.[15] The scope of the Commission's power has been amended by the Agricultural Adjustment Act[16], the Trade Expansion Act of 1962[17], the Trade Act of 1974[18] (which changed the name to the ITC), the Trade Agreements Act of 1979[19], the Trade and Tariff Act of 1984[20], the Omnibus Trade and Competitiveness Act of 1988[21], and the Uruguay Round Agreements Act.[22]

Today, the ITC describes itself as "an independent, quasi-judicial Federal agency with broad investigative responsibilities on matters of trade."[23] The ITC also "adjudicates cases involving imports that allegedly infringe intellectual property rights."[24] The ITC has five major operations that serve its external customers, however, the only operation at issue here is the Intellectual Property-Based Import Investigation.[25]

---

[12] *Id.*
[13] *Id.* at 579
[14] *Id.*
[15] Id. at 578-79
[16] 7 U.S.C.A., Ch. 35 (West 2013).
[17] 19 U.S.C.A., Ch. 7 (West 2013).
[18] 19 U.S.C.A., Ch.12 (West 2013).
[19] 19 U.S.C.A., Ch. 13 (West 2013).
[20] Trade and Tariff Act of 1984, Pub. L. No. 98-573, 98 Stat. 2948 (1984).
[21] Omnibus Trade and Competitiveness Act, Pub. L. No. 100-418, 102 Stat. 1107 (1988).
[22] Uruguay Round Agreements Act, Pub. L. No. 103-465, 108 Stat. 4809 (1994).
[23] UNITED STATES INTERNATIONAL TRADE COMMISSION, *supra* note 1.
[24] *Id.*
[25] *Id.*

III. The ITC as a Patent Forum

ITC intellectual property investigations are initiated under §337 of the Tariff Act of 1930. This section gives the ITC authority to investigate claims that the importation of goods into the United States infringes patents, trademarks, or copyrights or otherwise constitutes an unfair method of competition.[26] The ITC is an attractive forum for plaintiffs for two reasons: the expedited nature of the proceedings; and the strength of the available remedies.[27] According to the 2012 Patent Litigation Study, the average time-to-trial in a federal court proceeding, from complaint to the first day of trial, is 2.5 years.[28] This number is gradually rising with the increased volume of complaints to the federal court system.[29] On the other hand, the Administrative Law Judge (hereinafter "ALJ") in an ITC proceeding will generally issue a decision within one year.[30] In fact, in 2011, the average completion time from institution of an investigation to a decision was 13.7 months.[31]

[26] Steptoe & Johnson LLP, *Section 337 Frequently Asked Questions (2012), available at* http://www.steptoe.com/resources-detail-6611.html.
[27] Steptoe & Johnson, *supra* note 26.
[28] Chris Barry ET AL, *2012 Patent Litigation Study: Litigation continues to rise amid growing awareness of patent value,* PricewaterhouseCoopers (2012) *available at* http://www.pwc.com/en_US/us/forensic-services/publications/assets/2012-patent-litigation-study.pdf.
[29] *Id.*
[30] Steptoe & Johnson, *supra* note 26.
[31] Marianne Purzycki, *The ITC: Patent Forum Remains Red Hot*, HILDEBRANT BLOG (July 5, 2012), http://hildebrandtblog.com/2012/07/05/the-itc-patent-forum-remains-red-hot/.

i. Obtaining Injunction and the Public Interest

Until the Supreme Court's decision in *eBay v. MercExchange*[32] in 2006, obtaining an injunction in federal court was almost guaranteed to a plaintiff once patent infringement was found.[33] In *eBay*, the Court decided instead that the patentee must also meet a traditional four-factor test to obtain a permanent injunction.[34] The traditional test requires a plaintiff to "demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law; such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardship between the parties, a remedy in equity is warranted and (4) that the public interest would not be disserved by a permanent injunction."[35] The more stringent *eBay* test sets a higher bar for the plaintiff to meet before the court will consider an injunction. The ITC is not bound by the holding in *eBay*, but "is required to consider the impact that an injunction would have on competition and consumers."[36]

In contrast with the strict factors that must be met in the *eBay* test, Section 337 does not compel the ITC to issue an exclusion order, but instead requires it to take four specific "public interest factors" into consideration. The statute states:

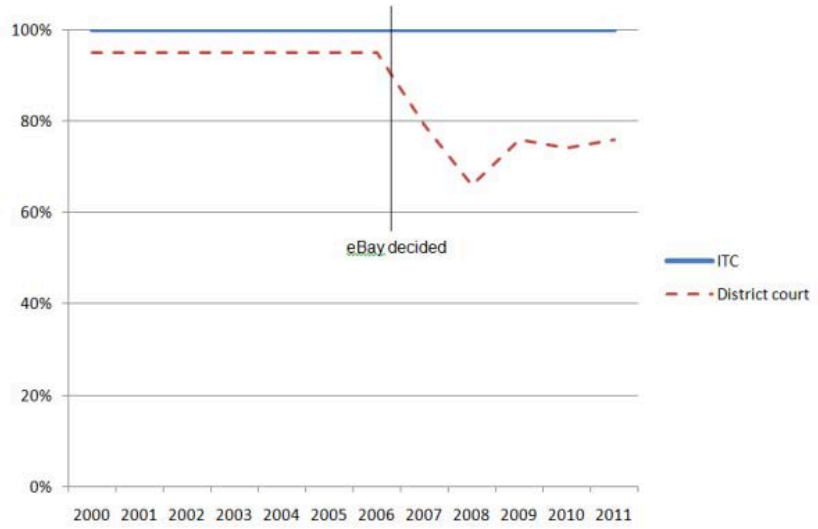
> If the Commission determines, as a result of an investigation under this section, that there is a violation of this section, it shall direct that the articles concerned, imported by any person violating the provision of this section, be excluded from entry into the United States, unless after considering the effect of such exclusion upon the public health and welfare, competitive conditions in the United States economy, the production of like or

[32] eBay Inc. v. Mercexchange, L.L.C., 547 U.S. 388, 393 (2006).
[33] Earnest Grumbles ET AL, *The Three Year Anniversary of eBay v. MercExchange: A Statistical Analysis of Permanent Injunctions*, INTELLECTUAL PROPERTY TODAY (2009), http://www.iptoday.com/issues/2009/11/articles/three-year-anniversary-eBay-MercExchange.asp.
[34] Earnest Grumbles ET AL, *supra* note 33.
[35] eBay, *supra* note 32.
[36] Crouch, *supra* note 8.

> directly competitive articles in the United States, and United States consumers, it finds that such articles should not be excluded from entry.[37]

The ITC has the power to interpret these four public interest factors and make fair, case-by-case decisions on whether and how to block products from entering the country.[38] The interpretation of the public interest factors is supplemented by third party submissions on behalf of or against an exclusion order.[39] The chart below shows the effect that the *eBay* decision had on the number of injunctions granted in federal court as opposed to the ITC.

Figure 1: Pre and Post *eBay* Injunctions in the ITC and District Courts.[40]

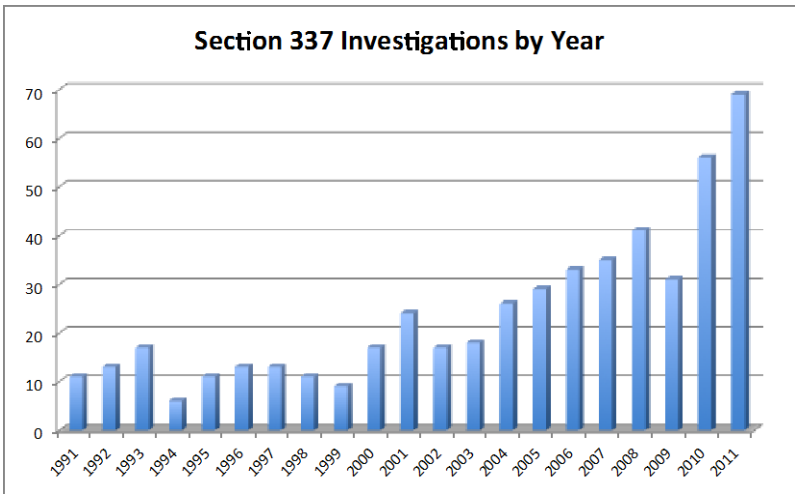


The graph shows that after the decision in *eBay*, injunctions were granted in as low as 70% of cases where infringement was found, as opposed to 100% of cases in the ITC where

[37] 19 U.S.C. §1337(d)(1)(2004).
[38] Colleen V. Chien & Mark A. Lemley, *Patents and the Public Interest,* N.Y. TIMES(Dec. 13, 2011), http://www.nytimes.com/2011/12/13/opinion/patents-smartphones-and-the-public-interest.html?_r=1&.
[39] *Id.*
[40] Colleen V. Chien & Mark A. Lemley, *Patent Holdup, the ITC, and the Public Interest* (Stanford Pub. Law, Working Paper No. 2022168, 2012).

infringement was found. The decrease in percentages of injunctions granted in district court also seems to correlate with the increase in investigations filed with the ITC.[41] The number of investigations in the ITC has doubled since the Supreme Court instituted a more stringent test for obtaining injunctions in district court.

Figure 2: Section 337 Investigations by Year[42]



The ITC is not only attractive to plaintiffs because of its higher percentage of injunctions granted, but also because of the sweeping effect of its multiple remedies.

ii. Available Remedies

The relief potentially available to a domestic plaintiff seeking to stop an infringing import through an ITC investigation includes: a limited exclusion order, a general exclusion order, and a cease and desist order.[43] A limited exclusion order prohibits only the named Respondent from

[41] *Section 337 Statistical Information*, U.S. INT'L TRADE COMMISSION, http://www.usitc.gov/press_room/337_stats.htm (last visited Sept. 13, 2013).
[42] Author analysis based on, *Number of Section 337 Investigations Instituted by Fiscal Year*, U.S. INT'L TRADE COMMISSION (2012) *available at*, http://www.usitc.gov/intellectual_property/documents/fy_337_institutions.pdf.
[43] Steptoe & Johnson, *supra* note 26.

importing the product at issue.[44] A general exclusion order on the other hand prohibits all imports of the product at issue by anyone, including non-parties to the ITC investigation.[45] A recent ITC opinion held that a general exclusion order may be issued regardless of whether an importer has been heard.[46] A cease and desist order is like a limited exclusion order in that it prohibits only the Respondent from importing the product at issue, but it also includes the added restrictive ban on selling the products that are already in the United States.[47] As a result of the more favorable procedural tools available in the ITC, there has been an upward trend of section 337 investigations in the last 20 years.[48]

Thus, the ITC seems like an attractive forum for plaintiffs to bring their complaints of infringing imported products because of the powerful remedies and the lower bar for granting injunctions. Figure 1 shows the injunctions in district courts falling while the ITC's injunctions remained at 100% into 2011. What if the ITC's percentage of injunctions began to fall as well? What if there is a case where an infringement is found, and for some reason the ITC cannot satisfy the plaintiff? That very situation arose in 2011 when the ITC handed down a determination in *Certain Personal Data and Mobile Communications Devices and Related Software* (Apple v. HTC).[49]

---

[44] Steptoe & Johnson, *supra* note 26.
[45] Steptoe & Johnson, *supra* note 26.
[46] Michael Best & Friedrich LLP, *Pay Attention: ITC Exclusion Orders May Block Your Imports If You Don't*, NATIONAL LAW Review (Jun. 27, 2012), http://www.michaelbest.com/pubs/pubDetailMB.aspx?xpST=PubDetail&pub=3131
[47] *Id.*
[48] *Section 337 Statistical Information*, *supra* note 39.
[49] Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, *available at* http://info.usitc.gov/ouii/public/337inv.nsf/RemOrd/710/$File/337-ta-710.pdf?OpenElement.

IV. Apple v. HTC

In furtherance of its new aggressive patent patrolling policy, Apple filed a complaint for the ITC to begin an investigation into certain HTC smartphones.[50] The resulting investigation, called *Certain Personal Data and Mobile Communications Devices and Related Software*, resulted.

i. Apple's Complaint

Apple originally brought suit against HTC on April 6, 2010 for infringing ten patents and then dropped six of them, leaving only patents No. 5,946,647 ("the '647 patent"); No. 6,343,263 ("the '263 patent"); No. 5,481,721 ("the '721 patent"); and No. 6,275,983 ("the '983 patent").[51] The '721 patent relates to "a means of allowing computer programs running one process to access objects that are located within a different process."[52] Before the '721 patent, separate processes were executed independently even when they were run simultaneously, and could not access resources from each other.[53] The '647 patent recognizes data such as phone numbers, addresses, and dates, and performs related actions such as offering the user the choice of making a phone call to the number.[54] The '263 patent "discloses the use of real-time application programming interfaces (APIs) interposed between application software or driver software and the real-time process subsystem."[55] For each patent Apple alleged that the HTC products "are made for use in an infringement of these claims and are not staple articles of commerce suitable for substantial non-infringing use." [56] Apple provided numerous examples of allegedly infringing

[50] *See* Han & Singer, *supra* note 4.
[51] Complaint, *supra* note 7.
[52] Complaint, *supra* note 7, at 8.
[53] Complaint, *supra* note 7, at 8.
[54] Complaint, *supra* note 7, at 12.
[55] Complaint, *supra* note 7, at 14.
[56] Complaint, *supra* note 7, at 8.

HTC products such as the Nexus One, Touch Pro, Touch Diamond, Tilt II, and Droid Eris.[57] Apple made it clear that the United States is their largest geographic marketplace and that 54% of their sales in 2009 came from inside the United States.[58]

ii. Initial Determination and Commission Decision

The ALJ issued an Initial Determination ("ID") finding a violation of section 337 by reason of the importation and sale of articles that infringe the '647 patent and the '263 patent.[59] The ITC affirmed the ALJ's finding that '647 patent had been infringed, but reversed the finding with regards to the '263 patent.[60] The ITC also affirmed the ALJ's finding that there was no violation of the '721 and '983 patents.[61]

iii. Third Party Submissions as to the Public Interest

As described in the previous section, in deciding what sort or remedy is appropriate, the ITC takes into account public interest factors and can also take into account submissions from third parties.[62] In the vast majority of ITC determinations, the public interest factors have not affected the ITC's decision to issue an exclusion order. In the present case, the ITC received

[57] Complaint, *supra* note 7, at 8.
[58] Complaint, *supra* note 7, at 27.
[59] Opinion, Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, Doc. ID 467457 (accessed by logging into the Electronic Document Information System at www.usitc.gov.).
[60] *Id.*at 6.
[61] *Id.*
[62] *See* Burger, *supra* note 37.

lengthy public interest submissions by third parties T-Mobile and Google, both opposing any type of exclusion order.[63]T-Mobile stated in its submission that:

> Due to the lack of short-term substitutes, issuing an exclusion and/or cease-and-desist order against HTC's Android smartphones would harm T-Mobile's U.S. customers and impede U.S. policy of promoting the rapid adoption of next generation wireless networks and smartphones.[64]

T-Mobile also stated that it is the only national carrier that does not offer the Apple iPhone, and therefore it would be more vulnerable to the effects of an exclusion order due to its reliance on HTC Android products.[65] As a result of this vulnerability, T-Mobile requested that if the ITC entered an exclusion order, that it allow a "four-to-six month transition period.[66] Google argued that that an exclusion order would "drive up prices, diminish service, decrease consumers' access to the technology, and reduce innovation."[67] Google also argued that excluding HTC Android devices from the United States would threaten the Android platform itself and increase the likelihood that Apple would obtain a monopoly over the mobile device industry.[68]

---

[63] Eric Schweibenz & Lisa Mandrusiak, *Technology Properties Limited Files New 337 Complaint Regarding Certain Computers and Computer Peripheral Devices*, ITC LAW BLOG (Mar. 29, 2012, 9:39 PM), http://www.itcblog.com/20120329/technology-properties-limited-files-new-337-complaint-regarding-certain-computers-and-computer-peripheral-devices/.
[64] Third Party T-Mobile USA, Inc.'s Statement Regarding Public Interest, Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, Doc. ID 460918 (accessed by logging into the Electronic Document Information System at www.usitc.gov.).
[65] Additional Views of Commissioner Pinkert on Remedy and the Public Interest, Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, Doc. ID 467458 (accessed by logging into the Electronic Document Information System at www.usitc.gov.).
[66] *Id.*
[67] Submission of Google Inc. in Response, Certain Personal Data and Mobile Communications Devices and Related Software, Inv. No. 337-TA-710, Doc. ID 460904 (accessed by logging into the Electronic Document Information System at www.usitc.gov.).
[68] *Id.*

iv. The Commission's Analysis of the §337 Public Interest Factors

The ITC examined the case under each of the four public interest factors. Under the first factor, "Public Health and Welfare," HTC argued that the public health would be in jeopardy due to the lacking benefits of mobile telephone applications.[69] The ITC quickly dismissed this point because HTC did not show any evidence that its phones handled the applications better than other Android carriers.[70] The ITC was also not persuaded by the second factor, "the effect of exclusion on United States consumers[71]," because HTC could not demonstrate the unavailability of substitutes for their smartphones.[72] The third factor, "Production of Like or Directly Competitive Articles in the United States," also carried no weight because no smartphones are manufactured in the U.S. and therefore the exclusion order would not result in a deficiency in production.[73] The ITC was however persuaded by T-Mobile's argument under the public interest factor, "Competitive Conditions in the United States Economy." The ITC found that due to T-Mobile's impact on the smartphone market their request for a four-month transition period was reasonable. Although the "Competitive Conditions" factor has never been cited as a reason for denying injunction, it is consistent with the legislative intent when §337 was adopted.[74]

---

[69] T-Mobile USA' Statement, *supra* note 64.

[70] T-Mobile USA' Statement, *supra* note 64.
[71] *See supra* note 37.
[72] *See supra* note 65.
[73] *See supra* note 65.
[74] Congress indicated that competitive conditions were intended to be an important part of the public interest analysis. From the legislative history:

> "Should the Commission find that issuing an exclusion order would have a greater adverse impact on the public health and welfare; on competitive conditions in the United States economy; on production of like or directly competitive articles in the United States; or on the United States consumer, than would be gained by protecting the patent holder (within the context of the U.S. patent laws) then the Committee feels that such exclusion order should not be issued. This would be particularly true in cases where there is any evidence of price gouging or monopolistic practices in the domestic industry."

S. Rep. No. 93-1298, 93rd Cong., 2d Sess. 197 (1974)

v. The Commission's Modified Exclusion Order

The ITC "has broad discretion in selecting the form, scope, and extent of the remedy in a section 337 proceeding."[75] As a result of the section 337 violations and based on the public interest factors, the ITC determined that the appropriate remedy was a limited exclusion order.[76] The order prohibits the entry of personal data and mobile communications devices and related software that infringe claims 1 or 8 of the '647 patent.[77] This seems consistent with the expected ITC action of issuing an injunction once an infringement has been found. What was inconsistent and surprising was the ITC's determination that "based on consideration of the competitive conditions in the United States economy," the exclusion order would not commence until April 19, 2012, in order "to provide a transition period for U.S. carriers."[78] The date set by the ITC for the commencement of the exclusion order provided HTC with a four-month window to not only design around the infringed patent, but also to continue selling and importing the infringing product in the United States. The ITC also determined, "based on consideration of the effect of exclusion on United States consumers, that until December 19, 2013, HTC may import refurbished handsets to be provided to consumers as replacements."[79] The ITC specified that HTC may not call new devices "refurbished" and import them as replacements.[80] They also did not recommend a cease and desist order because HTC inventories of the accused products in the United States are used for testing only and are not for sale.[81]

---

[75] Viscofan, S.A. v. United States Int'l Trade Comm'n, 787 F.2d 544, 548 (Fed. Cir. 1986).
[76] *See supra* note 49.
[77] *See supra* note 49.
[78] *See supra* note 49.
[79] *See supra* note 49.
[80] *See* Chien & Lemley, *supra* note 38.
[81] *See* Opinion, *supra* note 59.

V. Previous Instances of Public Interest Outweighing Injunction

Only three times since its formation has the ITC denied injunctive relief after an infringement has been found.[82] These three determinations occurred over 25 years ago and were made in light of an impending oil crisis, military research, and concerns for public health, respectively.

i. Certain Automatic Crankpin Grinders

The first instance occurred in 1979 with *In re Certain Automatic Crankpin Grinders*. There, the ITC denied an exclusion order for seemingly similar reasons to our case at hand; the primary one being that "the domestic industry cannot supply the demand for new orders of the patented product within a commercially reasonable length of time."[83] The second reason for denying an exclusion order was that the order would severely jeopardize Ford's ability to meet Congress' and the President's established policy on increasing fuel economy.[84] Because of a major oil crisis in 1979, the ITC found that protecting the increased fuel economy policy outweighed the harm flowing from the importation of an infringing product.[85]

ii. Certain Inclined-Field Acceleration

The second instance occurred in 1980 in *Certain Inclined-Field Acceleration Tubes and Components Thereof*. In that investigation, the ITC refused to exclude the infringing tubes

---

[82] *See* Chien & Lemley, *supra* note 38.
[83] Certain Automatic Crankpin Grinders, Inv. No. 337-TA-60, USITC Pub. 1022 at 18 (Dec. 1979).
[84] *Id.*
[85] *See* Chien & Lemley, *supra* note 38.

because they were "substantially less expensive" and "indispensable to research."[86] It turns out that the research that the ITC was protecting was related to nuclear technology and used for weapons development.[87] Because of the potential importance of this research to the public, the ITC decided that an exclusion order was not warranted.[88]

iii. Certain Fluidized Supporting Apparatus and Components Thereof

The third previous time the ITC refused to grant injunction was in 1984 in *Certain Fluidized Supporting Apparatus and Components Thereof.* In that case the ITC found that the infringing products, burn beds, should not be excluded from importation and use because their exclusion would cause patients to "not have access to burn beds at all."[89] The ITC based its decision on competitive conditions and the availability of replacements, but primarily pointed to the public health concern of not having enough burn beds for victims.[90]

None of these cases preceding Apple v. HTC had the type of limited exclusion order seen here. Where the previous decisions were outright refusals to exclude based on the public interest, the novel decision in Apple v. HTC delayed the exclusion order in the interest of one company. The preceding cases demonstrate that the ITC considers a variety of factors to be relevant to its decision regarding remedies, including the immediate effects of the exclusion order (oil crisis of 1979), the future consequences (nuclear research), and public health (burn beds).

---

[86] Certain Inclined-Field Acceleration Tubes and Components Thereof, Inv. No. 337-TA-67, USITC Pub. 1119 at 27 (Dec. 1980).
[87] *Id.*
[88] *Id.*
[89] Certain Fluidized Supporting Apparatus and Components Thereof, USITC Inv. No. 337-TA-182/188, USITC Pub. 1667 at 23 (Oct. 1984).
[90] *Id.*

VI. ITC Investigations Since Apple v. HTC

As of January 2013, of the 151 section 337 investigations initiated since Apple v. HTC, only fifteen have found violations of section 337. Of the fifteen investigations resulting in a violation determination and some sort of exclusion order or cease and desist order, none of them contained a similar extended effective date as Apple v. HTC. This may suggest that the determination in Apple v. HTC is an outlier and will not affect the plaintiff's use of the ITC as a patent forum. It is however useful to look at the ITC's reasoning in substantially similar cases to determine what was so special about Apple v. HTC to warrant the modified exclusion order.

i. Microsoft v. Motorola

Microsoft filed a complaint in the ITC against Motorola in 2010, the same year Apple initiated its suit against HTC.[91] Microsoft alleged that certain Motorola smartphone products such as the Droid 2, Droid X, and Backflip infringe Microsoft patents.[92] This is a remarkably similar case to Apple v. HTC in that it involved the owner of software patents suing infringing smart phones for allegedly using similar software. The result here, however, was different. Here, Microsoft obtained a limited exclusion order prohibiting Motorola from importing any infringing products into the United States. Unlike Apple v. HTC, this limited exclusion order did not contain an extended time line for Motorola to modify their product before taking effect. Just as in Apple v. HTC, there were third party submissions accepted by the ITC on the issue of the effect an exclusion order would have on the public interest. Two companies, the Association for

[91] Certain Mobile Devices, Associated Software, and Components Thereof, Inv. No. 337-TA-744, USITC Pub. 4384 at 23.

[92] Complaint with Public Exhibits, Certain Mobile Devices, Associate Software, and Components Thereof, USITC Inv. No. 337-TA-744, Doc. ID. 434802 (accessed by logging into the Electronic Document Information System at www.usitc.gov).

Competitive Technology, Inc. ("ACT")[93] and Google, submitted briefs in support of and against an exclusion order respectively. ACT argued for an exclusion order by stating that; (1) the patents at issue are "not standard-essential"; and (2) the "competition in the mobile devices market is currently robust."[94] ATC's main point was that an exclusion of Motorola's products would not be to the detriment of the public because either Microsoft or "any of the other 32 handset manufacturers competing in the mobile space"[95] would be able to fill consumer demand.[96]

Google's argument was essentially the exact same one it made in Apple v. HTC; that an exclusion order would harm U.S. consumers through "increases in prices, decreases in service, decreases in selection, or decreases in innovation and long-term economic growth."[97] Google also argued that the Android system was the only open mobile computing platform available in the U.S. and that the public interest in continued access to Android weighed against an exclusion order.[98] It is important to note that only a month after Google submitted its brief against an

[93] "ACT is an international grassroots advocacy and education organization representing more than 5,000 small and mid-size app developers and information technology firms. It is the only organization focused on the needs of small business innovators from around the world. ACT advocates for an environment that inspires and rewards innovation while providing resources to help its members leverage their intellectual assets to raise capital, create jobs, and continue innovating. In addition to its small business membership, ACT and ACT 4 Apps has several Sponsor Members including Apple, AT&T, BlackBerry, eBay, Facebook, Intel, Microsoft, Oracle, PayPal, VeriSign, and Verizon." *available at* http://actonline.org/about-us/.
[94] Certain Mobile Devices, Associate Software, and Components Thereof, Inv. No. 337-TA-744, Doc. ID. 482094, Comm'n Op. at 27 (June 5, 2012).
[95] *See* Certain Mobile Devices, Associate Software, and Components Thereof, *supra* note 91. (ACT represents some of those 32 other competitors and is also sponsored by Microsoft, which makes it easy to see why they filed on their behalf.)
[96] *Id.* at 28.
[97] *Id.*
[98] *Id*. at 29.

exclusion order due to "public interest" factors, it finalized its purchase of Motorola for $12.5 billion dollars.[99]

The ITC was ultimately persuaded by the arguments of Microsoft and ACT and issued a limited exclusion order, prohibiting the importation and sale of certain infringing Motorola devices. Why did Motorola not get a four-month window to design around the patents as HTC did? What in this case was different for the ITC to come to a different conclusion?

The only obvious difference between the two decisions is the submission in Apple v. HTC by T-Mobile stating that its business would suffer under an HTC exclusion order. In fact, T-Mobile argued that because of its reliance on HTC Android devices, its only other smartphone, the Samsung Galaxy, would not be able to meet expected consumer demand in the short term, and therefore requested a "four-to-six month transition period…so that T-Mobile and the rest of the industry could change to other devices."[100] If T-Mobile's submission that an exclusion order would harm it was the deciding factor in extending the order, would Motorola have been given the same opportunity if, say a company like AT&T submitted a similar brief on their behalf? I believe the answer may be yes.

The ITC also referenced the President's policy of wireless coverage infrastructure development as a factor in modifying the exclusion order in the HTC investigation. It quoted a Department of Justice report;

> "Innovation in wireless technology drives innovation throughout our 21st-century information economy, helping to increase productivity, create jobs, and improve our daily lives. Vigorous competition is essential to ensuring continued innovation and maintaining low prices."[101]

---

[99] David Goldman, *Google seals $13 billion Motorola buy,* CNN MONEY (May 22, 2012, 10:20AM), http://money.cnn.com/2012/05/22/technology/google-motorola/index.htm.
[100] Opinion, *supra* note 59, at 79.
[101] Opinion, *supra* note 59, at 80.

The DOJ went further and explicitly endorsed T-Mobile; "T-Mobile has also been an innovator in terms of network development and deployment."[102] The ITC stated that "to the extent an immediate exclusion of HTC Android smartphones would have a substantial impact on T-Mobile's competitiveness, such an order would not be in the public interest."[103]

Figure 3: Android Market Share by Original Equipment Manufacturer (OEM)[104]

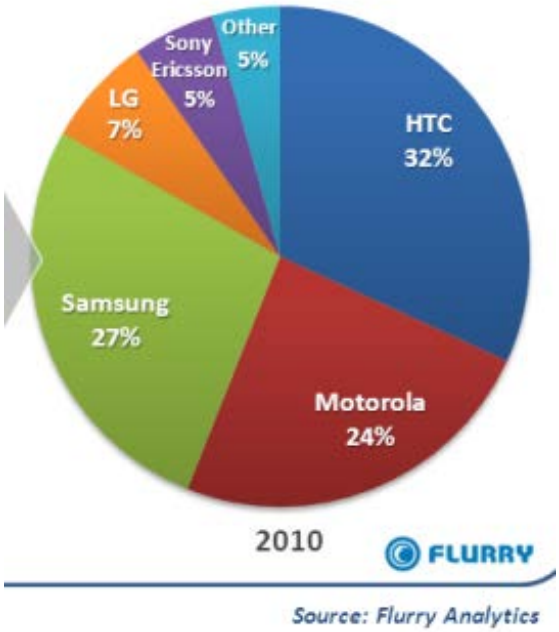


Figure 3 shows that in 2010, the year both Apple's and Microsoft's suits were initiated in the ITC, Motorola had a 24% market share of Android products, only 8% less than HTC. T-Mobile argued that since it is the only carrier to not carry the Apple iPhone, the loss of HTC Android products would be detrimental to its business. As it turns out, T-Mobile is not the only cell phone carrier that does not sell the iPhone. U.S. Cellular, the 8th largest provider in the

[102] Opinion, *supra* note 59, at 80.
[103] Opinion, *supra* note 59, at 81.
[104] Peter Farago, *Android Special Report: Is Samdroid the new Wintel?*, FLURRY BLOG (Jan. 5, 2011), http://blog.flurry.com/default.aspx?Tag=HTC.

United States (T-Mobile is 4th largest), also does not carry the iPhone.[105] Therefore, with the exclusion order against Motorola, U.S. Cellular was unable to sell the Android phone with 24% of the market share. With these statistics, the two cases become even more similar, and it appears that a simple submission from a company such as U.S. Cellular on Motorola's behalf may have been sufficient for the ITC to have issued a modified exclusion order, thereby giving Motorola time to design around the infringed patent.

Essentially, it appears that the ITC granted the modified exclusion order, delaying it for four months, solely because of the effect it would have on the competitiveness of one company that was furthering a government policy of network building. This seems contrary to an argument in the *Microsoft v. Motorola* case with which the ITC agreed; that the competition in the mobile field is robust enough to fill in any gaps left by the exclusion order. T-Mobile's third party submission essentially nullified Apple's victory in having an infringement found. Apple's competition was not stopped, but instead was given the opportunity to continue selling infringing products.

VII. Policy Implications

Future ITC holdings consistent with the one in *Apple v. HTC* could significantly weaken patentees' ability to stop competitors from getting their products onto the US market.[106] One view is that the weakened ability to obtain injunctions in both federal court and the ITC will force companies and other patentees instead, to fight one another in the marketplace, thereby

[105] *Grading the top 10 U.S. carriers in the first quarter*, FIERCE WIRELESS, http://www.fiercewireless.com/special-reports/grading-top-10-us-carriers-first-quarter-2012 (last visited Mar. 16, 2013).
[106] Steven Seidenberg, *ITC ruling could weaken patentees' rights*, INSIDE COUNSEL (Mar. 1, 2012), http://www.insidecounsel.com/2012/03/01/itc-ruling-could-weaken-patentees-rights.

benefiting consumers.[107] An opposing view is that the modified exclusion orders, allowing infringing products to continue to be imported and sold for a time period, are a violation of the patentee's fundamental property rights. The issue seems to be how the ITC will balance the newly championed public interest factors against the property interests of patent holders.

The dichotomy between the holdings in the Apple and Microsoft investigations also make it difficult to predict the outcome of an investigation once an infringement is found. After examining the similarities and differences between *Apple v. HTC* and *Microsoft v. Motorola*, it appears that the two important factors are; how important the infringing product is to the consumer, and whether a third party submission on the effect of an exclusion order on its economic status is persuasive. It seems that, as in *Apple v. HTC*, it only takes a third party submission from one influential company to persuade the ITC to modify its orders and render the patentee's victory only nominal.

What about upholding principles of intellectual property law? Patents are essentially a right given to the owner to exclude others from using the invention. Allowing the competitive interests of one company to trump our fundamentals of property law does not seem fair. Is it Apple's fault that T-Mobile is carrying an infringing product? Maybe it should be up to T-Mobile to police its products and make sure that none of them are infringing. Instead, it looks like the ITC is telling Apple that its interests in its own property are not as important as T-Mobile's competitive stance in the marketplace. Microsoft may have been one third-party submission away from possibly getting the same treatment as Apple. If this is the case, and third parties wield this much power, then it seems that we are abandoning our history of intellectual property protection.

[107] Seidenberg, *supra* note 106.

The valid response to this author's concerns about Apple's intellectual property rights is this: it is not the ITC's function to protect intellectual property rights. That function remains with the federal courts. Instead, the purpose of the ITC is to promote fair trade and competition in products.[108] This purpose is protected by the domestic industry requirement in the statute.[109] A litigant who simply holds a patent does not have standing to file suit in the ITC like they do in federal court. The ITC must determine that the patent holder is part of a domestic industry before starting the investigation. Congress made this distinction clear, calling the domestic industry requirement the "gatekeeper," that prevents the "[transformation of] the ITC into an intellectual property court."[110] The increasing number of ITC litigants suggests that the ITC is being utilized as an intellectual property court instead of a fair trade agency, where patentees are taking advantage of the ITC's powers but without any regard to the agency's function. The decision in *Apple v. HTC* may be an example of the ITC putting its foot down and finally functioning as it is intended to. While this is a good sign for the ITC and for consumers, it may not be for patent holders looking for alternative forums than federal court.

ITC exclusion orders have historically followed the "all-or-nothing" approach.[111] The ITC has regularly stopped the importation of products even if they infringe only a tiny aspect of the patent at issue.[112] The application of the all-or-nothing approach, coupled with inclusion of the public interest factors, creates the possibility that patentees may technically win their case, but receive little or no relief. It is not clear whether or not the ITC will continue to use the public

---

[108] UNITED STATES INTERNATIONAL TRADE COMMISSION, *supra* note 1.
[109] 19 U.S.C. §1337(a)(1)(A) (2004).
[110] Colleen V. Chien, *Protecting Domestic Industries at the ITC*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 169, 178 (2011) (citing 132 CONG. REC. 30,816 n.5 (1986) (statement of Rep. Kastenmeier)).
[111] Chien & Lemley, *supra* note 38.
[112] Seidenberg, *supra* note 8.

interest factors to modify or deny exclusion orders, but there are many practitioners who support it.

Law professors Colleen Chien and Mark Lemley are concerned with the impact that strict exclusion orders have on the public and say that cases like Apple v. HTC "have many people concerned that soon judicial decisions, rather than consumers, will decide what products make it onto Santa's sleigh."[113] But Chien and Lemley think the all-or-nothing approach is not the only way. They believe that §337 gives the ITC broad discretion to tailor an appropriate remedy for each case.[114] They both supported the modified exclusion order made by the ITC and just weeks before the decision came down, they recommended delaying injunctions to "allow a defendant to redesign its product," and it appears that the ITC took their advice.[115] Chien and Lemley are proponents of the ITC increasing the application of case specific and tailored remedies to each violation so as to completely take both the public interest and the patentee's interests into account.[116]

There are three statutory powers given to the ITC that Chien and Lemley believe can provide the flexibility to create more case specific forms of relief: (1) the power of what to exclude; (2) when to exclude it; and (3) whether to set a bond.[117] Grandfathering certain products is one of the ways that Chien and Lemley would like the ITC to tailor its remedies.[118] By limiting the exclusion order to only future versions of the product, and allowing current versions to remain, both the "consumers and competition are less likely to suffer."[119]

---

[113] Chien & Lemley, *supra* note 38.
[114] Chien & Lemley, *supra* note 40.
[115] Chien & Lemley, *supra* note 38.
[116] Chien & Lemley, *supra* note 40.
[117] Chien & Lemley, *supra* note 40, at 5.
[118] Chien & Lemley, *supra* note 40, at 43.
[119] Chien & Lemley, *supra* note 40, at 43.

Chien and Lemley also suggest delaying exclusion orders. The first reason is so that consumers do not have to go without the infringing products until they can be replaced.[120] The second reason is so that the respondent can attempt to design around the patent.[121] While patentees would argue that giving the respondent time to design around the patent is unfair and harmful, Lemley says that the design around period will be useful to distinguish what patents are critical and which ones are not.[122] His reasoning is that if a respondent can design around the patent within say, six months, then the invention must not be that valuable, especially not enough to hold up production of the respondents entire product.[123] Professor Arti Rai of Duke Law School believes that the ITC may continue to delay import bans "in situations where the number of infringed patents is small, a design-around is fast, and the patents represent only a small piece of the [infringing] product."[124] This approach was beneficial to HTC because it only infringed two claims of an easily designed around software patent.[125] What if the patent is not for software? Will the delayed exclusion order still be beneficial? Hardware makers generally require more time and effort to design around patents, therefore they will not likely benefit from the short delay of an exclusion order.[126] If the ITC grants more extensive delays in the exclusion order, then the patentee's domestic industry may be harmed. Professor Jonas Anderson of American University's Law School thinks that a "major factor in the ITC's decision" will be "if

[120] Chien & Lemley, *supra* note 40, at 43.
[121] Chien & Lemley, *supra* note 40, at 34.
[122] Chien & Lemley, *supra* note 40, at 36.
[123] Chien & Lemley, *supra* note 40, at 35.
[124] Seidenberg, *supra* note 106.
[125] Seidenberg, *supra* note 106.
[126] Seidenberg, *supra* note 106.

a patentee's domestic industry will be harmed by a delay," and that if so, then the ITC is "unlikely to delay."[127]

Finally, Chien and Lemley recommend that the ITC use its power to set temporary bonds more often and for longer periods of time.[128] They suggest the combination of a delayed exclusion order and an extended bond period to have the effect of the respondent essentially paying a royalty for the privilege of selling their infringing products.[129] This will ensure that the patentees are compensated during the transition period.

Chien and Lemley make these suggestions in the public's interest as a defense against product hold-up. As an indication that Chien and Lemley's suggestions are gaining support, the ITC utilized two of them in Apple v. HTC; both grandfathering in existing HTC smart-phones, and delaying the exclusion order. Another indication that the ITC may be more open to tailoring its remedies is its 2011 rule change which allows the ALJ, under Commission order, to take public interest evidence throughout each stage of the case, instead of waiting until the end.[130] This new procedure will allow third parties to respond to each issue as it arises instead of attempting to sway the ITC with a single argument at the close of the investigation.

All in all, it seems that the ITC may be softening its stance on automatic injunctions where an infringement is found. While there are still only four examples of this tailoring occurring, there is a compelling argument by practitioners that this practice should continue and become more prevalent. As a result of the decision in Apple v. HTC and the push for more tailored relief, patentees may need to meet a higher burden to show that their economic status is harmed by continued importation of the infringing product. The possibility of tailored remedies may also

---

[127] Seidenberg, *supra* note 106.
[128] Chien & Lemley, *supra* note 40, at 35.
[129] Chien & Lemley, *supra* note 40, at 41.
[130] 19 C.F.R. §210 (2011).

only effect patentees with widely used or important products. The examples of tailored remedies seen so far have been issued either because the product was critical to public health, scientific research, or harm to the consumers. If the patentee's product is not widely used by the public or critical to some other public interest factor, then there is little evidence that they would be unable to obtain a strict exclusion order against a violating product. It is the patentees with more pervasive products that may encounter the tailored remedies simply because their product is more likely to fall under the umbrella of the §337 public interest factors.[131] The number of increasing investigations suggests that patentees are not dissuaded from continuing to try their luck in the ITC. James Adduci, co-founder of the top ranked patent boutique in the country, said in 2012, "The ITC has become the hottest forum for litigating IP rights of U.S. and foreign companies."[132]

VIII. Conclusion

The ITC has denied immediate injunctions in its history for reasons including, oil crisis, nuclear research, public health, and now to protect the competitiveness of a cellular communications provider. It appears that a defendant in an ITC investigation may get off the hook by having an economically important friend that can submit a third party brief indicating that an exclusion order would harm their business. This could be bad news for patentees attempting to exclude their competitors imported products. The ITC may have been taking a stand in Apple v. HTC, showing future litigants that the ITC is meant to promote fair trade, not to litigate patent disputes. If the ITC continues to issue tailored remedies, patentees may have to

[131] *See* Crouch, *supra* note 9.
[132] Purzycki, *supra* note 31.

be satisfied with the lengthy process of litigating in federal court. Luckily for future ITC plaintiffs, the numbers indicate otherwise. The number of investigations is increasing regularly each year, and the ITC has never been a more popular place to litigate issues of intellectual property.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 5, PAGE 171

Sending Servers to the Sky: Can Bit Torrent Piracy be Perpetuated by the Use of Unmanned Drones?

David Hutchinson

TABLE OF CONTENTS

INTRODUCTION 172

I. TERRITORIALITY & COPYRIGHT LAW 175

A. BERNE CONVENTION 176

B. TRIPs 177

C. WTC 178

D. PROPOSED SOLUTIONS 180

II. DRONES 184

A. DOMESTIC USE 186

B. INTERNATIONAL USE 188

CONCLUSION 190

MODEL CLAUSE FOR AN INTERNATIONAL TREATY 191

INTRODUCTION

> ***"With the development of GPS controlled drones, far-reaching cheap radio equipment and tiny new computers... we're going to experiment with sending out some small drones that will float some kilometers up in the air. This way our machines will have to be shut down with aeroplanes in order to shut down the system. A real act of war."***[1]
>
> **– The Pirate Bay**

On March 18th 2012 "the galaxy's most resilient Bit Torrent site,"[2] The Pirate Bay declared war on copyright laws around the world. It threatened to take its Bit Torrent piracy programs to the sky in order to avoid jurisdiction.

Bit Torrent is a system by which Internet users can connect to one another's computers to share files.[3] Users visit a website, such as the aforementioned The Pirate Bay, and can then access torrent files from the website's network of users.[4] One user must create a Torrent file of the content he or she wishes to share.[5] That file then serves as a guide for other users on a given network to access and download the content.[6] Each time a file is downloaded from the user, a copy is made which increases access for the next user seeking to download the same content. A user can then download a number of fragments of each file from a number of different users until the download is completed, making the process rather quick.[7] The more users in a given network, the more access a user has to fragments of a desired file, and the faster that user is able

---

[1] MrSpock, THE PIRATE BAY, *TPB Loss*, (Mar. 18, 2012), http://thepiratebay.se/blog/210 (last visited Oct. 27, 2013).
[2] THE PIRATE BAY, http://thepiratebay.se (last visited Oct. 27, 2013).
[3] Grace Espinosa, *Internet Piracy: Is Protecting Intellectual Property Worth Government Censorship?*, 18 Tex. Wesleyan L. Rev. 309, 313-14 (2011).
[4] *Id.*
[5] Luke M. Rona, *Off with the Head? How Eliminating Search and Index Functionality Reduces Secondary Liability in Peer-to-Peer File-Sharing Cases*, 7 Wash. J.L. Tech. & Arts 27, 34 (2011).
[6] *Id.*
[7] Espinosa, *supra* note 3.

to download that particular file.[8] Due to the quick nature of the downloading process, as well as the user driven content stream, Bit Torrent has become the most popular type of peer-to-peer downloading system for copyright protected files.[9] [10]

Although Bit Torrent systems have legitimate purposes,[11] they are most commonly used to share, or "pirate," copyright protected content illegally.[12] Files such as movies, music, books and computer software can all be easily shared between users via Bit Torrent.[13] Due to the way in which files are spread, the most popular content is the easiest to access on each Bit Torrent network, as more and more users will provide access to the fragments of those files.[14] This system complicates who should bear responsibility for each infringement: the users of the peer-to-peer system who actually share the files, or the network's creators who lead each user to the content?[15] On the one side, holding users responsible would be complicated as there are millions of Bit Torrent users, all of which uploading only fragments of the copyright protected material.[16] On the other, the websites responsible for creating this network don't actually share any of the files from their servers; they simply facilitate the peer-to-peer file sharing by showing which users are sharing fragments of which files.[17]

---

[8] *Id.* at 313.
[9] John Malcolm, *Film Piracy and the Pirate Bay Cases Indiana University School of Law-Bloomingto*n, April 13, 2010, 12 Engage: J. Federalist Soc'y Prac. Groups 25 (2011).
[10] Espinosa, *supra* note 3, at 313.
[11] Sandra Leigh King, *While You Were Sleeping*, 11 SMU Sci. & Tech. L. Rev. 291, 304 (2008)
[12] Matthew Helton, *Secondary Liability for Copyright Infringement: Bittorrent As A Vehicle for Establishing A New Copyright Definition for Staple Articles of Commerce*, 40 Colum. J.L. & Soc. Probs. 1, 22 (2006).
[13] *Id.*
[14] *Id.*
[15] Rona, *supra* note 5.
[16] Rona, *supra* note 5.
[17] *Id.*

The Pirate Bay, a Bit Torrent website known for unapologetically providing access to the world's most popular collection of pirated files, exists centrally within these copyright controversies. The group responsible for The Pirate Bay has become a figurehead of the online piracy movement, often embracing challenges to the legal validity of Bit Torrent systems for sharing pirated material.[18] As such, the group continues to create innovative ways to make its system work within an antiquated legal framework that has yet to catch up to technologies such as Bit Torrent.

Until now, The Pirate Bay has necessarily operated from stationary servers at different on-ground locations around the world. Now, however, the group's latest innovation threatens to launch its servers into the skies using Low Orbit Service Stations, so as to avoid any particular jurisdiction and, more likely, further complicate the issues surrounding Internet piracy.[19] If such a system were to come to fruition, an already controversial debate about the reaches of international copyright law would take on new complexities. This note seeks to analyze some of the general international copyright issues, such as territoriality in copyright law, as well as issues specific to The Pirate Bay's latest threat, such as international and domestic airspace regulation. Ultimately this note will conclude by offering a model clause for an international treaty, seeking to address the complexities with international copyright in hopes that the solution to this worldwide piracy problem can stop short of any "real act of war."[20]

[18] Malcolm, *supra* note 9.
[19] Wired, *The Pirate Bay Plans Low Orbit Server Drones to Escape Legal Jurisdiction*, March 19, 2012, http://www.wired.co.uk/news/archive/2012-03/19/pirate-bay-drones (last accessed January 23, 2013).
[20] The Pirate Bay, *supra* note 1.

TERRITORIALITY & COPYRIGHT LAW

If all internet-connected nations would agree on unified copyright laws, how would piracy ever escape jurisdiction? Although the answer is it couldn't, unifying copyright law has never been a simple task.[21] A fundamental question of copyright law remains which territory's law to apply to copyright infringement.[22] This question is further complicated when works can be released in a number of different countries simultaneously, and downloaded from users all over the globe simultaneously via the Internet. If choice of law were tailored to where the work was downloaded from, courts would be forced to apply numerous foreign laws to any case of online infringement.[23]

All copyright is territorially based,[24] in large part because each nation differs in the values it places on intellectual property rights.[25] Efforts to unify copyright laws among nations, such as the Berne Convention, and the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPs"), have helped to provide minimum standards of intellectual property rights among their signatory nations.[26] More recently the WCT treaty has attempted to address the problem that as technology changes so do the ways in which infringement takes place.[27] Although each of these treaties has been important to international

[21] Edward Lee, *The New Canon: Using or Misusing Foreign Law to Decide Domestic Intellectual Property Claims*, 46 Harv. Int'l L.J. 1, 8-9 (2005).
[22] Jane C. Ginsburg, *The Cyberian Captivity of Copyright: Territoriality and Authors' Rights in A Networked World*, 20 Santa Clara Computer & High Tech. L.J. 185, 186 (2003).
[23] *Id.*
[24] Ginsburg, *supra* note 22.
[25] Lee, *supra* note 21.
[26] *Id.*
[27] Stephen Bright, *The Current State of Bittorrent in International Law: Why Copyright Law Is Ineffective and What Needs to Change*, 17 New Eng. J. Int'l & Comp. L. 265, 285 (2011).

intellectual property rights, each has stopped short of effective unification of laws, to the continuous detriment of copyright holders around the world.

BERNE CONVENTION

The Berne Convention for the Protection of Literary and Artistic Works is said to be "the oldest and most elaborate international arrangement governing the protection of copyright."[28] 131 countries have ratified the treaty, which was originally created in 1886, and has been adhered to by the United States since becoming a signatory nation in 1989.[29] The purpose of the Berne Convention was to allow all signatory nations to maintain separate bodies of copyright law while still maintaining a minimum standard of copyright protection.[30] Locally, implementing the Berne Convention was said to be essential for preventing piracy of American works, such as movies, music and art overseas, and was referred to as a "clear and unmistakable signal to foreign pirates that we will insist upon fair trade in copyrights based upon the [Berne Convention's] minimum guarantees."[31]

While the Berne Convention has been important to the prevention of certain types of international piracy, it provides myriad examples of why the unification of intellectual property laws has yet to truly come to fruition. One such example is the absence of public interest in the text of the Berne Convention. In the United States a number of competing public interests typically serve as justifications for the implementation of copyright laws, such as fostering

[28] Leonard D. Duboff, *Creativity and Copyright*, Or. St. B. Bull., January 1989, at 4.
[29] *Id.*
[30] Katherine S. Deters, *Retroactivity and Reliance Rights Under Article 18 of the Berne Copyright Convention*, 24 Vand. J. Transnat'l L. 971, 972 (1991).
[31] Duboff, *supra* note 28

societal progress and providing access to information.[32] But public interests differ across nations as each have their own challenges and values to address. Many public interests are served by the Berne Convention's contemplation of the educational importance of copyright.[33] Ultimately, however, the failure to define public interest in the text of the Berne Convention represents one example of the inability of differing nations to agree on what purpose copyright laws should serve; a clear impediment to the unification of intellectual property laws.

TRIPs

Similar to the Berne Convention, the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPs") seeks to provide certain minimum standards for IP protection for the over 140 countries in the World Trade Organization.[34] This agreement extends the protections provided by Berne by encouraging enforcement procedures that are not only reactive to incidents of infringement but also preventative and deterrent.[35] The TRIPs agreement has been lauded as embracing "an understanding that new forms of technology need to be protected, and that similar advancements are being made in the ways in which infringement can occur."[36]

TRIPs represents a global acknowledgement of the need for increased intellectual property protections amid ever-changing technology. However, the agreement further illustrates spaces where countries are unable to agree, thus making international intellectual property protections ineffective. TRIPs allows WTO members to take preventative and deterrent measures

[32] Edward L. Carter, *Harmonization of Copyright Law in Response to Technological Change: Lessons from Europe About Fair Use and Free Expression*, 30 U. La Verne L. Rev. 312, 317 (2009).
[33] Carter, *supra* note 32.
[34] Lee, *supra* note 21.
[35] Bright, *supra* note 27, at 283.
[36] *Id.*

to protect intellectual property rights.[37] Despite this, the agreement creates no duty to do so.[38] This leaves countries like the United States, which plays a relatively active role in intellectual property protection,[39] and countries like Spain and Sweden with more lenient protections[40], at odds with each other in terms of enforcement. As a result, precedents set in one nation have no bearing on the enforcement of protections in another. This allows a network such as The Pirate Bay to operate freely from a nation with more relaxed intellectual property laws, despite the fact that its conduct implicates intellectual property rights globally.[41] With unified regulation of intellectual property violations across the globe, networks like The Pirate Bay would have no safe haven.

WTC

In further response to the ever-changing technological landscape across, the World Intellectual Property Organization Copyright Treaty ("WCT") of 1996 was introduced.[42] The WTC's provisions operate to "protect the integrity of electronic rights management" and "prevent the facilitation of copyright infringement through the circumvention of technological anti-copying devices."[43] As forms of digital media have advanced, producers have developed ways to encrypt files with anti-copying protections known as DRM or digital rights

[37] Scott Burger, *Eradication of A Secondary Infringer's Safe Havens: The Need for A Multilateral Treaty Addressing Secondary Liability in Copyright Law*, 1 Mich. St. J. Int'l L. 143, 151 (2009).
[38] *Id.*
[39] Tara Touloumis, *Buccaneers and Bucks from the Internet: Pirate Bay and the Entertainment Industry*, 19 Seton Hall J. Sports & Ent. L. 253, 262 (2009)
[40] Burger, *supra* note 37.
[41] Touloumis, *supra* note 39.
[42] Ryan J. Shernaman, *The Digital Millennium Copyright Act: The Protector of Anti-Competitive Business Models*, 80 UMKC L. Rev. 545, 550 (2011).
[43] Neil W. Netanel, *The Next Round: The Impact of the Wipo Copyright Treaty on Trips Dispute Settlement*, 37 Va. J. Int'l L. 441, 442 (1997)

management.[44] Though DRMs serve the purpose of limiting opportunities for piracy, some of the encryptions can limit file functionality, which could theoretically have the undesirable result of limiting the ways people can communicate via the Internet.[45] Because of this, encryptions can only be so complex, and though they prevent the average person from creating copies of copyrighted files, savvy pirates have still managed to circumvent these encryptions. Additionally, DRMs have been criticized as encouraging a switch in focus from production of copyrighted works to protection of copyrighted works.[46] Both of these concerns were addressed by the treaty, which acknowledges the need for narrow tailoring of laws in order to prevent DRMs potential limitations.[47]

As with the Berne Convention and the TRIPs agreement, the WCT stops short of creating an effective unified system of intellectual property law. In fact, the WCT is recognized as giving countries "considerable latitude" in allowing DRM use for protecting copyright owners' exclusive rights.[48] This means that DRMs in some countries can be weaker or stronger depending on the country. By continuing to allow weaker DRM protections, encryptions can continue to be circumvented, and the bigger problem, mass infringements via Bit Torrent, will persist.[49] Though the WCT provides some greater protections for copyright holders, a unified system of intellectual property law is still necessary before piracy can be effectively addressed.

---

[44] Shernaman, *supra* note 42.
[45] Netanel, *supra* note 43.
[46] Michael Boardman, *Digital Copyright Protection and Graduated Response: A Global Perspective*, 33 Loy. L.A. Int'l & Comp. L. Rev. 223, 245 (2011).
[47] Boardman, *supra* note 46.

[48] *Id.*
[49] Burger, *supra* note 37.

PROPOSED SOLUTIONS

As noted above, Bit Torrent systems make it difficult to place blame on any one party when infringement occurs because of the sheer number of users, and the form in which files are shared. One popular solution has been simply to change the culture surrounding online piracy.[50] The Recording Industry Association of America attempted to do this through litigation and pro-copyright publicity.[51] By pursuing claims against users, the RIAA hoped to create a deterrent effect, educating all users, and in many cases their parents who own the computer being used for piracy, what potential liability exists for acts of online piracy.[52] Some scholars believe this attempt at deterrence is a lost cause, however, as the anti-copyright sentiment runs deep in the users of peer-to-peer file sharing's mentality.[53] Where the RIAA hit its biggest snag in pursuing these claims was with discovering the identity of each user in order to bring the claims. Internet Service Providers such as AT&T and Verizon were unwilling to disclose information about their users, so the RIAA largely abandoned this effort starting in 2008.[54] But even if this were a locally successful solution, it also ignores the over-arching problem of jurisdiction. Even if each user in the United States were deterred from file sharing, millions of users would still exist in other countries, where litigation may not be diligently pursued.

Another local solution to the peer-to-peer file-sharing problem is for the RIAA to come to an agreement with Internet Service Providers about enforcing copyright via a graduated response system. Users who are known to be infringing would be given warnings about their conduct, and

---

[50] Sandra Leigh King, *While You Were Sleeping*, 11 SMU Sci. & Tech. L. Rev. 291, 334 (2008).
[51] Genan Zilkha, *The Riaa's Troubling Solution to File-Sharing*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667, 685 (2010).
[52] Ben Depoorter & Sven Vanneste, *Norms and Enforcement: The Case Against Copyright Litigation*, 84 Or. L. Rev. 1127, 1128 (2005).
[53] *Id.*
[54] Zilkha, *supra* note 51 at 88.

eventually dropped from their provider if the infringing conduct persists. Though these responses may have a deterrent effect on users, many issues arise with enforcement. One such issue is cost. Internet Service Providers would be required to incur the cost of investigating claims in order to issue each response.[55] Additionally, each time a user is banned from their provider, that user is no longer a paying customer. A similar system in the United Kingdom was estimated to cost providers around 500 million pounds (80 Million U.S. dollars) over ten years.[56] More worrisome to such a system, however, has to be the international community's unenthusiastic response.[57] The European Parliament voted 633-13 against implementation of an international agreement that would require signatory nations to adopt such a system.[58] That agreement has now been modified to remove any such requirement.[59] Similar to the attempt at litigating claims against users directly, if this graduated response system of copyright enforcement does not catch on internationally, millions of users can continue to engage in online piracy around the world.

Such a system has recently been introduced in the United States. Since the RIAA has for the moment stopped pursuing claims against those who download copyrighted files in the United States, copyright holders have begun to work with Internet service providers in order to implement a graduated response type system. The details of the system are somewhat vague as the system is so new, but it is rumored to be a system in which a user gets six separate warnings. The first few simply let the user know that they may be penalized if they continue to engage in online piracy. The next step is to then block internet access until the user signs-in, acknowledging receipt of the messages. From there the system is rumored to then reduce the

---

[55] Peter K. Yu, *The Graduated Response*, 62 Fla. L. Rev. 1373, 1391 (2010).
[56] Yu, *supra* note 55.
[57] 2011 B.C. Intell. Prop. & Tech. F. 1.
[58] *Id.*
[59] John M. Owen, *Graduated Response Systems and the Market for Copyrighted Works*, 27 Berkeley Tech. L.J. 559, 585 (2012).

user's internet speed if the piracy continues. There are no details as to what the penalty for reaching all six warning messages will be, but many speculate it would lead to a ban from using internet through the user's current internet service provider.

Perhaps the most practical solution to online piracy has been to punish the network organizations, such as The Pirate Bay, directly under a theory of secondary liability. As mentioned above, pursuing claims against those who facilitate online piracy through establishing Bit Torrent networks is difficult because the networks themselves store no copyrighted content.[60] As such, the networks don't engage in direct copyright infringement.[61] Some courts, including in the United States, however, have begun to accept secondary liability as a means of holding parties liable for copyright infringement.[62] Essentially, secondary liability permits a finding of vicarious copyright infringement where a Bit Torrent network system is marketed for illegitimate purposes and income is derived.[63] In The Pirate Bay's case, the organization has a reputation for taunting those who pursue claims against it.[64] When Apple sent The Pirate Bay cease and desist letters ordering it to remove torrent files of Apple's programs, The Pirate Bay posted the letter and requested Apple send more, as the letters were "entertaining."[65] This kind of act would likely lend substance to a claim that the network is used for illegitimate purposes. Additionally, through the sale of banner ads on its website and contributions from users, The Pirate Bay

[60] Rona, *supra* note 5 at 33.
[61] *Id.*
[62] Burger, *supra* note 37.
[63] *Id*
[64] Ankur R. Patel, *Bittorrent Beware: Legitimizing Bittorrent Against Secondary Copyright Liability*, 10 Appalachian J.L. 117, 140 (2011).
[65] *Id.*

claimed to be making $3 million per year.[66] It seems that, by this definition, networks like The Pirate Bay would not be able to escape secondary liability if it existed in every jurisdiction.

Secondary liability isn't new, however as of now it is inconstantly applied across nations, and not applied at all in some.[67] In the United States, secondary liability exists, though its statutory basis is debated.[68] In the seminal United States secondary liability case, the court took a stance against online piracy by saying such businesses "can't take a 'see no evil, hear no evil, speak no evil' approach to the use of its product".[69] This has had the effect of removing illegal torrent sites from United States soil, although many users in the United States still access illegal torrents.[70] Similarly, in the U.K., secondary liability exists where the individual had knowledge of the copyright.[71] There, as here, if The Pirate Bay continued to operate, the cease and desist letters it so defiantly posts to its website would serve as proof of knowledge that its actions infringed copyright. In Sweden and Spain, The Pirate Bay can continue to operate today due to the lack of substantive laws pertaining to secondary liability.[72]

Due to the inconsistent, and in some cases absent application of secondary liability, online piracy can continue to thrive in all countries because of the housing of pirates in some countries. Many posit that an international treaty could ensure Bit Torrent communities are no longer safeguarded by their jurisdictions to the detriment of all internet-connected nations.[73] By

---

[66] John Malcolm, *Film Piracy and the Pirate Bay Cases*, April 13, 2010, 12 Engage: J. Federalist Soc'y Prac. Groups 25, 26 (2011).
[67] Burger, *supra* note 37, at 148-49.
[68] Burger, *supra* note 37, at 151.
[69] Asher Meir, *Grokster File-Sharing and Glue-Sniffing*, JERUSALEM POST, July 3, 2005, at 17.
[70] Burger, *supra* note 37, at 152.
[71] Lynda J. Oswald, *International Issues in Secondary Liability for Intellectual Property Rights Infringement*, 45 Am. Bus. L.J. 247, 267 (2008).
[72] Burger, *supra* note 37, at 152.
[73] Oswald, *supra* note at 280, Bright, *supra* note 27, at 289.

providing in such a treaty mandatory adoption of secondary liability, illegitimate Bit Torrent networks can be eradicated worldwide as they have been here in the United States and elsewhere.

DRONES

Aircrafts are typically thought of as requiring a pilot. Until recently, our concept of unmanned aircrafts was likely limited to remote control toy helicopters. Now, unmanned aircrafts come in all shapes and sizes, and can be used for all purposes.[74] Called "unmanned aircrafts" by the Federal Aviation Administration[75] but better known as "drones", these machines have been hard to define and regulate.[76] This is due in large part to the varying nature of their size (from the size of an insect to the size of a football field)[77] and capability (from recreational use to military use).[78] Despite this, their popularity has grown as their potential uses continue to excite, and in some cases unnerve an anxious public.[79] Domestically, the government is in the midst of modernizing the Federal Aviation Administration to account for the relative certainty that such aircrafts will populate American airspace for any number of uses.[80]

[74] Benjamin Kapnik, *Unmanned but Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, 77 J. Air L. & Com. 439, 443 (2012).
[75] *Id.* at 442.
[76] *Id.* at 443.
[77] NPR, *Popularity of Drones Takes Off For Many Countries*, July 11, 2011, http://www.npr.org/2011/07/11/137710942/popularity-of-drones-takes-off-for-many-countries (last accessed January 28, 2013).
[78] Kapnik, *supra* note 74 at 443.
[79] NPR, *supra* note 77.
[80] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331, 126 Stat. 11.

While some imagine a world where a "Tacocopter" will deliver your take-out dinner without the need for a pilot,[81] others contemplate less innocent ways drone capabilities could be exploited. The Pirate Bay has threatened to use drones to act as Low Orbit Server Stations housing the servers it uses to facilitate Bit Torrent piracy.[82] Similar to how their systems work today, these Low Orbit Server Stations would not house any actual copyrighted content, rather, act as a hub directing users around the world to where copyrighted works could be downloaded by other users via Bit Torrent files.[83] This radical idea, The Pirate Bay suggests, would allow it to avoid any particular jurisdiction, and negate the need to continuously move its servers to new locations as countries become less hospitable to its conduct.

Though certainly an innovative use of drone technology, such a system has many practical and legal obstacles that would likely prevent its success. First, Newton's Law of Gravity suggests that what goes up must come down, and as the technology stands today, this remains true for unmanned aircrafts as they require routine maintenance.[84] Second, the system as The Pirate Bay contemplates it would still require an on-land location to transmit signals and direct the aircraft via GPS.[85] Presumably this on-land location would subject the drone operators to the laws of that particular jurisdiction. The remainder of this paper will focus, however, on the

---

[81] Huffington Post, *Tacocopter Aims to Deliver Tacos Using Unmanned Drone Helicopters,* August 20, 2012, http://www.huffingtonpost.com/2012/03/23/tacocopter-startup-delivers-tacos-by-unmanned-drone-helicopter_n_1375842.html (last accessed January 28, 2013).

[82] MrSpock, *supra* note 1.

[83] US News, *The Pirate Bay to Fly 'Server Drones' to Avoid Law Enforcement*, March 19, 2012, http://www.usnews.com/news/articles/2012/03/19/the-pirate-bay-to-fly-server-drones-to-avoid-law-enforcement (last accessed January 28, 2013).

[84] Cristina Costantini, *U.S. Border Patrol Increases Use of Unmanned Drones for Surveillance*, HUFFINGTON POST, http://www.huffingtonpost.com/2012/05/01/us-border-patrol-increase_n_1467196.html (last updated May 01, 2012).

[85] MrSpock, *supra* note 1.

legal impracticality of The Pirate Bay's idea. Both domestically, and internationally, airspace is regulated very heavily. As drone technology continues to grow, so too will the bodies of law regulating airspace both locally, and abroad. It is highly unlikely The Pirate Bay will be able to find a place that welcomes drone technology for such blatant and unapologetic illegal activity.

DOMESTIC USE

Generally, individual interest in airspace is limited.[86] When an aircraft is flying relatively low, below 500 feet, the nuisance and trespass law of the jurisdiction over which it flies typically governs its use.[87] If the use and enjoyment of the land has been interfered with due to the aircraft flying through the airspace, a cause of action may exist as a property right has essentially been taken.[88] Flights above this 500-foot mark are generally thought to be in a safe zone of airspace from causing detriment to property owners.[89] If an aircraft does exceed this 500 foot level, it can become a danger to other aircrafts and therefore federal aviation regulation governs whether the aircraft is a legitimate use of the airspace, or a threat to safety.[90]

Drones, however, are subject to special rules as these aircrafts are, by definition, unmanned.[91] Since drones are able to fly above or below 500 feet constantly, the Federal Aviation Administration requires the aircrafts to be registered to ensure each drone is fit for safe

---

[86] Major Walter S. King, *The Fifth Amendment Takings Implications of Air Force Aircraft Overflights and the Air Installation Compatible Use Zone Programs*, 43 A.F. L. Rev. 197, 200 (1997)
[87] Paul Stephen Dempsey, *Local Airport Regulation: The Constitutional Tension Between Police Power, Preemption & Takings*, 11 Penn St. Envtl. L. Rev. 1, 8 (2002).
[88] Colin Cahoon, *Low Altitude Airspace: A Property Rights No-Man's Land*, 56 J. Air L. & Com. 157, 191 (1990).
[89] King, *supra* note 86.
[90] Timothy M. Ravich, *The Integration of Unmanned Aerial Vehicles into the National Airspace*, 85 N.D. L. Rev. 597, 612 (2009).
[91] *Id*.

performance.[92] Additionally, no drone may be registered for operation without having at least one person who is responsible for it, both while it is in the air and on the ground.[93] The drone must also be in constant contact with air traffic control so as to further avoid collision.[94] As for what the drone is allowed to do, the Federal Aviation Administration requires all applications for drone registration state what the intended use of the drone will be, as well as the time period during which the flight will take place.[95]

In the United States, drone technology is poised to become extremely popular. This has had the effect, however, of stoking the concerns of many Americans as to how drones will be ultimately used.[96] As such, federal aviation regulation has, to this point, been very strict on who can operate drones and for what use.[97] Some less worrisome proposed uses have been for farmers to monitor and water their crops, and for local police to investigate felonies.[98] But even these uses have many individuals pushing for a bill that would at most prevent these uses, and at least highly regulate them.[99]

All of this seems to suggest that, in the United States at least, sending a drone into orbit for the purpose of facilitating copyright infringement is a highly improbable proposition. First,

---

[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] Ravich, *supra* note 90, at 614.
[96] Ben Wolfgang, *Bill Would Clip Wings of Private Drone Use*, THE WASHINGTON TIMES, July 20, 2012, http://www.washingtontimes.com/news/2012/jul/20/congress-steps-efforts-regulate-drones/.
[97] Wolfgang, *supra* note 96.
[98] Spencer Ackerman, *Drone Boosters Say Farmers, Not Cops, are the Biggest U.S. Robot Market*, WIRED.UK.COM (Feb. 5, 2013, 3:05 PM), http://www.wired.com/dangerroom/2013/02/drone-farm/.
[99] Emily Ramshaw, *Bill Would Ban Drone Surveillance of Private Property*, THE MONITOR (February 5, 2013), http://www.themonitor.com/news/local/article_6fabaaf4-6f1a-11e2-966c-0019bb30f31a.html.

such a drone would never be granted registration, as it could not provide a legitimate purpose for its use. Second, each drone requires a person on the ground to be accountable for it. Even if the drone's true use was hidden during registration, there would have to be someone willing to be held accountable for it when its true purpose for flying became known. Lastly, a drone flying in the United States can never be hidden in otherwise empty airspace, as it must necessarily be in constant contact with Air Traffic Control. Theoretically with the laws the way they are in the United States, an individual could fly a drone around in his or her backyard without fear of detection or the need for registration. For the purposes of facilitating Internet piracy, however, the drone would have to be constantly transmitting signals online, eventually revealing its location the same way on-ground servers have in the past. If, domestically, we are concerned with allowing farmers to water their crops via drones, it is unlikely such a system as the one threatened by The Pirate Bay could ever occupy American airspace.

INTERNATIONAL USE

As is commonly the case with technology, the United States is a bit behind the times when it comes to adopting drone technology for private uses. In the U.K. for example, over 130 organizations have permission to fly drones for private use.[100] These organizations include everything from The National Grid, who uses them to inspect power lines, to Video Golf Marketing, who uses drones to make videos for golf courses, and even MBDA, a missile manufacturer for the Ministry of Defense.[101] In Australia, the process for obtaining an

[100] Nick Hopkins, *Revealed: Who Can Fly Drones in UK Airspace*, THEGUARDIAN (25 January 2013), http://www.theguardian.com/world/2013/jan/25/who-can-fly-drones-uk-airspace.
[101] *Id.*

"operator certificate", a requisite for flying a drone, requires even less.[102] If the drone is to be used for flight under 400 feet, the drone simply needs to provide a flight plan such that it is apparent the drone will not collide with any structures or power lines.[103] One such drone flies so close to the ground, it hovers above an individual as he or she runs, tracking pace and keeping track of the runner's movements.[104] Much like where the United States anticipates drones may be used domestically, Japan has already has implemented drone use for spraying and monitoring farmlands.[105]

But even these communities have been similarly unwelcome to the idea of drones as the American people. In the UK, new regulations have been proposed in order to raise the "very low bar" set on the protections of privacy in the wake of private drone use.[106] There, as in the United States, use of drones requires application with the Civil Aviation Authority, and is subject to certain requirements such as height limits and distance limits from the operator.[107] In Australia, although the requirements for an operator certificate are much looser than in the United States, operators are still required to provide a purpose for the aircraft use that is submitted for approval.[108] This undoubtedly provides a buffer for inappropriate conduct for which a drone might be engaged. Japan, unlike the aforementioned nations, has a more heavily regulated drone use policy. The only use of drones authorized by the government is for

[102] Mark Edward Peterson, *The UAV and the Current and Future Regulatory Construct for Integration into the National Airspace System*, 71 J. AIR L. & COM. 521, 584 (1964).
[103] *Id.*
[104] Tom Metcalfe, *Private Drone Aircraft: Your Eyes in the Sky*, KIDELA (Oct. 30, 2012), http://www.kidela.com/technology/private-drone-aircraft-your-eyes-in-the-sky.
[105] Peterson, *supra* note 102.
[106] The Guardian, *supra* note 100.
[107] Hopkins, *supra* note 100.
[108] Peterson, *supra* note 102.

spraying crops, and for ensuring environmental compliance in farming.[109] Although the government allows drone research to be done on its own soil,[110] the only use of drones authorized is for farming, occurring only in uncontrolled airspace.[111] In international airspace, it is equally unlikely favorable laws could be introduced or existing laws exploited by The Pirate Bay in order to facilitate internet piracy.

CONCLUSION

There is no doubt that the use of unmanned drones for legitimate purposes is expanding worldwide. Technology is such that the utility of drone technology is seemingly limitless. Ultimately, no matter where it were to fly, The Pirate Bay's contemplated drone system would still be subject to the laws governing the airspace it occupies. Unless The Pirate Bay were to advocate successfully for favorable airspace laws, or find a way to exploit existing laws, it is extremely unlikely their servers could be sent to the sky to avoid jurisdiction. The issue then remains one of international intellectual property regulation. Whether hidden in a secret mountain cave,[112] or flying over the Prime Minister's office in Stockholm, Bit Torrent networks will continue to prosper if they can benefit from forum-shopping that frees them from any secondary liability for their acts of internet piracy. A treaty must be introduced or amended in order to include a clause that provides secondary liability for those networks and organizations that perpetuate internet piracy.

---

[109] Peterson, *supra* note 102.
[110] Silicon Angle, *Japanese Firm Develops World's First Private Security Drone*, December 28, 2012, http://siliconangle.com/blog/2012/12/28/japanese-firm-develops-worlds-first-private-security-drone/ (last accessed February 6, 2013).
[111] Peterson, *supra* note 102.
[112] Ernesto, *The Pirate Bay Ship New Servers to Mountain Complex*, TORRENT FREAK (May 16, 2011), http://torrentfreak.com/the-pirate-bay-ships-new-servers-to-mountain-complex-110516/ (last visited Oct. 30, 2013).

MODEL CLAUSE FOR AN INTERNATIONAL TREATY

This model clause for an international treaty is meant to incorporate and address issues with secondary liability as noted in United States case law, the Act For Trust in the Digital Economy of France and case law derived therefrom,[113] and is largely based on Article 14 of the European E-Commerce Directive 2000/31 of the European Parliament.[114] Without a similar clause adopted by Internet connected nations, piracy advocates like The Pirate Bay will continue to operate from jurisdictions, whether on the ground or in the sky, without fear of liability.

1. Where an information network service is provided that consists of the storage of information provided by a recipient of the service, Signatory Nations shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;[115] or

---

[113] *See* Amelie Blocman, *France: Liability on the Part of Video Sharing Sites*, IRIS MERLIN*(* October 8, 2007), http://merlin.obs.coe.int/iris/2007/8/article17.en.html (last visited Oct.30, 2013).

[114] Article 14 of European E-Commerce Directive 2000/31.EC (July 17, 2003), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML (last visited Oct. 30, 2013).

[115] This additional subsection is meant to incorporate inducement liability where the provider consciously avoids obtaining knowledge or awareness of the infringing activity. *See Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005). Such direct language about the type of provider the clause is aimed at may also prevent the potential threat secondary liability poses to innovative mediums. *See* Kevin M. Lemley, *The Innovative Medium Defense: A Doctrine to Promote the Multiple Goals of Copyright in the Wake of Advancing Digital Technologies*, 110 Penn St. L. Rev. 111, 141 (2005). Additionally, this subsection may nullify a defense under subsection (1)(c) where a takedown or other such notice by the copyright holder is not practicable. *See* Seagull Haiyan Song, *How Should China Respond*

(b) the provider, through nuance or direct advertisement, does not encourage illegal activity or information, regardless of actual knowledge or awareness; or

(c) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not preclude any right to relief from the recipient of the service for infringement.[116]

4. This Article shall not affect the possibility for a court or administrative authority, in accordance with Signatory Nations' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility, for Signatory Nations, of establishing procedures governing the removal or disabling of access to information.

---

to Online Piracy of Live Sports Telecasts? A Comparative Study of Chinese Copyright Legislation to U.S. and European Legislation, 2010 Den. U. Sports & Ent. L.J. 3, 20 (2010) discussing the impracticability of takedown notices for live broadcast infringements.

[116] This additional subsection is meant to address a noted downfall of secondary liability, that the "real offender", the recipient of the service, is often cleared of liability. *See* Florence Chafiol-Chaumont, *MySpace and Dailymotion: simple storing providers held liable*, LEXOLOGY (Nov. 1, 2007), http://www.lexology.com/library/detail.aspx?g=d1581b4f-d357-429e-81a4-c4f4d0ee2350 (last accessed Oct. 30, 2013).

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 6, PAGE 193

Use of Patented Inventions after FDA Approval: How to Define the Hatch-Waxman Safe Harbor in Light of *Momenta* and *Classen*

Madeline Schiesser[*]

Abstract

This paper will discuss the apparent inconsistencies in the recent *Classen v. Biogen* and *Momenta v. Amphastar* decisions by the Court of Appeals for the Federal Circuit regarding the Hatch-Waxman Safe Harbor. Although it is well settled that the Drug Price Competition and Patent Term Restoration (Hatch-Waxman) Act permits a generic drug company to use the patented invention of another party to develop a generic drug for approval by the United States Food and Drug Administration ("FDA"), the court's recent decisions have raised a question as to whether the safe harbor may protect activity subsequent to FDA approval of the generic drug. Clarification is needed on this issue and should to be provided forthwith by the judiciary. Without judicial guidance, the institutions responsible for the development and financial support of new and generic pharmaceuticals will be plagued by both legal and business uncertainty, which will adversely affect all stakeholders, including patentees, generic drug companies, and consumers.

[*] Ms. Schiesser is a Registered Patent Agent and student at Syracuse University College of Law, Juris Doctor expected May 2014. She received her Bachelor of Science in Biological Engineering from Cornell University in 2011. Ms. Schiesser wishes to express her heartfelt appreciation for the guidance and mentorship provided by Professor Theodore M. Hagelin and Ronald A. D'Alessandro, Esq. in the pursuit of her legal education and the development of this note.

Table of Contents

Introduction 195

I. Legal Context 196

A. The Hatch-Waxman Act 196

B. Pertinent Case Law 199

II. Inconsistency within the CAFC 202

A. *Classen v. Biogen* 202

B. *Momenta v. Amphastar*. 204

C. Post-FDA Approval Controversy 206

III. Judiciary Should Resolve Scope of the Safe Harbor 208

IV. Where the Safe Harbor Boundary Should Reside 211

V. Impact of Inconsistent Interpretations of the Law 215

Conclusion 217

Introduction

As is well established, it is an act of infringement to make, use, offer to sell, sell, or import a patented invention without the permission of a patent owner.[1] However, the U.S. Patent Act makes a specific experimental use exception under the Hatch-Waxman Act for uses related to developing generic pharmaceuticals and devices for approval before the United States Food and Drug Administration (FDA).[2] This experimental use exception, known as the Hatch-Waxman safe harbor, allows generic pharmaceutical companies to prepare otherwise infringing material for an Abbreviated New Drug Application ("ANDA") before the FDA. Moreover, it is understood that activity in which the generic company engages to gain approval is not considered infringement.

However, two recent and seemingly contradictory cases before the Court of Appeals for the Federal Circuit ("CAFC") have called into question the extent of this safe harbor: *Classen v. Biogen* (decided August 31, 2011) and *Momenta v. Amphastar* (decided August 3, 2012). In the former, activities conducted after FDA market approval did not receive safe harbor protection.[3] Yet, in the latter, such protection was granted to activities having specific bearing on sales after approval.[4]

This paper will begin with a background of the Hatch-Waxman Act in order to explain the purpose and intent of the law. Recent litigation concerning pertinent cases will then be examined in order to explore how the courts have addressed the Hatch-Waxman safe harbor. The controversy within the CAFC will then be discussed in more detail in order to provide a better understanding of the issue at hand. This paper will then discuss the urgent need for the

[1] 35 U.S.C. § 271(a) (2010).
[2] 35 U.S.C. § 271(e) (2010).
[3] *Classen Immunotherapies v. Biogen IDEC*, 659 F.3d 1057 (Fed. Cir. 2011).
[4] *Momenta Pharm. v. Amphastar Pharm.*, 686 F.3d 1348 (Fed. Cir. 2012).

CAFC or Supreme Court of the United States ("Supreme Court") to resolve this issue, and proffer some suggestions for what the scope of the safe harbor should be. Finally, effects of the current ambiguity of the safe harbor boundaries will be discussed.

I. Legal Context

In this section, the Hatch-Waxman Act and pertinent cases will be discussed in order to provide background so as to better understand the issues behind the controversy within the CAFC. While there is case law precedent for expanding the original reading of the Hatch-Waxman Act, courts that have expanded the Act have consistently done so by further interpreting the existing Act.

A. The Hatch-Waxman Act

The 1984 Hatch-Waxman (Drug Price Competition and Patent Term Restoration) Act was created to address several problems existent at that time with the patent and FDA processes.[5] During that period, the term of a patent was 17 years from the date of issue, but a patent owner could not begin to sell a patented pharmaceutical until after receiving FDA approval, generally after the patent had issued. Such FDA approval took years, sometimes consuming as much as half of the patent term. This left patent owners with relatively short patent terms in which to maximize commercial sales of a new drug before generic companies would have an opportunity to enter the market when the patent term expired.[6] On the other hand, generic companies desired to begin sales of a generic equivalent of the patented pharmaceutical as soon as possible after the

[5] BRUCE D. ABRAMSON, THE SECRET CIRCUIT: THE LITTLE KNOWN COURT WHERE THE RULES OF THE INFORMATION AGE UNFOLD 184 (Rowman and Littlefield Publishers 2007).
[6] Abramson, *supra* note 5, at 183.

patent term expired.[7] To do this, they too would need FDA approval, which required substantial clinical trial testing, therefore necessitating the use of the patented pharmaceutical: an act of infringement.[8]

The Hatch-Waxman Act offered succor to both patent owners and generic companies. The Act returned to patentees some of the patent term lost during the FDA approval process, thereby extending the patent term for a period beyond the original 17 years for patentees who had not received the benefit of the beginning of their patent term.[9] The Hatch-Waxman Act furthermore created the Abbreviated New Drug Application ("ANDA"), which allowed generic drug companies to substitute safety and efficiency testing from the patentee's application into their ANDA if the generic companies could show "bioequivalence."[10] This decreased the material necessary for a generic company to submit to receive approval, as compared to that of an original drug company under a New Drug Application ("NDA"), thereby streamlining the process.

Most notably, the Act allowed the generic company to make and use the patented product in order to show the requisite "bioequivalence" without constituting patent infringement, under what is known as the Hatch-Waxman safe harbor, codified under 35 U.S.C. §271(e).[11] Therefore, the generic company could begin the ANDA before the patentee's patent had expired and be ready to receive FDA approval and roll out generic equivalents of a just-expired patented pharmaceutical shortly after the expiration of the patent.

---

[7] *Id.* at 183.
[8] *Id.*
[9] *Id.* at 184.
[10] *Id.*
[11] Abramson, *supra* note 5, at 184; 35 U.S.C. § 271(e) (2013).

However, under the Act, the very deed of submitting an ANDA could nevertheless trigger patent infringement litigation. When submitting an ANDA reading on patented subject matter, the generic applicant had to acknowledge the existence of the patent, but had two options as to how to proceed.[12] Under one option, the generic applicant could acknowledge that the patent(s) would expire and wait until that expiration date to receive FDA approval.[13] Alternatively, the generic applicant could claim that the patent was invalid or would not be infringed (and provide a detailed statement of the factual basis for this assertion) and request immediate FDA approval.[14] The latter was known as a Paragraph IV proceeding, and invited the patentee to bring an infringement suit within forty-five days of receiving notification of the generic applicant's assertion.[15] If no suit was brought, the applicant could potentially receive immediate FDA approval.[16] If a suit was initiated, the FDA could not approve the generic product for thirty months, or until the generic applicant had successfully defended himself, whichever occurred first.[17]

The Hatch-Waxman Act also impacts the average American consumer because it dictates the interactions of the FDA with generic drug companies and sets the stage for infringement suits between patentees and generic companies. These events in turn determine when generic equivalents of pharmaceuticals may enter the market, the access to which increases healthcare options and decreases healthcare costs.

---

[12] Kenneth J. Burchfiel, *Biotechnology and the Federal Circuit,* 778 (2nd ed. 2010).
[13] *Id.;* 21 U.S.C. § 355(j)(2)(A)(vii).
[14] Burchfiel, *supra* note 12, at 778-79.
[15] *Id.* at 779.
[16] *Id.*
[17] *Paragraph Four Explained*, ParagraphFour.com, (2012) http://www.paragraphfour.com/explained/process.html (last visited Dec. 21, 2012).

B. Pertinent Case Law

In the most pertinent Supreme Court cases, the Court has shown a willingness to expand the boundaries of the safe harbor. However, the Court has also been mindful of the intent of the Hatch-Waxman Act. It has also shown caution and not expanded the bounds of the safe harbor so far as to obliterate the Act's goals of lengthening a patentee's valuable patent term and streamlining the lab-to-FDA approval process through which generic companies must go. With this in mind, a brief discussion of the three most related Supreme Court and CAFC cases on the Hatch-Waxman Act is in order.

In 1990, the Court ruled on the case of *Eli Lilly v. Medtronic*. Originally, it had been assumed that the Hatch-Waxman Act only applied to pharmaceuticals submitted to the FDA for approval. However, the Supreme Court found that the safe harbor protection against infringement actions was granted against the "patented invention."[18] There was therefore no provision limiting submissions before the FDA to just pharmaceuticals. Therefore, in *Eli Lilly*, the Court widened the material covered by the safe harbor to also include medical devices.[19]

More recently, the Supreme Court heard *Merck KGAA v. Integra Lifesciences* in 2005. The Court was tasked with determining whether experimental activity that was never used in an ANDA could still fall within the safe harbor provision.[20] Specifically, the Court looked at pre-clinical test results, which if not found to be within the safe harbor would constitute infringing activity.[21] Reasoning that pre-clinical testing is reasonably related to the development and submission of information under the applicable federal laws governing the regulation of drugs,

[18] *Eli Lilly & Co. v. Medtronic*, 496 U.S. 661, 665 (1990).
[19] *Eli Lilly*, 496 U.S. at 665.
[20] *Merck KGaA v. Integra Lifesciences I*, 545 U.S. 193, 195 (2005).
[21] *Id.*

the court ruled that pre-clinical testing is included in the protections of the Hatch-Waxman Act.[22] This even included pre-clinical testing that does not lead to an FDA submission. The Court recognized that at the time of pre-clinical testing, it is not foreseeable whether current and future testing results will be sufficiently successful to warrant an FDA application.[23]

The *Merck* decision led to controversy among patentees, scholars, and the scientific community, however. While a liberal interpretation of the Hatch-Waxman Act enabled pharmaceutical companies to conduct pioneering research in an inexpensive manner, a benefit which was ultimately passed on the consumer, concern about how far the scope of "reasonably related" went was expressed.[24] For example, if patentees could not protect the research tools and methods used in the laboratory and manufacturing stages to create a patented pharmaceutical from being appropriated by competitor generic companies and used to make bioequivalent drugs, then the incentive to patent these tools would be lost.[25] Instead, patentees would keep their research tools to the best of their abilities as trade secrets, effectively stifling development and technological growth.[26]

The CAFC offered some guidance on this matter two years later in *Proveris v. Innovasystems* when a panel of judges took the surprising turn of limiting the extent of the safe harbor.[27] The case asked the CAFC to look at the alleged infringements of a patented drug delivery device system, described as an accessory item to the drug for which FDA approval was

[22] *Id.* at 206.
[23] *Id.* at 207.
[24] Jonathan McPherson, *The Impact of the Hatch-Waxman Act's Safe Harbor Provision on Biomedical Research Tools after Merck KGaA v. Integra Lifesciences I, LTD,* 10 MICH. ST. U. J. MED. & L. 369 (Spr. 2006).
[25] *Id.*
[26] *Id.*
[27] Proveris Scientific v. Innovasystems, 536 F.3d 1256 (Fed. Cir. 2008).

being sought on an ANDA.[28] The court reasoned that the ability to receive a patent term adjustment went hand in hand with the scope of the Hatch-Waxman safe harbor.[29] Consequently, because the drug delivery device system was not eligible for a patent term adjustment, declaring its use within the bounds of the safe harbor in association with the preparation of an application for submission before the FDA was also not appropriate.[30] The Court did not address whether the patented drug delivery device system, or other research tools, would be considered "reasonably related" to the development and submission of information to the FDA.[31]

After *Proveris*, patentees, scholars, and the scientific community again reacted to the shifting perception of the law. One deficiency identified in the ruling was an inability to protect research tools that had not been labeled as research tools by the FDA.[32] It was also suggested that the CAFC's decision was influenced by the conduct of the alleged infringer, who did not merely make the device for its own use, but instead for sale to pharmaceutical companies.[33] Another criticism is that the CAFC may have narrowed the definition of "patented invention" as the Supreme Court had defined it in *Merck*. In the earlier case, the Supreme Court defined "patented invention" broadly under § 271(e)(1) to "include all inventions, not drug-related inventions alone."[34] However, in *Proveris*, the CAFC appeared to be tailoring that definition to only those inventions requiring FDA approval, thereby narrowing potential candidates for inclusion in the safe harbor.[35]

---

[28] *Id.* at 1258.
[29] *Id.* at 1263.
[30] *Id.*
[31] *Proveris Scientific*, 536 F.3d at 1260.
[32] Adam Sibley, *The FDA safe Harbor Provision After Proveris*, 21 SYRACUSE SCI. & TECH. L. REP. 36, 38 (Fall 2009).
[33] *Id.* at 42.
[34] *Id.* at 45.
[35] *Id.* at 46.

Recognizing that broad definitions of research tools may be under or over inclusive, particularly in light of multiple uses of such tools, scholars have also suggested a case-by-case analysis by courts in order to determine whether unauthorized use of an invention would constitute a safe harbor exemption to infringement.[36]

II. Inconsistency within the CAFC

Although the Supreme Court and CAFC have held that the Hatch-Waxman safe harbor protects experimental activity prior to and related to applications for FDA approval, the CAFC's position on post-approval activity is far less clear. There is a need to define where the safe harbor boundary stops between experimental use and infringement in the marketplace.

A. ***Classen v. Biogen***

In 2011, a panel of judges on the CAFC heard the case of *Classen Immunotherapies v. Biogen IDEC*.[37] Although the case was primarily concerned with the patent eligibility of claims containing a mental step under 35 U.S.C. §101, the court also discussed whether experimental activity performed after market approval by the FDA could receive Hatch-Waxman safe harbor protection.[38] The claims in the litigation involved mental steps, sometimes coupled with an act; the court, for reasons outside of the scope of this paper, held some of the claims valid and infringed, and others invalid.[39]

---

[36] Chenwei Wang, *In search of the Boundary of the Safe Harbor,* 19 FED. CIRCUIT B.J. 617, 627 (2010).
[37] *Classen*, *supra* note 3.
[38] *Id.* and Jason Rantanen, *Classen Immunotherapies v. Biogen: The Broad, Broad Scope of Statutory Subject Matter*, Patentlyo (August 31, 2011), http://www.patentlyo.com/patent/2011/08/classen-immunotherapies-v-biogen-the-broad-broad-scope-of-statutory-subject-matter.html (last visited Dec. 21, 2012).
[39] Rantanen, *supra* note 38.

However, as to the Hatch-Waxman Act, the Court firmly found, in an opinion written by Judge Newman and joined by Chief Judge Rader, that the Hatch-Waxman safe harbor only applied to pre-market experimental activity.[40] To support its findings, the court cited to the legislative history of the Hatch-Waxman Act to discern that the purpose of the safe harbor is only to protect activity in preparation of seeking FDA approval.[41] Specifically, the court cited to the House Report associated with the legislation, which stated that it is not an act of patent infringement "for a generic drug maker to import or to test a patented drug in preparation for seeking FDA approval if marketing the drug would occur after expiration of the patent."[42] The court further emphasized from the legislative history that the information that can be developed under the Hatch-Waxman Act is "the type which is required to obtain approval of the drug."[43] The CAFC interpreted the Supreme Court's earlier *Eli Lilly* and *Merck* decisions as strictly applying to pre-clinical research where there is "a reasonable basis for believing that the experiments will produce "the types of information that are relevant to an IND [investigational new drug application] or NDA [new drug application].' "[44] Judges Newman and Chief Judge Rader firmly asserted that the Hatch-Waxman safe harbor would not and could not apply to activities taking place after market approval by the FDA.

Judge Moore dissented, however, and advanced a theory that Hatch-Waxman safe harbor did not merely apply to pre-approval activity.[45] In her dissent, Judge Moore took particular note of the discussion of 35 U.S.C. §271(e) in *Merck* in which the Court stated that "the statutory text

---

[40] *Classen*, *supra* note 3, at 1070.
[41] *Id.*
[42] *Classen*, *supra* note 3, at 1071, quoting H.R. Rep. No. 98-857, pt. 1, at 15, 1984 U.S.C.C.A.N. 2647, 2648 (1984).
[43] *Classen*, *supra* note 3, at 1071 (quoting H.R. REP. No. 98-857, pt. 1, at 45 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 2647, 2678.
[44] *Classen*, *supra* note 3, at 1072 (quoting *Merck, supra* note 20).
[45] *Classen*, *supra* note 3, at 1083 (Moore, dissenting).

makes clear that it provides a wide berth for the use of patented drugs in activities related to the federal regulatory process" and that the §271(e) exemption "extends to all uses of patented inventions that are reasonably related to the development and submission of any information under the FDCA [Food, Drug, and Cosmetic Act]."[46] Judge Moore argued that any activity, regardless of research stage, may be eligible for protection under the Hatch-Waxman safe harbor if reasonably related to submitting any information before the FDCA, including information regarding post-approval uses.[47]

B. *Momenta v. Amphastar*

Only a year later, a slightly different panel of judges: Judge Dyk, Judge Moore and Chief Judge Rader, heard *Momenta Pharmaceuticals v. Amphastar Pharmaceuticals*. The difference of one judge led to startlingly different conclusion in the *Momenta* case as compared with *Classen* with respect to the Hatch-Waxman safe harbor. After Amphastar received its FDA approval in Autumn 2011, Momenta, holder of method patents for manufacturing processes of a generic version of the low molecular weight heparin Lovenox, or enoxaparin, promptly brought a patent infringement lawsuit against Amphastar.[48]

Although Momenta was not the patentee of the original enoxaparin pharmaceutical, the patent for which had been held by Sanofi-Aventis, Momenta holds method patents on methods of making enoxaparin and was the first generic drug company to successfully receive FDA approval for a generic version of enoxaparin.[49] In its complaint, Momenta specifically alleged

---

[46] *Classen*, *supra* note 3, at 1083 (quoting *Merck*, *supra* note 20).
[47] *Classen*, *supra* note 3, at 1083.
[48] *Momenta, Sandoz file patent suit against Amphastar and Watson over Enoxaparin Sodium Injection*, NEWS-MEDICAL (Sept. 23, 2011) http://www.news-medical.net/news/20110923/Momenta-Sandoz-file-patent-suit-against-Amphastar-and-Watson-over-Enoxaparin-Sodium-Injection.aspx.
[49] *Momenta*, *supra* note 4, at 1351.

infringement of Momenta patents 7,790,466 and 7,575,886 on methods of making and analyzing generic enoxaparin.[50] Momenta believed that Amphastar had used Momenta's methods in order to prepare enoxaparin samples for testing in preparation for bringing the drug to market after Amphastar had received FDA approval for a generic version of enoxaparin.[51]Amphastar, however, argued that its post-approval testing fell with the scope of the Hatch-Waxman safe harbor.[52]

Initially, the District Court of Massachusetts granted Momenta a preliminary injunction, stopping the sales of Amphastar's generic enoxaparin. However, Amphastar appealed to the CAFC, whose majority viewed the injunction skeptically.[53] The CAFC vacated and remanded the injunction to the district court, with strict language discouraging the injunction.[54] The CAFC stated that as the party seeking the injunction, Momenta bore the burden of establishing that it was entitled to the "extraordinary relief" of the injunction, and had failed to meet this burden.[55]

Defending its activities, Amphastar asserted that its actions fell within the Hatch-Waxman safe harbor, a defense originally rejected by the District Court.[56] However, the CAFC majority agreed with Amphastar, taking a broad interpretation to the activities covered within the safe harbor. In an opinion written by Judge Moore, largely consistent with her dissent in *Classen*, the court found that the safe harbor could include post-FDA-approval activities, because the Hatch-Waxman statute did not specify under what Federal laws information need be

[50] *Momenta, Sandoz file patent suit*, *supra* note 48.
[51] *Momenta, supra* note 4, at 1352.
[52] *Id.*
[53] Kevin E. Noonan, *Momenta Pharmaceuticals, Inc. v. Amphastar Pharmaceuticals, Inc. (Fed. Cir. 2012),* PATENT DOCS (Aug. 9, 2012), http://www.patentdocs.org/2012/08/momenta-pharmaceuticals-inc-v-amphastar-pharmaceuticals-inc-fed-cir-2012.html (last visited Dec. 20 2012).
[54] Noonan, *supra* note 53.
[55] Noonan, *supra* note 53.
[56] *Id.*

submitted, and as such, activity need not be limited to that required for FDA approval.[57] Accordingly, the CAFC ruled that Amphastar's use of Momenta's processes, although after FDA approval, was within the bounds of the Hatch-Waxman safe harbor.[58] Therefore, Amphastar's defense was valid.[59]

Chief Judge Rader took great umbrage with the court's decision and in his dissent argued that the court had failed to follow its own precedent from *Classen*, creating substantial inconsistency within the circuit.[60] He argued that because Momenta's patented processes had been used to test Amphastar's samples for the market after Amphastar's FDA approval, Amphastar's activity should not fall into the Hatch-Waxman safe harbor.[61]

Following the decision of the CAFC panel, Momenta petitioned the Supreme Court of the United States for *writ of certiorari*, but the petition was denied in June 2013.[62] In a related case, in light of outcomes in the Amphastar litigation, Momenta also failed in July 2013 to assert its '886 patent against Teva Pharmaceuticals USA.[63]

C. Post FDA Approval Controversy

Between the CAFC's decisions in *Classen* and *Momenta*, an inconsistency has presented itself concerning what activity is protected within the bounds of the Hatch-Waxman safe harbor. Judge Newman, joined by Chief Judge Rader, held in *Classen* that activity conducted after FDA

---

[57] *Momenta*, 659 F.3d at 1355.
[58] Noonan, *supra* note 53.
[59] *Id.*
[60] Eric W. Guttag, *Momenta Pharmaceuticals: The Hatch-Waxman "Safe Harbor" Widens to Include Post-FDA Approval Activity*, IP WATCHDOG (Aug. 7, 2012, 10:27 am), http://www.ipwatchdog.com/2012/08/07/momenta-pharmaceuticals-the-hatch-waxman-safe-harbor-widens-to-include-post-fda-approval-activity/id=27191/ (last visited Dec. 20, 2012).
[61] *Momenta Pharm., Inc. v. Amphastar Pharm., Inc.*, 686 F.3d at 1362 (Rader, C.J., dissenting).
[62] *Momenta Pharm., Inc. v. Amphastar Pharm., Inc.*, 133 S.Ct. 2854 (2013).
[63] *Momenta Pharm., Inc. v. Teva Pharm. USA, Inc.*, 2013 WL 3893417, *2 (Mass. Dist. Ct. July 19, 2013).

market approval is clearly not within the safe harbor. However, Judge Moore, joined by Judge Dyk, was of the opinion in *Momenta* that activity is within the bounds of the safe harbor if the activity is reasonably related to the development and submission of information before the FDA, regardless of whether that activity is conducted before and as part of the FDA approval process, or even after approval.

When presented with a judicial framework which does not have an FDA approval cut-off for activity within the safe harbor, it is further unclear when activity ceases to be reasonably related to submissions before the FDA. For example, would activity necessary to meet certain federal formalities be reasonably related? Would activity conducted prior to FDA approval but having little bearing on the approval process be considered reasonably related? Under the current *Momenta* decision, district courts now not only have contradictory instructions, but also have only vague guidelines for how to address potentially infringing activity.

Furthermore, as Chief Judge Rader argued in his dissent in *Momenta*, the majority failed to appreciate that the language of 35 U.S.C. §271(e)(1) contains the limitation "solely," which limits the purpose of the activities that can be admitted into the safe harbor.[64] Under the Chief Judge's construction, an activity that has another purpose, such as marketing, and is not "solely for uses reasonably related to the development and submission of information under a Federal law," does not qualify under the safe harbor.[65]

---

[64] *Momenta Pharm., Inc. v. Amphastar Pharm., Inc.*, 686 F.3d at 1374 (Rader, C.J., dissenting).
[65] 35 U.S.C. § 271(e)(1) (2010); *Momenta Pharm., Inc. v. Amphastar Pharm., Inc.*, 686 F.3d at 1374 (Rader, C.J., dissenting).

III. Judiciary Should Resolve Scope of the Safe Harbor

In September 2012, Momenta petitioned for a rehearing *en banc* in part to resolve the inconsistencies that the court had seemingly created in the Hatch-Waxman safe harbor law.[66] Classen Immunotherapies filed an *amicus curiae* brief in support of the petition because Classen also wished to see the law resolved.[67] Classen had petitioned the Supreme Court on the issue, but was denied *certiorari* and the case was not heard.[68] Classen was also concerned that until the coverage of the Hatch-Waxman safe harbor was resolved, its ability to litigate its patents would be negatively impacted.[69] Momenta and Classen are correct; there is a need for resolution of this matter.

The CAFC should accept the petition from Momenta to rehear the case *en banc* in order to provide a more definitive resolution of the question as to what activity is covered within the Hatch-Waxman safe harbor. If, for some reason, the court refuses to rehear *Momenta en banc*, a need will still exist for the law to be settled in this area. Accordingly, if the CAFC does not agree to hear *Momenta*, the court should nonetheless agree to hear a similar case *en banc* to resolve this matter.

However, given the importance of this issue, a timely resolution of the apparent inconsistency in the Hatch-Waxman safe harbor law is needed. Given that *Momenta* presents a clean issue that if resolved either for or against widening the Hatch-Waxman safe harbor would present a clear precedent for future cases in the lower courts, the *Momenta* case would be an

---

[66] Petition for Rehearing En Banc, Momenta Pharm., Inc. v. Amphastar Pharm., Inc., 686 F.3d 1348 (2012) (No. 2012-1062), 2012 WL 4662298.
[67] Brief of Amicus Curiae Classen Immunotherapies, Inc. in Support of the Petition for Rehearing En Banc, Momenta v. Amphastar, 686 F.3d 1348 (2012) (No. 2012-1062) 2012 WL 4762489.
[68] *Id.*
[69] Brief of Amicus Curiae Classen Immunotherapies, *supra* note 67.

appropriate vehicle for an *en banc* rehearing. Moreover, since similar cases are likely to be seen in increasing numbers in district courts going forward, there is a need for this issue to be resolved forthwith.

In view of the 2-1 split decisions in the *Momenta* and *Classen* cases, this issue is ripe to be heard by the full panel CAFC judges. Between the two cases, it appears that Judge Newman and Chief Judge Rader favor an exclusively pre-approval based interpretation of the Hatch-Waxman safe harbor, which is derived from legislative intent.[70] Contrastingly, Judge Dyk and Judge Moore have advocated for a "reasonably related to approval" interpretation. This interpretation of the Hatch-Waxman safe harbor is based on a textual approach.[71] The opinions of the other sitting judges are as of yet unknown with respect to this matter. Accordingly, given the apparent deadlock in opinion, now would be an appropriate time for the full panel to weigh-in on this matter.

Moreover, a full bench opinion would also sufficiently crystalize the issue were it to appear before the Supreme Court as a second petition in *Momenta* or embodied in a separate case. Although parties can appeal directly to the Supreme Court from a panel decision by the CAFC, as can be inferred by the Supreme Court's denial of *certiorari* in *Momenta*, the Supreme Court is unlikely to accept appeals that have not first been reviewed by the full panel, but may be persuaded to do so after a full review. The CAFC is also itself more likely to accept cases for an *en banc* hearing where the panel originally hearing the matter was split.

Although currently the Supreme Court has denied Momenta *certiorari* and the CAFC has remained further silent, continued action before the CAFC and the Supreme Court is urged. The issue of whether post-FDA approval activity constitutes infringement, a question which has

[70] *Classen, supra* note 3; *Momenta, supra* note 4, (Rader, dissenting).
[71] *Classen, supra* note 3 (Moore, dissenting); *Momenta, supra* note 4.

profound implications for the pharmaceutical industry, is of sufficient importance that a full bench hearing before the CAFC is warranted to clarify this issue. Additionally, if further clarification remains necessary, the Supreme Court should then grant *certiorari* to timely resolve this matter.

How the Supreme Court would decide an appeal from *Momenta* would be another question. The *Eli Lilly* and *Merck* decisions suggest deference for a broad interpretation of the Hatch-Waxman safe harbor. Even so, the Supreme Court never showed an interest hearing *Proveris* or granting *certiorari* on a similar case, which would suggest that the Supreme Court favors certain limits on the extent of the safe harbor. Certainly, the Supreme Court has an interest in fostering innovation and protecting the property rights of patentees; it also desires to assist the interests of the health care system by removing obstacles in the path of generic pharmaceutical companies as they move their products to market. However, with regard to patent cases, the Supreme Court has rendered surprising decisions at times.

Alternatively, the Legislative Branch could also provide guidance as to what exceptions to infringement the Hatch-Waxman safe harbor should provide to generic pharmaceutical companies. Even though the Patent Act has recently undergone major revisions in the form of the America Invents Act (AIA), no changes were made to infringement statute 35 U.S.C. §271.[72] It is unclear whether the lack of changes to the Hatch-Waxman safe harbor exception in the AIA is intended as a tacit concurrence on the present wording of the law, or a mere oversight by Congress to address the need for specific rules in this area governing where the infringement line resides. However, technical amendments are still being made to the AIA and will most likely continue to be made for some time into the future as courts and the U.S. Patent and Trademark

[72] 35 U.S.C. § 271 (2013).

Office adjust to the new law. Accordingly, there is still time for legislators to offer resolution. In fact, Senator Hatch and Representative Waxman should both be sufficiently concerned by the unraveling of the legislation they sponsored to be motivated to enact measures clarifying the intent of the Act, thereby making further judicial intervention unnecessary.

IV. Where the Safe Harbor Boundary Should Reside

The CAFC should establish a boundary for the safe harbor so as to protect experimental work prior to FDA approval, while excluding from protection all activity conducted thereafter that is necessary for FDA approval. This arrangement would protect companies and other entities interested in developing generic pharmaceuticals, while simultaneously protecting the market interests of patentees during the terms of their patents.

Entities that experiment with a patented pharmaceutical need to be able to do so without fear of a patent infringement suit. Such entities should include prospective generic drug companies, as well as universities that are merely interested in studying the operation of the pharmaceutical, but which are most likely not interested in direct commercialization. Under *Merck*, even preliminary experimentation that may never lead to an ANDA is protected within the Hatch-Waxman safe harbor, so long as there is a reasonable expectation that such experimentation could lead to an ANDA.[73] However, under *Proveris*, research tools are specifically excluded from the safe harbor.[74] This allows a patentee of the tool to receive the full benefit of the patent term and creates an incentive to develop such tools without fear that they will be appropriated by others for "experimental use." With this foundational case law, there

[73] *Mereck KGaA v. Integra Lifesciences I, Ltd*., 545 U.S. 193, 195 92005).*supra* note 20.
[74] *Proveris Scientific Corp. v. Innovasystems,* Inc., 536 F. 3d 1256 (Fed. Cir. 2008).

appears to be a directive from the courts to sponsor research and innovation. This directive would be frustrated if the infringement status of post-FDA approval activity is not made clear.

Accordingly, the CAFC should establish precedent so that the Hatch-Waxman safe harbor does not touch upon any activity conducted subsequent to activities necessary for FDA approval. As Chief Judge Rader explained in his dissent in *Momenta*, when legislators wrote the Hatch-Waxman Act, their purpose was to resolve inadequacies in the old law: seemingly truncated patent terms for patentees and a tedious FDA approval process for generic companies that could only begin after the expiration of the original patent.[75] It was never the legislators' intent to give generic companies entrance into a patentee's market while a patent was still in force.

Allowing a generic company to reach beyond FDA approval and engage in subsequent activities constitutes a taking for which the government provides tacit approval. Even if a generic company did not being selling a FDA approved product until after the patent has expired, the generic company would still have received a substantial head start on bringing the generic to market. After receiving FDA approval for a new drug or product, the original patentee must blaze the path of the drug to the marketplace. Considerable resources, including capital and time from the patent term, are devoted to determining best manufacturing processes, making inroads with distributers, and advertising the new drug to healthcare professionals and the general public. The patentee must work to garner the reputation of the new drug, carve out a market, and determine lucrative off label uses for the drug. Evidently, there is significant lead time between FDA approval and actual market entry. While this time will be shorter for a generic company

[75] *Momenta Pharms. Inc. v. Amphastar Pharms, Inc.*, 686 F. 3d 1348, 1364 (Fed. Cir. 2012) (Rader, R., dissenting); Abramson, *supra* note 5, at 184.

that has the advantage of the patentee's drug's reputation, it should not be non-existent. If a generic company is permitted to engage in post-approval activities such as manufacturing while the patent is still in force, it bypasses this lead time, which is an unjust taking from the patentee.

As Chief Judge Rader indicated in his dissent, quoting from the legislative history:

> The purpose of 271(e)(1) and (2) is to establish that **experimentation** with a patented drug product, when the purpose is to prepare for commercial activity which will begin after a valid patent expires, is not a patent infringement. Since the Committee's Subcommittee on Health and the Environment began consideration of this bill, the Court of Appeals for the Federal Circuit held that this type of **experimentation** is infringement. In Roche Products, Inc. v. Bolar Pharmaceutical Co., [] the Court of Appeals for the Federal Circuit held that the **experimental use** of a drug product prior to the expiration date of a patent claiming that drug product constitutes patent infringement, even though **the only purpose of the experiments is to seek FDA approval** for the commercial sale of the drug after the patent expires. It is the Committee's view that **experimental activity** does not have any adverse economic impact on the patent owner's exclusivity during the life of a patent, but prevention of such activity would extend the patent owner's commercial exclusivity beyond the patent expiration date.[76]

Chief Judge Rader further indicated from the legislative history:

> Section 202 [of the bill] does not authorize any activity which would deprive the patent owner of the sale of a single tablet during the life of a valid patent. In fact, the limited testing activity required to obtain FDA approval of a generic drug would not normally result in the use of even a single generic tablet for its therapeutic purpose during the life of a valid patent.[77]

As the Chief Judge indicated from the legislative history, the legislators understood at the time the Hatch-Waxman Act was being put together that the safe harbor would be carving out some

---

[76] *Momenta Pharms. Inc. v. Amphastar Pharms, Inc.*, 686 F. 3d 1348, 1364 (Fed. Cir. 2012)(Rader, R., dissenting);(quoting H.R.Rep. No. 98–857, pt. 1, at 45–46 (1984), *reprinted in* 1984 U.S.C.C.A.N. 2647, 2678–2679 (emphases added).

[77] *Momenta Pharms. Inc.*, 686 F.3d at 1364 (Rader, R., dissenting) (quoting *Innovation and Patent Law Reform: Hearing on H.R. 3605 Before the Subcomm. On Courts, Civil Liberties and the Admin. Of Justice of the H. Comm. On the Judiciary*, 98th Cong. 926 (1984) (memorandum of Alfred B. Engelberg, Patent Counsel, Generic Pharmaceutical Industry Association) (emphasis added)).

very specific exceptions for experimentation to seek FDA approval for commercial sales after patent expiration. It was never their intent to grant generic companies the ability to build upon a patentee's successful market development while the patentee still held a patent, thereby siphoning sales from the patentee.

Chief Judge Rader also took particular issue with the failure of the majority in *Momenta* to address the phrase "*solely* for uses reasonably related to the development and submission of information under a Federal law which regulates the manufacture, use, or sale of drugs or veterinary biological products" (emphasis added).[78] The Chief Judge found the word "solely" to be key. Under Rader's construction of the phrase, activity must be "solely" for development and submission before the FDA. Further development, such as that leading to the market, is impermissible under this statute.[79] This results in a narrower amount of information which may be protected within the safe harbor. It is a long held principle that it is necessary to consider all terms when construing a statute. It appears that the CAFC panel majority failed to give adequate weight to the term "solely" and therefore construed the Hatch-Waxman safe harbor too broadly.

Momenta also brought to the forefront the need to address the process patent protection within the Hatch-Waxman safe harbor. If a generic company is permitted to use a process after FDA approval in order to make a product ready for market in such a way that the patented invention has been used, then under traditional construction, patent infringement has occurred. Yet, the majority in *Momenta* believed this is not the case and would effectively permit such activity to continue for the full term of the patent. Patented processes are certainly statutory subject matter under the Patent Act to the same extent as patented compounds, and should

[78] *Momenta Pharms. Inc.*, 686 F.3d at 1374 (Rader, R., dissenting); 35 U.S.C.A. § 271(e)(1) (2010).
[79] *Momenta Pharms. Inc.*, 686 F.3d at 1374 (Rader, R., dissenting).

therefore be afforded the same degree of protection and recognition under the Hatch-Waxman Act.[80]

However, while a literal interpretation of the Hatch-Waxman Act may indeed suggest that any activity required by a federal law should fall under the safe harbor, as was suggested by the majority in *Momenta*, this would open the safe harbor to potential abuses. As federal regulations govern and require many acts, even those far removed from the manufacture, use, or sale of drugs, it would become increasingly unclear which post-FDA approval activities were within the safe harbor and which were not. Therefore, the safe harbor must be construed to *solely* include pre-FDA approval activities within the scope of the harbor, as is consistent with the intent of the drafter and how the Act has been interpreted up until this point in time.

V. Impact of Inconsistent Interpretations of the Law

As provided in the U.S. Constitution, Congress has the power "To promote the progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Rights to their Writings and Discoveries."[81] Accordingly, the term of a patent grant is meant to run for only a limited period of time. The current state of the law is contradictory to this, as it does not give patentees the full term to which they are entitled and creates uncertainty such that generic companies may be deterred from entering the market. It was certainly not the intent of 35 U.S.C. § 271(e)(1) to curtail a patent grant to a patentee once a generic company had achieved FDA approval.[82] Such increased uncertainty in the law is detrimental to all stakeholders involved.

---

[80] 35 U.S.C. § 101.
[81] U.S. Constitution, Art. I, Section 8, ¶8.
[82] *Momenta Pharms. Inc.*, 686 F.3d at 1374 (Rader, R., dissenting).

Under pre-*Momenta* interpretations of the Hatch-Waxman safe harbor, patentees had a high degree of certainty that their patent monopoly would end only when their patent expired, and that their market monopoly would subsequently come to an end when a generic competitor achieved FDA approval.[83] If the generic competitor has already completed the requirements for FDA approval during the patent term, the patentee would be aware of this, and could prepare itself for market loss once its patent expires.[84] However, under *Momenta's* interpretation of the Hatch-Waxman safe harbor, it is far less clear what activities the generic competitor can engage in while the patent is still in force. For example, this may allow the competitor to potentially break into the patentee's market during the patent term. Consequently, patentees will not have a clear understanding of when their patent monopolies will effectively expire or what activities constitute infringement of that monopoly. This increased uncertainty trickles into other areas, including business uncertainty, because the inability to assess a patent can have dire consequences in terms of lost revenue.[85] By contrast, corporations that hold patents and their shareholders desire to minimize risk and shift capital to fields where the law and patent rights are less uncertain.[86]

Generic companies are also at a disadvantage by not having a clear understanding of what activities are and are not permissible under the Hatch-Waxman Act. Preparing to bring a generic drug to market requires resources, including funding, preparation of manufacturing facilities, and

[83] Abramson, *supra* note 5, at 184.
[84] Abramson, *supra* note 5, at 184.
[85] Roger D. Blair and Thomas F. Cotter, *Rethinking Patent Damages*, 10 TEX. INTELL. PROP. L.J. 1, 7-9 (Fall 2001).
[86] Douglas O. Edwards, *An Unfortunate "Tail": Reconsidering Risk Management Incentives After the Financial Crisis of 2007-2009*, 81 U. COLO. L. REV. 247, 247 (Winter 2010).

clinical testing mandated by the FDA.[87] If any of these activities may be construed as an infringement, investors and shareholders may not be willing to assume the heightened risk that such uncertainty creates. Moreover, as a drug patent nears the end of its term, there is often more than one generic company circling around the patented invention. If some generic companies develop the patented pharmaceutical significantly past the point of FDA approval whereas others do not, it will provide an unfair advantage to some companies when the patent expires and generic companies are clearly free to enter the market.

Furthermore, consumers and the healthcare system face a twofold disadvantage. First, prices are likely to be higher from companies insulating themselves from business uncertainty in the wake of a poorly understood Hatch-Waxman safe harbor.[88] Second, the availability and variety of generic products requiring FDA approval are likely to be reduced through less willing competition on the market due to the greater potential for infringement suits and deterioration of patent rights.[89]

Conclusion

The Patent Act grants for a limited time to a patentee a right to exclude all others from an invention, with specific exceptions. One of those exceptions is the Hatch-Waxman safe harbor, which allows for experimental use prior to and as a part of the submissions process before the FDA under 35 U.S.C. § 271(e)(1). However, differing opinions have arisen among the judges of the CAFC as to the extent of the safe harbor as it pertains to post-approval activities. There is a

[87] *How to Market Your Device*, FDA, http://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/default.htm (last updated Sept. 25, 2013).
[88] Eric L. Talley, *On Uncertainty, Ambiguity, and Contractual Conditions,* 34 DEL. J. CORP. L. 755, 760 (2009).
[89] Edwards, *supra* note 86; Abramson, *supra* note 5, at 184.

considerable need to know among patentees, generic drug companies, and the medical industry in general what post FDA approval activities constitute infringement. The willingness of capital markets to provide financial support to bring new drugs to market and very shape of the patentee-generic relationship are at stake.

The balance struck by the Hatch-Waxman (Drug Price Competition and Patent Term Restoration) Act should be maintained. Patentees should receive the full benefit of their patent term with a minimum of interference from competitor generic companies. Conversely, once that patent term has expired *and only* once that patent term has expired, generic drug companies should be able to take full advantage of the freedom opened up by the lack of patent restriction. However, generic companies should not be able to interfere in the patentee's market while the patent is still in force or attempt to gain a comparative advantage with respect to other generic companies. Such conduct is a disincentive to the market and impacts all parties involved, including consumers. Likewise, such conduct discourages innovation and the creation of new pharmaceuticals. The original intent of the Hatch-Waxman Act must be respected.

SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 29 FALL 2013 ARTICLE 7, PAGE 219

Legally Poisoned: How the Law Puts Us at Risk from Toxicants

By Carl F. Cranor

Citation: CARL F. CRANOR, LEGALLY POISONED: HOW THE LAW PUTS US AT RISK FROM TOXICANTS (Harvard University Press, 2011).

Reviewed by: Alessandra Baldini

Relevant Legal and Academic Areas: Environmental Pollutants; Environmental Policy and Law; Public Health Policy and Law.

Introduction

In Legally Poisoned, Cranor lays out the frightening details of chemical proliferation in our modern world. In this well-researched work, the author makes clear the extent to which we are exposed to chemical toxicants, and the danger of this exposure to our health. Cranor clearly illustrates the process by which we are "legally poisoned," as the title says: the regulatory regime of the nation is one that assumes safety in all of the thousands of chemicals we encounter daily. It is only when harmful effects are shown after the fact that the government steps in to reduce or eliminate the use of a chemical. No effort is made to protect our citizens until some portion are injured.

Nowhere to Hide

Commercial chemicals invade our everyday lives.[1] For instance, "if you are sitting on your couch as you read this, the cushions likely contain brominated fire retardants:

[1] CARL F. CRANOR, LEGALLY POISONED: HOW THE LAW PUTS US AT RISK FROM TOXICANTS, 16 (Harvard University Press, 2011).

polybrominated diphenyl ethers, or PBDEs."[2] With time, PBDEs can be found in the floor, air, red meat, chicken, electronics, and your lungs.[3] Perchlorate, another commercial chemical used in rocket fuel and fireworks, can be found in tap water, or even California Imperial Valley lettuce.[4] Perchlorates can "interfere with thyroid production, which developing children need for proper neurological growth and function."[5]

Dichlorodiphenyltrichloroethane, or DDT, is a banned sprayed pesticide used over fifty years ago.[6] Women who were alive during this spraying have a five times greater risk for breast cancer.[7] Polychlorinated biphenyls, or PCBs, are currently banned from commerce; however, they are still present in our bodies.[8] Although PCBs can be found in meat and fish, vegetarians can also be exposed if they live near chemical disposal sites.[9] People living in Northern Canada and the United States usually have lower exposure levels than those living in the lower 48 states.[10]

All of these compounds are identified toxicants that are "probable human carcinogens, substances that can adversely affect the development of children, reproductive toxicants, and neurological toxicants."[11] These compounds can be very concerning and there are few ways to impede their entry into our bodies – "some products may directly contaminate us; others invade

---

[2] *Id.*
[3] CRANOR, *supra* note 1, at 16.
[4] *Id.*
[5] *Id.*
[6] *Id.*, at 16-17.
[7] *Id.* at 17.
[8] CRANOR, *supra* note 1, at 17.
[9] *Id.*
[10] *Id.*
[11] *Id.*

more insidiously during routine living, as secondary contaminants from poorly disposed products or wastes."[12]

"Exposure" is an ambiguous term that "may merely mean that a toxicant has come into 'contact' with a person's body."[13] A "body burden" is "the amount of substance that can be measured in a person's tissues or fluids by biomonitoring."[14] "Exposure," as used in this book, refers to external bodily contacts, whereas "body burden" refers to an internal exposure.[15] Typically, we are not aware of our daily exposures to contaminants; although we can be aware of "smoke, pesticide spray, air pollution, or brackish water or see mercury 'beads' on surfaces, . . . we [can]not detect harmful molecular components of the exposures."[16]

Even if we are aware of exposure, we can still become contaminated, with toxicants found in our "tissues, organs, blood, and urine."[17] However, due to increases in technology, we are now able to monitor the amounts of toxicants in our bodies through biomonitoring techniques.[18] As the Centers for Disease Control and Prevention ("CDC") indicates, "biomonitoring permits determination of people's exposure to toxic substances in the environment 'by measuring levels of chemicals that actually are in people's bodies,' as detected in blood or urine."[19] Biomonitoring allows us to know the exact measure of contamination, which allows researchers to forgo the traditional method of estimation.[20]

---

[12] CRANOR, *supra* note 1, at 18.
[13] *Id.*
[14] *Id.* at 19.
[15] *See id.*
[16] *Id.*
[17] CRANOR, *supra* note 1, at 19.
[18] *Id.* at 20.
[19] CRANOR, *supra* note 1, at 20.
[20] *Id.*

With the advent of biomonitoring, scientists were also more able to determine how long a toxicant survives in our bodies.[21] Now, "scientists [] know that many of [the industrial chemicals] can be in our bodies for hours, days, weeks, years, or sometimes decades. The measure of the longevity of toxicants is their 'half-life,' the period of time it takes for one-half the amount of a substance in our bodies to leave."[22] However, even if a toxicant has a short half-life, we may be constantly exposed to it, allowing it to remain in our bodies nearly permanently.[23] Substances with longer half-lives may indicate prior exposures rather than ongoing.[24]

Biomonitoring has led scientists to believe that "our bodies contain varying levels of hundreds of industrial chemicals, many of which are known or suspected toxicants."[25] As of 2009, the CDC was able to reliably identify 212 toxicants in our bodies.[26] These toxicants were identified through the use of "exposure markers."[27] A Canadian study tested body burdens among a wide variety of geographically different Canadians.[28] Although it was a small sample, the report concludes, "[n]o matter where people live, how old they are or what they do for a living, they are contaminated with measureable levels of chemicals that can cause cancer and respiratory problems, disrupt hormones, and affect reproduction and neurological development."[29] However, older participants had higher levels of PCBs than younger ones,

[21] *Id.* at 21.
[22] *Id.*
[23] *Id.*
[24] CRANOR, *supra* note 1, at 21.
[25] *Id.*
[26] *Id.*
[27] *Id.* at 22.
[28] *Id.*
[29] CRANOR, *supra* note 1, at 22.

which likely means that exposure rates are decreasing as we create better ways to prevent PCBs in the environment.[30]

In another small study performed by the NBC program Dateline, two families were tested for individual contaminants.[31] One family was vegetarian, ate mostly organic food products, and used "natural" cleaning products; the other family was "a more typical American family … [who] ate considerable amounts of eggs, cheese, sirloin steak, turkey, and many 'convenience' foods because of their schedules," and chose cleaning products based on their effectiveness rather than toxicity.[32] "Both families were tested for seventy-six industrial chemicals in their bodies… [the first family] had forty-two, and the [second family] had forty-three."[33] However, the second family had "three times as many perfluorinated compounds" as the first family.[34] The second family's children also had "more phthalates than 76 percent of the people tested in the United States."[35] On the other hand, the first family had greater levels of bisphenol A ("BPA"), whereas the second family's BPA levels were hardly detectable; due to a greater consumption of canned foods consisting mostly of refried beans, it appears that the first family ingested BPA from the can linings.[36] Since BPA is "quickly eliminated from the body," its presence suggests continuous exposure.[37]

At any given time, we are likely contaminated by hundreds of toxicants.[38] These and other studies suggest that there is little that we can do to avoid this exposure, and eating organic

---

[30] *Id.*
[31] *Id.* at 23.
[32] *Id.*
[33] *Id.*
[34] CRANOR, *supra* note 1, at 23.
[35] *Id.*
[36] CRANOR, *supra* note 1, at 23-24.
[37] *Id.* at 24.
[38] *Id.*

foods is not as effective as we may believe.[39] Apart from living in the Arctic Circle, there may be "systematic approaches" we can partake in to decrease our exposure levels.[40] For instance, the United States banned PCBs in the 1970s and the amounts of this compound have since been substantially lower.[41]

Discovering Disease, Dysfunction, and Death by Molecules

As aforementioned, industrial compounds have invaded our bodies, and we have hundreds of toxicants present on any given day.[42] However, some of these toxicants can cause harm, or even kill us "directly and quickly."[43] For instance, arsenic in high doses can kill quickly; in low doses, it will kill slowly.[44] Further, arsenic exposure during fetal development "can contribute to lung, skin, urinary, and bladder cancers long after arsenic has left a person's body."[45]

Exposure early in life to diethylstilbestrol ("DES") or DDT may increase a woman's "risk of breast cancer."[46] It has taken scientists "forty to fifty years to identify first vaginal cancer and then breast cancer in women exposed to DES in utero."[47] However, there may be difficulties in identifying sources of diseases, and it could take "years to separate normal variation in mental functioning from the acceleration of dementia in old age caused by pesticides or other neurotoxicants."[48] Studies can lead to false senses of security – for instance, "When we

[39] *Id.*
[40] *Id.*
[41] CRANOR, *supra* note 1, at 24.
[42] *Id.*
[43] CRANOR, *supra* note 1, at 47.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.* at 48.
[48] CRANOR, *supra* note 1, at 48..

are told that 'no human studies have shown that substance X poses risks to humans,' we may feel there is nothing to worry about, yet this is hardly the whole story."[49]

For example, an international group of scientists critiqued a study by IBM, which determined whether there were cancer risks in electronics plants.[50] They stated that since the study was "too small to detect cancer risks in electronics plants," IBM cited "the negative results, not as inconclusive, but as showing safety."[51] However, "a later researcher with access to the IBM data from a legal case found elevated risks of cancer among employees."[52] Such studies that result in "no effect" claims should be heeded with caution – "not all studies are conscientiously conducted; some are designed to minimize, not to discover, or even to hide adverse outcomes."[53]

Studies may not always be in the best interest of the consumer – "companies whose products may be threatened by scientific findings have commercial incentives to demand unreasonably high degrees of certainty, multiple studies, and 'proof' of risks or harm before the public can be protected."[54] Since studies take time to design and perform, are costly, and require independent confirmation of the results, we may not be adequately protected, as "no public health protections can be implemented until appropriate studies have been conducted."[55] Cranor suggests implementing "premarket testing laws" and policies to address this issue – "research would begin earlier on products and would be publicly available to a wider community [which

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] CRANOR, *supra* note 1, at 48.
[53] *Id.* at 49.
[54] *Id.*
[55] *Id.*

would] both increase[] the chance[] of identifying hazards before exposures and provide[] other scientists data to follow up and the opportunity to possibly discover more subtle risks."[56]

Caveat Parens: A Nation at Risk from Contaminants

Within the last forty years, scientists have evolved from prior ideas regarding the safety of a fetus. Previously, "the scientific community viewed a woman's womb as a sheltered, capsule-like environment, safe from the intrusions and dangers of the outside world."[57] Due the misconception that a woman's body served as a safe-haven for a developing fetus, women continued with their regular habits: "a pre-dinner cocktail, one or two glasses of wine with dinner – because her developing child was tucked safely inside her."[58] A pregnant woman could continue to smoke, drink, and use industrial chemicals because her baby was presumably safe inside.[59] However, this safe-haven notion quickly changed during the 1960s and 1970s, when "children born to women exposed to methylmercury in fish and to the pharmaceutical thalidomide raised the early alarms."[60]

From 1953 to 1968, "a Japanese petrochemical company disposed of about twenty-seven tons of methylmercury ("MeHg") in Minimata Bay, Japan."[61] As fish were exposed and became contaminated, MeHg entered our food chain.[62] MeHg has a half-life of about seventy to eighty days; therefore, humans who ingested the contaminated fish "developed neurological problems [such as] numbness and loss of feeling, some suffered ataxia, some had tunnel vision, some went

[56] *Id.*
[57] CRANOR, *supra* note 1, at 81.
[58] *Id.*
[59] *Id.*
[60] *Id.* at 82.
[61] *Id.*
[62] CRANOR, *supra* note 1, at 83.

blind," and others became permanently disabled or died.[63] Developing children were more susceptible to this toxicant "because of the way MeHg behaves biologically" –MeHg is actively transported through the placenta to the fetus, which led to "concentrations of MeHg [] at least five times greater in the fetal brain than in the mother's blood."[64] Many of the exposed children were born with "severe cerebral palsy at a much higher rate than unexposed children … [and] psychomotor retardation, blindness, deafness, and seizures."[65]

Thalidomide was a pharmaceutical sedative that was first sold in 1958 and marketed as "a strong sedative that was also remarkably safe … a drug that was almost as powerful as a barbiturate but with no noticeable side effects."[66] However, it was later discovered that side effects existed: "peripheral neuropathy (poisoning of the nerves) which created a 'tingling sensation and a feeling of numbness or cold' that could progress to 'cramps, weakness and loss of strength."[67] While these side effects were reversible, it was later discovered that more side effects existed for pregnant women.[68] Mothers who took thalidomide during pregnancy bore children who developed "phocomelia – meaning 'seal limbs' … [or lacked the] long bones in the arms and legs, which meant that the hands and feet or just the fingers and toes of the infants sprang directly from the trunk … it was also common for the baby to be born with no bowel opening, no ear openings, and segmented intestines."[69]

Exposure to thalidomide was more dangerous "twenty to thirty-six days following conception," which is when women often began feeling the symptoms of morning sickness, and

---

[63] *Id.*
[64] CRANOR, *supra* note 1, at 83.
[65] *Id.* at 84.
[66] *Id.*
[67] *Id.*
[68] *Id.* at 84-85.
[69] CRANOR, *supra* note 1, at 85.

asked for a sedative.[70] Pregnant women only needed to take the drug once for the side effects to occur.[71] Further, "[t]he disease or dysfunction rate among children born to mothers who took the drug was two hundred times the background rate of similar birth defects in nonexposed children."[72] Conservative estimates place the number of thalidomide babies in the seven to eight thousand range, with about five to seven thousand dying before birth.[73]

While thalidomide caused physical deformities at birth, methylmercury could cause less visible issues. However, both the catastrophes of methylmercury and thalidomide broke the notion that a woman's fetus was a "safe-haven" for developing fetuses.[74]

A More Prudent Approach to Toxic Invasions

With the dangers clearly presented, Cranor's work moves on to the weak regulations that currently govern the introduction of new chemicals into our environment. He moves on to suggest a number of ways in which our situation could be improved. Cranor draws from practical sources to draft his suggestions, and steers clear of any stifling regulatory burdens.

Premarket testing is the primary means to promote public safety with regards to the introduction of new chemicals.[75] As Cranor notes, pharmaceuticals, pesticides, and food additives are required to undergo testing before introduction to the market.[76] Cranor poses a reasonable question: why does this not apply to industrial and commercial chemicals?[77] The FDA dictates that new pharmaceuticals must undergo animal testing in order to provide for the

[70] CRANOR, *supra* note 1, at 85.
[71] *Id.*
[72] *Id.* at 85-86.
[73] *Id.* at 86.
[74] *Id.*
[75] CRANOR, *supra* note 1, at 178-79.
[76] *Id.* at 179.
[77] *See id.* at 178.

safety of the participants in required human trials[78] – an impressive dedication to human safety. The EPA regulates the testing of new pesticides by requiring pesticides, when used according to instructions, to pose no health risk to humans and only an acceptable risk to the environment.[79] Markedly, EPA regulations pay special attention to infants and children, a subpopulation at particular risk of complications arising from exposure to toxicants.[80]

With regards to human testing, there is legal precedent on tort actions. For instance, in 1978, there was a class-action suit for battery against researchers from the University of Chicago, "who, during 1950-1952, gave women diethylstilbestrol (DES) in a double-blind experiment as part of their prenatal care at the university's Lying-In Hospital."[81] These women were unaware that they were participating in research and did not consent to ingesting DES, which at the time was not known to be harmful but was later found to cause miscarriages.[82] As such, the district court found for the plaintiffs, stating that in a battery, "the actor must intend to cause the other, directly or indirectly, to come in contact with a foreign substance in a manner which the other will reasonably regard as offensive …Thus one need not be aware at the time of exposure to a foreign substance in order to regard it as offensive."[83] Cranor therefore analogizes, "manufacturers of industrial chemicals, who are substantially certain that their substances will come into contact with citizens in a manner that recipients could reasonably regard as offensive, could be subject to a battery action."[84]

---

[78] *Id.* at 179.
[79] *Id.* at 180.
[80] *Id.*
[81] *Id.* at 182.
[82] CRANOR, *supra* note 1, at 182-83.
[83] CRANOR, *supra* note 1, at 183.
[84] *Id.*

In addition, the intentional tort of trespass is applicable to toxicants.[85] Trespass can include "the deposition of molecules and particles, including gases, particulates, and lead on property."[86] Here, Cranor illustrates trespass with a hypothetical situation, stating:

> "Suppose you dispose of some trichloroethylene (TCE) from home experiments into my hot tub without permission. TCE is a probable human carcinogen and likely neurotoxicant, but diluting small amounts in a hot tub reduces any risk of harm…You did not actually harm or even pose a risk of harm to anyone exposed to it. But your TCE invaded, or trespassed on, my hot tub and my bodily integrity without my consent or license."[87]

Cranor further illustrates trespass by chemical companies on individuals' properties, stating "[s]hould not such invasions [by chemical companies] also require permission and justification by one who would cause the foreign substance to invade, just as trespasses on chemical company property requires permission and justification?"[88]

With the legal precedent clear on the topic of exposing others to known toxicants, as well as the clarity of regulations regarding testing of new pharmaceuticals, pesticides, and food additives, there is a strong case to be made for a reform of the regulations regarding industrial chemicals.[89] Industrial chemicals are definitely analogous to pesticides.[90] Cranor makes the argument that to protect citizens from illegal trespass and battery, as well as to show an equal

---

[85] *See id.* at 184.
[86] *Id.*
[87] CRANOR, *supra* note 1, at 185.
[88] *Id*. at 186 (footnote omitted).
[89] *See* CRANOR, *supra* note 1, at 187.
[90] *See id.*

concern to the public as to the test subjects, industrial chemicals should be subject to premarket testing.[91]

What Kind of World do We Want to Create?

In the book's concluding chapter, Cranor discusses where we, as a society, may proceed as we move forward in a world with evermore chemicals being introduced into our environment.[92] It is clear from the weight of the evidence in the rest of the book leading up to this point that there is only one reasonable direction to go, according to Cranor. That direction is toward premarket testing for all chemicals and potential toxicants with greater protection and respect for citizens.[93] With such scientific assessment, both of synergistic effects and risk to sensitive subpopulations, quality of life would be improved for everyone.[94] Such policies would reduce the harmful effects of negative externalities and help to reduce healthcare costs to consumers and the taxpayer.[95]

This book provides a comprehensive analysis of the ethical, legal, and regulatory issues facing the wide-scale use of untested chemicals. The weight of the data supports Cranor's well-reasoned arguments, which he uses to effectively push for increased responsibility and increased safety for all members of society.

[91] *See id.* at 192-207.
[92] *See id.*, at 208-09.
[93] *See id.* at 209.
[94] *See* CRANOR, *supra* note 1, at 218.
[95] *See* CRANOR, *supra* note 1, at 244-48.