HNBA JOURNAL OF LAW AND POLICY

HNBA/MICROSOFT INTELLECTUAL PROPERTY LAW INSTITUTE EDITION

ROBERT T. MALDONADO
EDITOR-IN-CHIEF

JORGE F. GONZALEZ
ASSISTANT EDITOR

FALL 2017

TABLE OF CONTENTS

Forewords 7

by Circuit Judge Jimmie V. Reyna and Catherine C.A. Romero

The EU Convention on Cybercrime:
Analyzing Nontraditional Crimes Utilizing Various
Jurisdictional Principals of International Law 11

by Wendy Onofre

Can One Infringe an Invalid Patent?
The Blindside of Patent Arbitration 33

by Luiz Miranda

Who's the Patent Troll? 47

by Edwin Garcia

Patents, Food Science, and Veganism 67

by Kimberly Pflug-Rodriguez

Demystifying the Algorithm in Employment
Hiring Disparate Impact Cases 77

by Crystal Araujo

Acknowledgments 96

THE IPLI

by Circuit Judge Jimmie V. Reyna

U.S. Court of Appeals for the Federal Circuit

The Hispanic National Bar Association/Microsoft Intellectual Property Law Institute ("IPLI") is unique. My experience is that most diversity programs ultimately venture into the realm of mentoring. The apparent idea is that mere exposure to an attorney of color will motivate a student to seek a career in the legal profession. The IPLI is different. The IPLI works to improve the grades of its law students, the Scholars, by improving their writing and presentation skills. The goal is to place them well on the road to become excellent practitioners and members of the bar.

This special edition of the HNBA Journal of the Law and Policy ("HJLP") is another step on that road by creating opportunities for Scholars to publish IP law related articles. This is not easy work. Each year, the Institute involves leaders in IP related U.S. governmental institutions, law firms that sign up as Fellows and commit to work with the Scholars over the course of a year, IP practitioners, and HNBA leadership. Three HNBA members merit specific mention for their leadership and work: Catherine Romero of Microsoft; Jennifer Trusso Salinas, partner with Troutman Sanders; and Mick Konowal of Microsoft. Mick has been the gravitating force in the planning and administration of each IPLI. To everyone involved, I doff my hat.

FOREWORD

by Catherine C. A. Romero

Five years ago, with the help of Circuit Judge Jimmie V. Reyna, a small team of lawyers from the Hispanic National Bar Association and Microsoft started the HNBA/Microsoft Intellectual Property Law Institute (IPLI). We had clear goals that we wanted to achieve with this program:

(1) increase the pipeline of Hispanic law students entering the field of intellectual property law;

(2) provide mentors and support to our student "Scholars" through law school;

(3) improve our Scholars' presentation and legal writing skills; and

(4) help our Scholars secure employment in the intellectual property field after graduation.

We knew that the third aim would provide the foundation that our Scholars would need to succeed in the legal profession.

Good writing and presentation skills present a challenge for many of our Scholars, for some of whom English is a second language. Other Scholars learned English at an early age but grew up in a family or community that does not speak or write English well, or at all. Many Scholars are the first in their family to go to college, let alone finish high school, and there isn't anyone at home to help with legal writing and presentation questions.

With these challenges in mind, Judge Reyna suggested a couple of years ago, that we publish a special edition of the HNBA Journal of Law and Policy. This edition would be reserved for our IPLI Scholars so that they could write articles on intellectual property and technology law, and submit them for publication consideration. At the five-year anniversary of the IPLI, we were ready to add this Journal Edition to our program.

I am so very proud of the five authors in this Journal Edition. These Scholars are the trailblazers that jumped at the opportunity to write articles on short notice; and worked diligently on many rounds of edits with law firm attorneys, Microsoft attorneys, HNBA attorneys, and the Journal's Editors. Some of these authors even studied and took their bar exam while finishing their articles!

Many of our Scholars received input and assistance from our law firm "Fellows," who partner with the IPLI to provide support and mentors for Scholars during the IPLI and throughout their law school careers. Our mentors provide advice on writing, presentations, resumes, and contacts for obtaining employment. I would like to thank our Fellows and the mentors for their commitment to our IPLI program.

Some of our mentors were part of the hardworking Editorial Staff, who spent time with Scholars on the phone to go over their comments and suggestions in detail, sometimes for two or three rounds. We also had IPLI alums, who are now superstar attorneys, on our Editorial Staff; as well as HNBA members who volunteered their time. I would like to give a big "Thank You!" to our wonderful Editorial Staff.

A huge "Thank You!" goes to our Editors, Robert and Jorge, for the significant commitment they made to review every article in detail and provide additional comments. I also want to thank them for the time they spent on the phone with me planning, mapping the timeline status, and reviewing all the details that go into putting out a publication. I am happy to report that they still answer my calls.

I'd like to thank the HNBA Leadership and past presidents Judge Peter M. Reyes, Miguel Alexander Pozo, Cynthia D. Mares, Robert T. Maldonado, and Pedro J. Torres-Diaz for their partnership in this IPLI endeavor. I'd like to recognize the awesome HNBA team of Alba Cruz-Hacker, Erika Lopez-Tello, Michelle Avelino, and Darcy Tharp who take care of a ton of IPLI logistics and details. I so appreciate the commitment President-Elect Jennifer Trusso Salinas has made to the IPLI over the past five years. In addition to the mentorship she provides to our Scholars, Jennifer has stayed up many nights to read applications multiple times and help me with the painful task of whittling a big list down to a class of 25. Thank You, Jennifer!

I would like to acknowledge and thank my employer, Microsoft Corporation, who has supported the IPLI financially and with many other resources since the beginning. I especially want to thank my colleague, Mick Konowal, who has put endless hours into making the IPLI a success. Thank You, Mick!

This Journal Edition was the brainchild of Judge Reyna. He is the gentle force that has nudged us in the right direction throughout our IPLI Program. Judge Reyna knew that it was important for our Scholars to go through the process of writing an article for publication. It is this dedication that makes our Scholars better writers and more equipped for their future careers in the legal profession, and it is this Journal Edition that allows our Scholars the opportunity to publish nationally in the capacity of true legal intellectuals. Thank you, Judge Reyna, for your guidance and your continued support of the IPLI and our Scholars.

The EU Convention on Cybercrime: Analyzing Nontraditional Crimes Utilizing Various Jurisdictional Principles of International Law

WENDY ONOFRE

Chicago-Kent College of Law | April 2017

This article was written in April of 2017, since then several instances of cybercrimes have occurred at the global level. Most notably, in June of 2017, and as reported by CNN[1]*, several global firms were targets of a malware attack that infected and locked computers.* To unlock the computers, targets *were ordered to pay $300 in Bitcoins. U.S. based Mondelez, FedEx, and British advertising agency WPP were among the global firms that were targeted. The origin of this malware is not yet known, but incidents like this highlight the continued importance of creating international cybercrime laws and adequate jurisdictional agreements.*

[1] Selena Larson and Jethro Mullen, *Global Cyber Attack: What You Need to Know,* CNN.com (June, 28, 2017). http://money.cnn.com/2017/06/28/technology/ransomware-attack-petya-what-you-need-to-know/index.html

ARTICLE TABLE OF CONTENTS

Introduction 14
I. Overview of the EU Convention on Cybercrime 14
a. Entry into Force 15
b. The Convention on Cybercrime Deals with Electronic Versions of Existing Crimes 15
c. Legislative Standards Under the Cybercrime Convention 16
d. Mutual Assistance Under the Convention on Cybercrime 17
e. Extradition Under the Convention on Cybercrime 17
f. Jurisdiction Pursuant to the Convention 18
II. Cybercrime 18
a. When a Crime is not a "Crime" 20
i. State Failure to Implement Cybercrime Laws 20
ii. Crimes Against Morality – Freedom of Speech vs. National sovereignty 21
iii. When Nothing is Taken – Distributed Denial of Services 22
III. Introduction to Principles of International Law 24
a. Nationality Principle 24
b. Territorial Principle 24
c. Protective Principle 25
d. Universality Principle 25
e. Passive Personality Principle 25
IV. EU Convention on Cybercrime and the Various Principles of International Law 25
a. Nationality Principle 26
b. Territorial Principle 27
c. Protective Principle 27
d. Universality Principle 28
e. Passive Personality Principle 28
V. Conclusion 28
Bibliography 29

Introduction

According to the International Telecommunication Union (ITU), an estimated 18% of the world was connected to the internet in 2005.[2] The ITU's 2016 report shows a dramatic increase in internet penetration, with a current global rate of 47%.[3] Technology giants like Facebook[4], Google[5], and Space X[6] are on a mission to provide free internet access to the world. Internet usage is unlikely to decrease in the years to come. Therefore, nations must address the legal uncertainties presented by the internet.

Cyberspace transcends traditional national geographic boundaries. Nations around the world are currently grappling with the notion of cybercrime and the laws that ought to be applied in this regard. In 2001, the Council of Europe adopted the European Union's Convention on Cybercrime.[7] Entering into force in 2004,[8] the EU Convention on Cybercrime[9] is the only Treaty addressing transnational issues relating to cybercrime[10].

This article addresses the main provisions of the EU Convention on Cybercrime. It provides a case study on recent cybercrimes to illustrate the various scenarios in which cybercrimes have occurred. Next, it presents a brief introduction to core principles of international law and analyzes the Convention against these international principles. This article ultimately concludes that the nontraditional nature of cybercrimes renders the Convention inadequate unless the Convention revises its jurisdictional basis. Revisions ought to include specific instances when the protective, universal, and passive principles of jurisdiction can be employed.

I. Overview of the EU Convention on Cybercrime

The Convention on Cybercrime ("COC") establishes "a common criminal policy aimed at the protection of society against cybercrime, among other things, by adopting appropriate legislation and

---

[2] International Telecommunications Union, *Facts and Figures* (2005). http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2005.pdf

[3] International Telecommunications Union, *Facts and Figures* (2016). http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

[4] Jessi Hempel, *Inside Facebook's Ambitious Plan to Connect the Whole World,* Wired.com (Jan. 19, 2016). https://www.wired.com/2016/01/facebook-zuckerberg-internet-org/

[5] Jon Russell, *Google Expands its Initiative to Provide Free Wi-Fi Hotspots in Emerging Markets,* TechCrunch.com (Sept. 27, 2016). https://techcrunch.com/2016/09/27/google-station-free-wifi-hotspots/

[6] Samuel Gibbs, *Elon Musk Wants to Cover the World with Internet Space,* The Guardian (Nov. 17, 2016). https://www.theguardian.com/technology/2016/nov/17/elon-musk-satellites-internet-spacex

[7] Convention on Cybercrime (Nov. 23, 2011), ETS NO. 185. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[8] *Id.*

[9] *Id.*

[10] Congressional Research Service, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, No. R42547.

fostering international co-operation."[11] The Convention is governed by the European Convention on Human Rights ("ECHR")[12] and consists of five major categories[13]: (1) illegal interception of and/or interference with computer data, illegal access to and/or interference with computer systems, and the misuse of devices to commit any of these offenses;[14] (2) Computer-related forgery and fraud[15]; (3) child pornography[16]; (4) infringement of copyright and related rights[17]; and (5) provisions governing the imposition of aiding and abetting and corporate liability.[18]

a. Entry into Force

Fifty-four (54) countries, or Parties, have signed the COC.[19] It entered into force in 2004 and is currently enforced in 52 countries.[20] Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States are among the non-Council of Europe members who have ratified the Convention.[21] Brazil, India, and Russia have notably declined to adopt.[22]

b. The Convention on Cybercrime Deals with Electronic Versions of Existing Crimes

Chapter 1, Article 1 of the COC defines computer system[23], computer data[24], service provider[25], and traffic data.[26] "Cybercrime" is not a defined term; instead, the COC utilizes the word "cybercrime" to refer to electronic versions of existing property crimes.[27] For example, the COC provisions make electronic trespass a cybercrime.[28] The illegal interception provision is an electronic invasion of privacy/burglary offense from unauthorized intrusions that results in appropriation of "property" in the form of data.[29]

---

[11] Convention on Cybercrime (Nov. 23, 2011), ETS No. 185 [hereinafter *COC*].

[12] *Id.*

[13] *Id.*

[14] Explanatory Report, *Convention on Cybercrime,* ETS No. 185, P 35 (Nov. 8, 2011) [hereinafter *Explanatory Report]*.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Council of Europe, Committee of Experts on Crime in Cyber-space, *Final Activity Report* (May 25, 2001) at Chapter 1 – P 33 [hereinafter *Final Activity Report*].

[19] Convention on Cybercrimes, *Chart of Signatures and Ratifications of Treaty 185*, ETS No. 185. (Last updated April 7, 2017) [hereinafter *Signatures and Ratifications*].

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *COC, supra* n. 10, at C.1, Art. 1.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Explanatory Report, supra* n. 13, at 44.

[29] *Id.* at 51-58.

The provisions outlawing computer-related forgery and fraud,[30] copyright infringement,[31] and aiding and abetting[32] also deal with electronic versions of traditional property crimes which incorporate computer technology as a tool for committing the crimes.

Child pornography is the only non-property crime addressed by the COC.[33] Child pornography is recognized as a crime by most countries.[34] The drafters of the COC included the child pornography provision in an effort to modernize laws that address "the ever-increasing use of the Internet as the primary instrument for trading such material."[35] The COC does not have any provisions regarding new cybercrimes, discussed below, nor does it establish procedures to expand the definition of cybercrime.[36]

c. Legislative Standards Under the Cybercrime Convention

The Treaty requires Parties to establish "effective, proportionate and dissuasive criminal . . . sanctions"[37] for the commission of the specified offenses. Most provisions in the Treaty require Parties to take legislative measures "as may be necessary to establish criminal offenses."[38] The COC's vague standard on adequate legislative measures allows for liberal interpretations that vary from country to country.[39]

The standard for legislative action becomes unclear in certain provisions. For example, Article 20, regarding Real-time collection of traffic data, compels service providers to provide assistance in the collection of relevant evidence "within its existing technical capability."[40] The Treaty imposes no sanctions for failure to comply.[41] Interest-based scholars believe the omission is unlikely to change state behavior; without these sanctions, there are no material consequences for

---

[30] *Id.* at 86-90.

[31] *Oracle USA, Inc. v. Rimini St. Inc.,* 2014 U.S. Dist. LEXIS 148519 at 5 (D. Nev. Oct. 14, 2014) (No meaningful distinction between "theft" and "copyright infringement" in the Ninth Circuit)

[32] Model Penal Code Section 5.01(3) ("A person who engages in conduct designed to aid another to commit crime . . . is guilty of an attempt to commit the crime, although the crime is not committed or attempted by such other person . . ."). Therefore, aiding-and-abetting in the commission of the cybercrimes as described by the COC constitutes theft of electronic property.

[33] *COC, supra* n. 10, at C.2, Art.9.

[34] *Id.*

[35] *Explanatory Report, supra* n. 13, at 93.

[36] *COC, supra* n. 10.

[37] *Final Activity Report,* supra n. 13, at Art. 13.

[38] *COC, supra* n. 10.

[39] *See* Parliament of Australia: Cybercrime Legislation Amendment Bill 2011 http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4575 (computer related crimes are punishable by imprisonment with no alternatives such as fines available as penalty) *Compare with* Computer Misuse Act 1990, c.18 (computer specific crimes subject to penalties varying from fines to imprisonment ranging from six months to 10 years depending on the nature of the crime)

[40] *COC, supra* n. 10, at art. 20(1)(b).

[41] *COC, supra* n. 10.

noncompliance.[42]

d. Mutual Assistance Under the Convention on Cybercrime

The United Nations' defines mutual assistance as the "process by which States seek and provide assistance in gathering evidence. . ."[43] The COC imposes on Parties a duty of "mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses. . ."[44] This provision was meant to address issues in tracing crimes to a specific computer.[45] Additionally, the COC imposes a duty of mutual assistance regarding access to evidence on stored data and real-time collection of data.[46] Generally, dual criminality requires that "the offence. . . 'is punishable under the domestic laws of both the requesting State Party and the requested State party.'"[47] Dual criminality was previously a prerequisite for mutual assistance for the expedited preservation evidence on stored computer data.[48] However, the COC explicitly eliminated the requirement of dual criminality for the preservation of stored computer data.[49]

The provisions requiring "mutual assistance to the widest extent possible" are restricted by Article 8 of the European Convention on Human Rights.[50] Article 8 guarantees Parties a right to privacy[51] and thereby weakens the duty of "mutual assistance" by Parties during cybercrime investigations.

e. Extradition Under the Convention on Cybercrime

Unlike "mutual assistance" requirements for evidence, the COC imposes a dual criminality requirement for extraditions made pursuant to it.[52] Dual criminality requires that the conduct for extradition must be criminalized in both the requesting and requested country.[53] The extradition principles set forth by the COC are to be carried out through "the application of relevant international instruments on international o-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and

---

[42] Oona A. Hathaway and Harold Hongiu Koh, *Foundations of International Law and Politics* 2 (2005).

[43] United Nations Office on Drugs and Crime, *Manual on Mutual Legal Assistance and Extradition* at 19 (2012) [hereinafter *Manual on Mutual Legal Assistance and Extradition*]. https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf

[44] *COC, supra* n. 10, c.3, art. 25-1

[45] *Id.* at art. 31.

[46] *Id.* at art. 33.

[47] *Manual on Mutual Legal Assistance and Extradition,* supra n. 43, at 48.

[48] *COC, supra* n. 10, at art. 29.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.* at art. 24 (Applies to extradition between Parties. . . provided the acts are punishable for a maximum period of at least one year or more under the laws of both Parties).

[53] Michael John Garcia & Charles Doyle, *Extradition to and from the United States: Over, Extradition and Rendition: Background and Issues* 8 (2011).

domestic laws." [54] The drafters did not intend for the COC to supersede other extradition instruments or arrangements between Parties.[55] The COC reserves to each Party "the right not to apply or to apply only in specific cases or conditions" the directives of the COC.[56] Thus, extradition requests are ultimately carried out at the discretion of each of the Parties.

f. Jurisdiction Pursuant to the Convention

The COC establishes that any violation of Articles 2 through 11 is to be prosecuted by the state/territory in which the crime occurred.[57] If the crime occurs on an aircraft or ship, the registered state/territory of the aircraft or ship will be responsible for prosecution.[58]

The Convention also allows a State to establish jurisdiction over "one of its nationals, if the offense is punishable under criminal law where it was committed or if committed outside the territorial jurisdiction of any State."[59] The Convention also allows Parties to establish jurisdiction in conformity with their domestic law.[60] Like the mutual assistance and extradition provisions, discussed above at section d, Parties to the Convention "reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down [in this article]."[61]

II. Cybercrime

The COC does not provide a definition of the term "cybercrime."[62] Similarly, the United States does not have an official definition of the term "cybercrime."[63] A comparative survey conducted by Canada's Ryerson University revealed that most countries with laws addressing cybercrimes do not have a concrete definition of cybercrime.[64]

---

[54] *COC, supra* n. 10, at art. 23.

[55] *Explanatory Report, supra* n. 13, at 244.

[56] *COC, supra* n. 10, at art 22.

[57] *Id.*

[58] *Id.*

[59] I*d.*

[60] *Id.*

[61] *Id.* at art. 22.

[62] *COC, supra* n. 10, at C.1, Art. 1.

[63] nalyzingnvention on Cybercrime: An Analysis of Nontraditional Crimes Utilizing Various Jurisdictional Principles of Internation *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement,* CRS Report No. R42547 (2015) [hereinafter *CRS Report No.* R42547]. https://www.hsdl.org/?view&did=762027

[64] Avner Levin and Daria Ilkina, *International Comparison of Cyber Crime* (March 2013) http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf

No single agency leads the fight against cybercrime at a global level.[65] Juniper Research, a leading market analyst, estimates that cybercrime costs will increase to $2.1 trillion globally by 2019.[66] This is a conservative measurement since cybercrime is often underreported by financial organizations, private companies and individuals.[67] Financial organizations may be deterred from reporting data breaches in fear of damaging their professional reputations. Financial organizations would be at risk of losing customers and risk consumers pulling their support and patronage.[68] Underreporting by financial organizations is especially relevant because these organizations are holders of sensitive personal data. As the 2008 financial crisis demonstrated, disruptions in the markets can have detrimental effects at a global level. A localized cybersecurity attack on one financial organization can pose serious risks to financial markets around the world due to the interconnected nature of the financial system.

In contrast, private individuals underreport for various other reasons. Most commonly, cybercrimes go undetected and it is not until later that an individual realizes s/he was a victim.[69] Even when detected, victims may not realize it is a reportable crime or may decide not to report for reasons of embarrassment or inconvenience.[70]

Cybercrime generally falls into two categories.[71] In the first category, the computer is the target of the crime.[72] This category includes attacks on network confidentiality, integrity and/or availability.[73] The second category consists of traditional offenses – such as theft, fraud, and forgery committed with the assistance or by means of computers, computer networks, and communication technology.[74] The COC was created in response to upward trends in internet-related crimes but its focus, discussed above at Sec. II(a)(ii), is on the second category of offenses.[75]

The COC does not have protocols for reviewing or updating its legal framework.[76] Therefore, cybercrimes which are not based on traditional offenses, discussed above at Section II, are not covered by the COC.[77] Consequently, there is little accountability between the Parties for the creation of legislation regarding

---

[65] *CRS Report No. R42547, supra* n. 51.

[66] Juniper Research, *Cybercrime Will Cost Business Over $2 Trillion by 2019* (May 2015) https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[67] *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement,* CRS Report NO. R42547 https://fas.org/sgp/crs/misc/R42547.pdf

[68] *Id.*

[69] 5 M.E. Kabay, *Computer Security Handbook* C.10 (2009)

[70] *Id.*

[71] *Id.* at 57

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *See COC, supra* n. 10.

[76] *See COC, supra* n. 10.

[77] *Id.*

these nontraditionally based crimes.[78] This has created an area of legal uncertainty since offenses which target computers cannot be punished unless laws are in place making them illegal. The following case studies illustrate these new cybercrimes and the hurdles countries face in addressing them.

a. When a Crime is not a "Crime"

One of the main issues in dealing with cybercrime is their innovative nature. Oftentimes states are unable to prosecute cybercriminals because states have failed to implement laws relating to cybercrime. However, even when countries have laws relating to cybercrime, the crime may be outlawed in the state where it was devised, but not in the country affected. The following cases illustrate the difficulty in prosecuting nontraditional cybercrimes:

i. State Failure to Implement Cybercrime Laws

In 2000, the "Love Bug" virus deleted files, disabled Belgium ATMs, shutdown L'Oreal's email servers, and caused Microsoft to sever its outside email links at its Redmond, WA headquarters.[79] The virus is estimated to have affected over forty million users in more than twenty different countries.[80] Experts traced the "Love Bug" to the Philippines.[81] The Philippines' National Bureau of Investigation worked alongside the United States Federal Bureau of Investigations.[82] Neither country was able to prosecute Onel de Guzman, the person responsible[83] for disseminating the "Love Bug." Guzman was never prosecuted because the Philippines had not criminalized hacking or the distribution of viruses.[84] This case highlights the need for all nations to implement cybercrime laws or face the risk of cybercrimes being committed with impunity. The "Love Bug" virus was one of the first major cyber attacks to showcase the transnational reach of cybercrime and the jurisdictional difficulties in dealing with it.

At the time of the cyber attack, the United States had laws in place regarding hacking and distribution of viruses.[85] The "Love Bug's" reach was transnational and occurred without Guzman ever setting foot outside of the Philippines. The Philippines had no laws on the subject.[86] Thus, the dual criminality principle kept Guzman safe from extradition to the United States. Both hacking and dissemination were

---

[78] *See* Avner Levin and Daria Ilkina, *International Comparison of Cyber Crime,* at 5 (Several bilateral agreements exist to combat cybercrime in countries that are the main point of origin of attacks, however, countries with limited domestic resources are less able to cooperate and comply with agreements).

[79] David Kleinbard and Richard Richtmyer, *U.S. Catches 'Love' Virus,* CNN.com (May 5, 2000). http://money.cnn.com/2000/05/05/technology/loveyou/

[80] *Id.*

[81] Colin Menzies, *Love Bug Was Just First Bite by a Very Dangerous Virus,* FINANCIAL REVIEWS, (JUNE 20, 2000). http://afr.com/reports/20000620/A19850-2000June19.html

[82] *Id.*

[83] Lori Enos, *Police Nab Love Bug Suspect,* ECOMMERCE TIMES, (MAY 8, 2000). http://www.ecommercetimes.com/story/3247.htmlhttp:/www.ecommercetimes.com/perl/story/3247.html

[84] Lynn Burke, *Love Bug Case Dead in Manila,* WIRED NEWS (Aug. 21, 2000). http://archive.wired.com/politics/law/news/2000/08/38342?currentPage=all

[85] *Id.*

[86] *Id.*

new cybercrimes at the time of the attack.[87] They are no longer considered new[88], but the "Love Bug" illustrates how difficult it is for legislators to create and enforce laws for new nontraditional cybercrimes.

ii. Crimes Against Morality – Freedom of Speech vs. National sovereignty

Cybercrimes against morality are another example of cybercrimes not addressed by the COC. Crimes against morality include illegal and harmful content such as prostitution, gambling, and organized crime.[89] Crimes against morality such as prostitution and gambling are not controversial in their enforcement.[90] Hence, countries tend to provide ample cooperation and mutual assistance for prosecuting these kind of morality crimes.[91]

However, laws concerning morality vary from country to country. An example of this is the United States expansive right to freedom of speech.[92] The United States refuses to enact laws criminalizing racist/hate speech on the internet. Meanwhile, countries like France, Germany, and several Middle Eastern nations have made criminalizing racist/hate speech on the internet a priority.[93]

The 2012 "Innocence of Muslims" video shows the difficulty in enforcing morality laws in cyberspace. The "Innocence of Muslims" is an American short film.[94] The film depicted Islam as a religion of violence.[95] The video portrayed the Prophet Mohammed as a foolish and power-hungry man.[96] It was seen by thousands of people within days of its release[97], and violent protests took place at various United States embassies as a result of the film.[98] Moreover, reactions to the film have been linked to at least seventy-five deaths and hundreds of injuries.[99]

As a result, Muslim-led countries began efforts to ban insults of Muslims.[100] The efforts would ultimately restrict individual freedom of speech related to hate/racism.[101] The United States Secretary of

---

[87] *Id.*

[88] *Id.*

[89] 3 Mark W. Janis, *Introduction to International Law* (1999) at 248 [hereinafter *Introduction to International Law*].

[90] *Id.*

[91] Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 130 Int. J. Law Info Tech. 10 (June 2002).

[92] *Id.*

[93] *COC, supra* n. 10.

[94] Q&A: Anti-Islam Film, BBC news: (Sept. 20, 2012) http://www.bbc.com/news/world-middle-east-19606155

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] Guy Taylor, *Muslim-Led Nations Seek Global Ban on Insults of Muhammad,* The Washington Times (Sept. 24, 2012). [hereinafter *Muslim-Led Nations Seek Global Ban on Insults of Muhammad*] http://www.washingtontimes.com/news/2012/sep/24/muslim-led-nations-seek-ban-on-insult/

[101] *Id.*

State publicly condemned the video.[102] However, the creator of the film was not sentenced or punished for any crime related to "Innocence of Muslims."[103]

Freedom of speech is embedded in the United States' Constitution and receives a high degree of protection.[104] Supreme Court Justice Breyer best encapsulates how most Americans believe freedom of speech ought to apply in cyberspace: "George Washington did not know about the Internet, but the value of "free speech" must apply to the internet."[105]

The lack of uniformity in laws concerning morality based cybercrimes create serious jurisdictional issues. The United States Constitution protected the creator of "Innocence of Muslims" even though the effects of the film where punishable in the countries where the deaths and injuries actually occurred.[106]

iii. When Nothing is Taken—Distributed Denial of Services

Recent trends have seen a rise in hacktivism. Hacktivism is the use of computer technology to achieve a political agenda through legally ambiguous means.[107] Hacktivism generally obstructs normal computer activity and does not cause physical injuries or significant monetary loss.[108] A common strategy in hacktivism is the use of distributed denial of services (DDoS) attacks.[109] DDoS attacks work by flooding the target webpage with coordinated traffic from multiple sources.[110] As a result, the target webpage is overwhelmed and becomes unavailable for use.[111]

DDoS attacks have targeted major internet businesses and governmental webpages. [112] In June 2015, several Canadian governmental webpages were the target of hacktivist DDoS attacks.[113] The hacktivist group by the name of Anonymous coordinated DDoS attacks against Canadian government

---

[102] Jennifer Epstein, Clinton: Video is "'Disgusting' and Reprehensible," Politico (Sept. 13, 2012) http://www.politico.com/blogs/politico44/2012/09/clinton-video-is-disgusting-and-reprehensible-135446

[103] Brooks Barnes, *Man Behind Anti-Islam Video Gets Prison Term,* The New York Times (Nov. 7, 2012) http://www.nytimes.com/2012/11/08/us/maker-of-anti-islam-video-gets-prison-term.html

[104] U.S. Const. amend. I; *see also* Frederick Schauer, *The Exceptional First Amendment,* The Social Science Research Network (Feb. 2005) (contrasting high level of protection the right to freedom of speech receives in the U.S. compared with the world). file:///C:/Users/w1o/Downloads/RWP05-021.pdf

[105] Stephen Breyer, *The Court and the World* at 275 (2015)

[106] *Muslim-Led Nations Seek Global Ban on Insults of Muhammad, supra* n. 100.

[107] Stanford University, *What is 'Hacktivism'* (accessed April 22, 2017) https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

[108] *Id.*

[109] *The Ten Biggest Security Incidents of 2016,* WeLiveSecurity.com (accessed April 20, 2017) https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

[110] *What is a DDoS Attack,* DigitalAttackMap.com (accessed April 20, 2017) http://www.digitalattackmap.com/understanding-ddos/

[111] *Id.*

[112] *Id.*

[113] Amy Minsky, *'Anonymous' Claims Responsibility for Cyber Attack that Shut Down Government Websites,* GlobalNews.com (June 17, 2015). http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/

webpages in protest of Canada's proposed Conservative anti-terror bill. [114] Webpage access was shut down for approximately four hours.[115] The attack produced no physical injuries or significant monetary loss, but it did raise cybersecurity concerns.[116]

The United States has prosecuted DDoS attacks under conspiracy to cause intentional damage to a protected computer, causing intentional damage to a protected computer, and aiding and abetting charges.[117]

One case involved a federal grand jury for DDoS attacks against California's Santa Cruz City webpage.[118] The government's webpage was attacked in protest of the new "Camping Prohibited" legislation. [119] The webpage was temporarily shut down.[120] The United States Attorney did not treat the attack as an act of protest protectable by the First Amendment.[121] Instead, the prosecution argued that the website and the servers were used in negatively affecting interstate and foreign commerce and communication.[122]

In the United States, the maximum statutory penalty for causing intentional damage to a protected computer and aiding and abetting is 2 to 10 years imprisonment[123], three years of supervised release,[124] and a fine of $250,000 plus restitution[125] when appropriate.

DDoS cyberattacks are a problem for countries worldwide. The internet's main feature—accessibility—means DDoS attacks are not preventable.[126] The EU Convention on cybercrime has criminalized DDoS attacks.[127] However, countries without specific legislation making DDoS attacks illegal cannot prosecute DDoS creators since no traditional property crime was ever committed. Parties to the EU Convention could use the Convention's mutual assistance and extradition provisions to extradite DDoS creators. Where DDoS creators attack a COC member party from a country where the COC has not entered into force, the target country does not have jurisdiction and thus is unable to prosecute.

---

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Charges in Distributed Denial of Service Attack Against Santa Cruz County Website,* Federal Bureau of Investigations (Sept. 22, 2011). https://archives.fbi.gov/archives/sanfrancisco/press-releases/2011/charges-in-distributed-denial-of-service-attack-against-santa-cruz-county-website

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] 18 U.S.C. § 1030(a)(5)(A)

[124] 18 U.S.C. § 1030(c)(4)(A)(i)(I)

[125] 18 U.S.C. § 1030(c)(40(B)(i)

[126] Amy Minsky, *'Anonymous' Claims Responsibility for Cyber Attack that Shut Down Government Websites,* GlobalNews.com (June 17, 2015).

[127] *COC, supra* n. 10, *T-CY Guidance Notes #5*, Art. 2, 4, 5, 11, 13

III. Introduction to Principles of International Law

International law governs relations and conduct between states and international organizations as well relations between states and persons natural or juridical. There are three main types of jurisdictional theories: prescription, enforcement, and adjudication. The main principles underlying international jurisdictional concepts include nationality, territorial, protective, universality, and passive personality principles. A summary of each of these basic principles is set forth below.

a. Nationality Principle

Under the nationality principle a state has jurisdiction over its own nationals even when they are physically outside of the state's borders.[128] The nationality principle stems from a belief that countries have responsibility over its nationals and their actions in other countries.[129] The nationality principle subjects the wrongdoer to the jurisdiction of the foreign state where the crime was committed and to the jurisdiction of its own national government.[130]

Steele v. Bulova,[131]a U.S. Supreme Court case, helps illustrate how states can utilize the nationality principle. The *Bulova* court addressed the extraterritorial application of the Lanham Act where a United States citizen sold Bulova-branded watches in Mexico without Bulova's authorization.[132] The *Bulova* court held that "Congress in prescribing standards of conduct for American citizens may project the impact of its laws beyond the territorial boundaries of the United States."[133] Furthermore, the *Bulova* decision asserted that states may "[govern] the conduct of its own citizens upon the high seas or even in foreign countries"[134] as long as "the rights of other nations or their nationals are not infringed."[135]

b. Territorial Principle

Under the territorial principle, a state has power to prescribe and adjudicate its own rules of law for any conduct occurring within its own territory.[136] The territorial principle is the most fundamental principle of jurisdiction.

The territorial principle has long been recognized by the United States. In *America Banana Co. v. United Fruit*, the court proclaimed it "the general and almost universal rule."[137] The court went further to state that to allow a country to determine an act unlawful based on the laws of another country is "not only . . . unjust, but would be an interference with the authority of another sovereign."[138]

---

[128] 3 Mark W. Janis, *Introduction to International Law* (1999) at 243

[129] *Id.*

[130] *Id.*

[131] *Steele v. Bulova*, 344 U.S. 280 (1952).

[132] *Id.*

[133] *Id.* at 282.

[134] *Id.* at 285.

[135] *Id.* at 286.

[136] *Id.* at 243.

[137] *America Banana Co. v. United Fruit*, 213 U.S. 347, 356 (1909)

[138] *Id.*

The territorial principle is no longer the exclusive basis for the assertion of state jurisdictional authority.[139] However, territoriality is seen as one of several foundations of jurisdiction, albeit the most fundamental.[140]

c. Protective Principle

The protective principle permits a state to exercise jurisdiction over conduct by persons who are not its nationals. The conduct typically referred to is one which is directed against the security of the state or a limited class of other state interest.[141] The protective principle applies only if the threat to security is generally considered to be a crime.[142] Typical crimes that fall in this category include counterfeit currency and passbook fraud. [143]

d. Universality Principle

The universality principle grants authority to punish universally dangerous acts.[144] Crimes typically associated with this principle include piracy, hijacking, terrorism, and drug trafficking.[145] The universality principle does not require a link between the state and the parties or the acts in questions.[146] The only requirement is that the State assuming jurisdiction must have the defendant in custody.[147]

e. Passive Personality Principle

The passive personality principle allows jurisdiction over foreigners when their acts affect the subjects of the state asserting jurisdiction, wherever they may be.[148] France is one of the few countries that actively embraces the passive personality principle.[149] The French have embodied it in the French Civil Code.[150] The French Civil Code gives French courts jurisdiction over persons anywhere who are legally responsible to French nations, even with respect to obligations incurred outside of France.[151]

IV. EU Convention on Cybercrime and the Various Principles of International Law

The COC utilizes the territoriality and nationality principles as its main basis of jurisdiction.[152] Both principles are easy to apply when traditional property based cybercrimes are committed. However,

---

[139] 3 Mark W. Janis, *Introduction to International Law* (1999) at 243.
[140] *Id.*
[141] *Id.* at 248.
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id. at* 249.
[149] *Id.*
[150] *Id.*
[151] *Id. at* 249.
[152] *See COC, supra* n. 10, at Art 22.

new non-traditional based crimes are created everyday on the internet.[153] The internet has become a sea of uncharted territory when it comes to prosecuting these nontraditional crimes. The following is an analysis of each of the jurisdictional principles of international law, discussed in Section III, as they relate to nontraditional cybercrimes.

a. Nationality Principle

The COC explicitly grants a Party jurisdiction over its nationals even if the cybercrime was committed outside of its physical territory.[154] Jurisdiction over nationals is not predicated on COC membership. Any country could assert jurisdiction on the basis of the nationality principle.

Prosecution is problematic when the country where the national committed the crime is unwilling to extradite the wrongdoer. Article 23 of the COC states that extradition procedures are subject to existing extradition agreements between countries.[155] Further, countries reserve the right to decline extradition requests.[156] The Edward Snowden case best illustrates this problem. Edward Snowden was a former National Security Agency contractor for the United States.[157] In 2013, Snowden used the internet to leak classified government documents.[158] The United States government brought charges against Snowden for theft of government property,[159] unauthorized communication of National Defense Information,[160] and willful communication of classified communications intelligence information to an unauthorized person.[161] Snowden fled the United States and is currently receiving asylum in Russia.[162] Snowden was in the United States when he leaked the documents.[163] Therefore, the United States has territorial jurisdiction, discussed below at section *b.* Pursuant to the EU Convention on Cybercrimes, the United States could exert jurisdiction over Snowden under the nationality principle. The United States is unable to obtain mutual assistance based on the nationality principle because Russia is not a party to the COC. Russia has made it clear they are unwilling to cooperate with extradition request; a reservation which is clearly permitted in the COC.[164] Therefore, even if Russia was a party to the COC, its choice not to assist the United States in the prosecution against Snowden would be permissible.

---

[153] Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Cybercrime,* 2002 UCLA J.L. & Tech 3 (March 2017).

[154] *COC*, *supra* n. 10, at art. 22.

[155] *COC*, *supra* n. 10, at art. 23.

[156] *Id.*

[157] Arjun Kharpal, *Edward Snowden: US Government 'Reckless Beyond Words' after WikiLeaks Docs Show CIA Hacking Tools* (March 8, 2017) http://www.cnbc.com/2017/03/08/edward-snowden-wikileaks-cia-hacking-us-government-reckless-beyond-words.html

[158] *Id.*

[159] Complaint, *United States of America v. Edward J. Snowden,* No. 1:13 CR 265 (CMH) (E.D. Wash. 2013)

[160] *Id.; see also* 18 U.S.C. 793(d)

[161] *Id.; see also* 18 U.S.C. 798(a)(3)

[162] Andrew E. Kramer, *Russia Extends Edward Snowden's Asylum* (Jan. 18, 2017) https://www.nytimes.com/2017/01/18/world/europe/edward-snowden-asylum-russia.html

[163] *Id.*

[164] *Id*.

The nationality principle of jurisdiction is inadequate when a national is in a country that is not a party to the COC or when a Party to the COC declines to cooperate.[165] The COC's nationality-based jurisdiction provision is well-intentioned. Certainly, there will be cases where Parties to the COC will benefit from this explicit power over nationals. The nationality based principle of jurisdiction can be better utilized, however, if countries establish cooperation and extradition agreements specific to cybercrimes.

b. Territorial Principle

The territorial principle of jurisdiction is explicitly provided for in the EU Convention of Cybercrime.[166] Its inclusion is not controversial as it is the original basis for jurisdiction.

The "Love Bug" case, discussed above at Section II(a)(i), emphasizes two problems with the territorial principle as the sole basis of jurisdiction in cyberspace. Territorial principle requires that countries have laws in place making these nontraditional cybercrimes illegal.[167] Moreover, the territorial principle requires that the "character of an act" be "determined wholly by the law of the country where the act is done."[168]

The second requirement raises a controversial and difficult question to address. In the "Love Bug" case the keystrokes that disseminated the virus were hit in the Philippines, but the "act" of deleting files, disabling ATM machines, and shutting down servers were done in various countries. In cases such as these, which country should be allowed to prosecute? The country which was most affected by the virus? The country with the strictest laws regarding the specific cybercrime? Or perhaps the country with the least restrictive laws?

The "Love Bug" case went unpunished because the Philippines was not a party to the COC and had no laws regarding nontraditional cybercrimes. However, the "Love Bug" raised important questions regarding where the "act is done." Cybercrimes are not neatly confined within specific geographical and state boundaries. Therefore, the territorial principle of jurisdiction is not viable as the sole basis of jurisdiction for cybercrimes.

c. Protective Principle

The EU Convention on Cybercrime does not grant jurisdiction based on the protective principle. The protective principle of jurisdiction is an adequate jurisdictional basis for conduct generally considered to be a crime. The COC provides a good basis for classifying general property-based crimes.[169] Its failure to acknowledge nontraditional cybercrimes, however, creates inconsistencies that make the protective principle hard to use.

The "Innocence of Muslims," discussed above at Section II(a)(ii), caused riots and violent protests that could be classified as a threat to national security in various countries. The speech was protected by the United States' broad freedom of speech right. The COC explicitly rejects any conduct that would encroach

---

[165] *See COC, supra* n. 10.

[166] *Id*. at art. 22.

[167] *Id.*

[168] *America Banana Co. v. United Fruit,* 213 U.S. 347 at 356.

[169] *COC, supra* n. 10, at art. 22, 23.

on a Party's sovereignty.[170] Therefore, the protective principle is unavailable where there is a difference between each country's definition of what constitutes threats to national security versus what is allowable as freedom of expression via the internet.

The COC ought to consider including the protective principle as a basis of jurisdiction only if it can agree on acts that constitute threats to national security. Further, the COC must acknowledge that in order to be effective, countries must be willing to give up some of their sovereignty. Otherwise content such as the "Innocence of Muslims" which threatens national security of specific countries will continue to go unpunished.

d. Universality Principle

The universality principle of jurisdiction is not a basis of jurisdiction under the EU Convention on Cybercrime *per se*. Crimes such as piracy, hijacking, terrorism, and drug trafficking are crimes considered universally dangerous. Thus, under the universality principle, countries can prosecute these crimes wherever they occur. The universally dangerous crimes generally have a tangible or physical aspect to them. The COC is focused on property based crime that are tangible to a certain degree. Therefore, parties to the COC could assert the universality principle of jurisdiction in cases where the internet is used to commit any of the universally dangerous crimes.

e. Passive Personality Principle

The passive personality principle allows jurisdiction over foreigners when their acts affect the state asserting jurisdiction. In theory, this is a useful jurisdictional basis that prevents countries from becoming safe havens for cybercrime. Countries who have not signed on to the EU Convention on Cybercrime or who have not implemented cybercrime laws are a cybercriminal's paradise. Cybercriminals can wreak havoc from within these territories and into other territories with impunity.

The main problem with the passive personality principle is that cyber attacks can be disseminated to multiple territories. Therefore, under the passive personality principle, multiple countries could assert jurisdiction for the same crime. It seems unlikely that countries would be willing to accept any changes to the COC that would allow the passive personality principle to subject their citizens to multiple jurisdictions.

I. Conclusion

The EU Convention on Cybercrime ("COC") is the first Treaty to address cybercrimes at a transnational level. And while it is a valuable tool for prosecuting property based cybercrimes, it fails to provide a legal framework for nontraditional cybercrimes. The COC explicitly provides nationality and territorial principles as a basis for jurisdiction. The transnational nature of the internet and nontraditional cybercrimes require that the COC revise its jurisdictional basis. Revisions ought to consider adding specific provisions for instances when the protective, universal, and passive principles can be utilized.

---

[170] *Id* at art. 23. (cooperation ought to be to the "widest extent possible")

Bibliography

Primary Sources

Treaties

Convention on Cybercrime (Nov. 23, 2011), ETS NO. 185

Statutes

18 U.S.C. § 1030(a)(5)(A)

18 U.S.C. § 1030(c)(4)(A)(i)(I)

18 U.S.C. § 1030(c)(40(B)(i)

Computer Misuse Act 1990

Model Penal Code Section 5.01(3)

Cases

America Banana Co. v. United Fruit, 213 U.S. 347 (1909)

Oracle USA, Inc. v. Rimini St. Inc., 2014 U.S. Dist. LEXIS 148519 at 5 (D. Nev. Oct. 14, 2014)

Steele v. Bulova, 344 U.S. 280 (1952)

Complaint, *United States of America v. Edward J. Snowden,* No. 1:13 CR 265 (CMH) (E.D. Wash. 2013)

Legislative Material

Congressional Research Service, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, No. R42547 (2015)

Convention on Cybercrimes, *Chart of Signatures and Ratifications of Treaty 185*, ETS No. 185. (Last updated April 7, 2017)

Council of Europe, Committee of Experts on Crime in Cyber-space, *Final Activity Report* (May 25, 2001)

Explanatory Report, *Convention on Cybercrime,* ETS NO. 185 (Nov. 8, 2011)

Parliament of Australia: Cybercrime Legislation Amendment Bill (2011) http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4575

Secondary Sources
Books

Michael John Garcia & Charles Doyle, *Extradition to and from the United States: Over,* EXTRADITION AND RENDITION: BACKGROUND AND ISSUES 8 (Brenden M. Zimmer, ed. 2011).

Oona A. Hathaway and Harold Hongiu Koh, *Foundations of International Law and Politics* 2 (2005).

3 Mark W. Janis, *Introduction to International Law* (1999)

5 M.E. Kabay, *Computer Security Handbook* C.10 (2009)

Stephen Breyer, *The Court and the World* at 275 (2015)

Law Reviews

Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 130 Int. J. Law Info Tech. 10 (June 2002).

Internet Sites

Amy Minsky, *'Anonymous' Claims Responsibility for Cyber Attack that Shut Down Government Websites,* GlobalNews.com (June 17, 2015). http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/

Arjun Kharpal, *Edward Snowden: US Government 'Reckless Beyond Words' after WikiLeaks Docs Show CIA Hacking Tools* (March 8, 2017) http://www.cnbc.com/2017/03/08/edward-snowden-wikileaks-cia-hacking-us-government-reckless-beyond-words.html

Avner Levin and Daria Ilkina, *International Comparison of Cyber Crime* (March 2013) http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf

Brooks Barnes, *Man Behind Anti-Islam Video Gets Prison Term,* The New York Times (Nov. 7, 2012) http://www.nytimes.com/2012/11/08/us/maker-of-anti-islam-video-gets-prison-term.html

Charges in Distributed Denial of Service Attack Against Santa Cruz County Website, Federal Bureau of Investigations (Sept. 22, 2011). https://archives.fbi.gov/archives/sanfrancisco/press-releases/2011/charges-in-distributed-denial-of-service-attack-against-santa-cruz-county-website

Colin Menzies, *Love Bug Was Just First Bite by a Very Dangerous Virus,* FINANCIAL REVIEWS, (JUNE 20, 2000). http://afr.com/reports/20000620/A19850-2000June19.html

David Kleinbard and Richard Richtmyer, *U.S. Catches 'Love' Virus,* CNN.com (May 5, 200). http://money.cnn.com/2000/05/05/technology/loveyou/

Frederick Schauer, *The Exceptional First Amendment,* The Social Science Research Network (Feb. 2005).

Guy Taylor, *Muslim-Led Nations Seek Global Ban on Insults of Muhammad,* The Washington Times (Sept. 24, 2012). http://www.washingtontimes.com/news/2012/sep/24/muslim-led-nations-seek-ban-on-insult/

International Telecommunications Union, *Facts and Figures* (2005) http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2005.pdf

International Telecommunications Union, *Facts and Figures* (2016) http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

Jennifer Epstein, Clinton: Video is "'Disgusting' and Reprehensible," Politico (Sept. 13, 2012) http://www.politico.com/blogs/politico44/2012/09/clinton-video-is-disgusting-and-reprehensible-135446

Jessi Hempel, *Inside Facebook's Ambitious Plan to Connect the Whole World,* Wired.com (Jan. 19, 2016) https://www.wired.com/2016/01/facebook-zuckerberg-internet-org

Jon Russell, *Google Expands its Initiative to Provide Free Wi-Fi Hotspots in Emerging Markets,* TechCrunch.com (Sept. 27, 2016) https://techcrunch.com/2016/09/27/google-station-free-wifi-hotspots/

Juniper Research, *Cybercrime Will Cost Business Over $2 Trillion by 2019* (May 2015) https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Lori Enos, *Police Nab Love Bug Suspect,* ECOMMERCE TIMES, (MAY 8, 2000) http://www.ecommercetimes.com/story/3247.htmlhttp:/www.ecommercetimes.com/perl/story/3247.html

Lynn Burke, *Love Bug Case Dead in Manila,* WIRED NEWS (Aug. 21, 2000) http://archive.wired.com/politics/law/news/2000/08/38342?currentPage=all

Samuel Gibbs, *Elon Musk Wants to Cover the World with Internet Space,* The Guardian (Nov. 17, 2016) https://www.theguardian.com/technology/2016/nov/17/elon-musk-satellites-internet-

Selena Larson and Jethro Mullen, *Global Cyber Attack: What You Need to Know,* CNN.com (June 28, 2017) http://money.cnn.com/2017/06/28/technology/ransomware-attack-petya-what-you-need-to-know/index.html

Stanford University, *What is 'Hacktivism'* (accessed April 22, 2016) https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

The Ten Biggest Security Incidents of 2016, WeLiveSecurity.com (accessed April 20, 2017) https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

United Nations Office on Drugs and Crime, *Manual on Mutual Legal Assistance and Extradition* at 19 (2012) [hereinafter *Manual on Mutual Legal Assistance and Extradition*]. https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf

U.S. Const. amend. I

Q&A: Anti-Islam Film, BBC news: (Sept. 20, 2012) http://www.bbc.com/news/world-middle-east-19606155

What is a DDoS Attack, DigitalAttackMap.com (accessed April 20, 2017) http://www.digitalattackmap.com/understanding-ddos/

Can One Infringe an Invalid Patent? The Blindside of Patent Arbitration

LUIZ MIRANDA

April 2017

Enforceability of U.S. Patents are primarily a matter for the Courts. However, when disagreement arises from an international patent licensing agreement, these matters typically end up in arbitration. Parties cite the many advantages of arbitration as the reasoning behind such arrangements. But given the availability of the new Post-Grant Review forums at the United States Patent and Trademark Office, are licensees of "weak" patents giving up too many rights by their use of arbitration?

This paper aims to educate its reader on the advantages of arbitration clauses in U.S. patent licensing agreements, yet stress the caveats of blindly pursing them. It will then illustrate scenarios of inequitable arbitration awards upheld by U.S. Courts, contrary to public policy, such as upholding an award that was based on a now invalid patent

I. *Introduction*

Arbitration disputes resulting from U.S. patent licensing agreements are on the rise.[1] Proponents of arbitration tout its various advantages, especially when international parties are involved.[2] Still, these disputes present unique challenges in the face of U.S. public policies relating to the patent system, due to the limited monopoly granted by the United States Patent and Trademark Office ("USPTO") to its recognized patent owners. However, new avenues now exist for potential patent licensees to question the validity of the very patents they are being compelled to license. Thus, a closer look at whether patent arbitration still lives up to its promise is warranted. Continuing from this introduction, Part II of this paper analyzes the advantages of arbitration, including arbitrator expertise, confidentiality, speed, cost, and international factors. Part III sheds light on the rise in the use of patent post-grant proceedings—such as the new inter partes review—as an alternative to arbitration. Part IV discusses the public policy considerations of upholding awards that contain findings of patent validity, including a discussion of the recent Court of Appeals for the Federal Circuit case *Bayer CropScience AG v. Dow Agrosciences LLC*. Finally, Part V highlights the importance of new considerations that should be taken into account when engaging into future international business transactions that include patent licensing agreements with arbitration clauses.

The Advantages of Patent Arbitration

The arbitration forum is touted by many scholars as a superior alternative to court litigation, even in patent disputes.[3] Patent-specific advantages such as arbitrator expertise support the familiar themes of increased confidentiality, advantageous speed, decreased cost and international considerations.

A. Arbitrator Expertise

Patent litigation is riddled with specialized topics increasingly requiring expert knowledge of science and technology. Its complexity often results in the need for the resolution of heavily disputed factual determinations. A major advantage to an arbitration proceeding, as opposed to a court proceeding, is the ability for party-appointed arbitrators to make those factual determinations as opposed to a jury.[4] The U.S. Court of Appeals for the Federal Circuit, a specialized court with the jurisdiction to hear nation-wide patent appeals, reverses 30% to 50% of all patent claim construction decisions of U.S. District Courts.[5] This high number of reversals is commonly blamed on "judges or juries who lack the expertise to deal with intricate and

---

[1] Ron Dimock, *7 Benefits Of Arbitration In A Patent Dispute*, LAW360 (Aug. 27, 2015) (discussing the many benefits of patent arbitration), https://www.law360.com/articles/695649/7-benefits-of-arbitration-in-a-patent-dispute.

[2] *See Id*.

[3] *Id*.

[4] Stephen R. Stern; Sloan J. Zarkin, *Why Arbitration Beats Litigation for Commercial Disputes*, 32 GPSolo 40, 44 (2015) (noting that "in those cases where a jury is involved, the court process becomes even more attenuated and costly").

[5] Mihir Chattopadhyay (Three Crowns LLP), *The Case for Arbitration of Patent Disputes*, KLUWER ARBITRATION BLOG (Feb. 25, 2016), http://kluwerarbitrationblog.com/2016/02/25/recent-event-the-case-for-arbitration-of-patent-disputes.

technical patent cases [and thus] often reach conclusions that are susceptible to successful challenges."[6]

Arbitration institutions, such as the International Chamber of Commerce ("ICC"), maintain a roster of highly-qualified arbitrators at their disposal, many of whom are registered patent lawyers and/or engineers.[7] The flexibility offered by the arbitration proceedings means that parties can appoint arbitrators who have the desired knowledge in the asserted patent's related field, instead of relying on delivering technical teachings to judges or to a jury.[8] This feature of arbitration facilitates the dispute because proceedings can be presented at higher technical levels due to the arbitrator's knowledge.[9] Simply put, "by oversimplifying the case for the jury, there is a risk of the jury not appreciating the details of a patent case, and therefore may lead to an irrational decision."[10] These irrational decisions may be overturned on appeal. Replacing the jury with expert arbitrators minimizes that risk.

B. Confidentiality

Another benefit of arbitral proceedings is confidentiality. In general, when agreed to by the parties, arbitration confidentiality may cover most materials produced in the arbitration including evidence, pleadings, and the arbitrator's deliberations.[11]

However, in patent disputes, confidentiality is undermined by the Patent Act, specifically 35 U.S.C. §§ 294(d) and (e). Under these provisions, arbitration awards must be reported to the USPTO, and no award arising from an arbitration clause in a patent agreement is enforceable until it has been delivered to the USPTO, where it becomes a part of the patent prosecution file.[12] In this regard, the Seventh Circuit has held that arbitration documents and awards that were kept confidential by the parties during arbitration discovery remain subject to disclosure in subsequent District Court proceedings in response to court orders and subpoenas, regardless of the level of confidentiality agreed to by the parties in arbitration.[13] The Seventh Circuit reasoned that "many litigants would like to keep confidential the salary they make, the injuries they suffered, or the price they agreed to pay under a contract, but when these things are vital to claims made in litigation they must be revealed."

---

[6] *Id*.

[7] Chris Neumeyer, *Think Patent Arbitration Can't Work? Think Again*, IPWatchdog (Jun. 10, 2013), http://www.ipwatchdog.com/2013/06/10/think-patent-arbitration-cant-work-think-again/id=41447.

[8] *Id*.

[9] *See* Dimock, *supra* note 1.

[10] *Id* (citing Priscilla Anne Schwab, *The Litigation Manual First Supplement,* United States of America: American Bar Association, 351 (2007)).

[11] Gary Born, *International Commercial Arbitration* § 20.03, 2783, 2791 (2n ed. 2014).

[12] 35 U.S.C. § 294(d); 35 U.S.C. § 294(e).

[13] *See Baxter Intern., Inc. v. Abbott Labs.*, 297 F.3d 544, 546–47 (7th Cir.2002).

To summarize, complete arbitration confidentiality is less possible in the U.S., and the risk of disclosure exists when the arbitration award is challenged, enforcement of the award is requested, or when unrelated third parties are involved. Nevertheless, because a *complete* record of the proceedings is not required to be revealed, the confidentiality outcome of arbitration disputes still holds superior to outright public court proceedings.

C. Speed and Cost

Other well-known benefits of arbitration are high speed and low cost. These benefits are especially important when compared to the high cost and time consuming aspects of patent litigation.[14] Patent litigation can cost between $2 and $5 million or more, with about half of these costs arising out of discovery and related motion practice.[15] In 2013, the World Intellectual Property Organization ("WIPO") published results of a survey finding that resolving technology disputes in arbitration saved, on average, more than 60% in time and up to 55% in costs, compared to litigation.[16]

Proponents of commercial arbitration maintain that international arbitration costs are better managed because 1) arbitration awards are final, without appellate review; 2) costs are better estimated and controlled when arbitrator's fees are set by the arbitration rules; and 3) a budget may be set.[17] In arbitration, the parties can further guarantee savings in both time and cost by minimizing the procedural aspects of the litigation with factors such as: decreasing the number of arbitrators, restricting the scope of discovery, limiting witnesses and submissions, limiting motions, submitting the case on the pleadings, making the award non-appealable, and so forth.[18]

Although there have been some reports of cases demonstrating increased time and cost of arbitration, it remains the exception, not the rule.[19] In those cases, the heightened costs are partially due to parties' tendencies to mirror litigation or engage in obstructive tactics.[20] To prevent similar situations, a strong tribunal president can serve an important role in reducing costs by resisting delay tactics and ensuring that the proceedings are conducted in a time and cost efficient manner.[21]

---

[14] Chattopadhyay, *supra* note 6.
[15] *Id*.
[16] Neumeyer, *supra* note 7.
[17] *Id*.
[18] Neumeyer, *supra* note 7.
[19] Chattopadhyay, *supra* note 6.
[20] *Id*.
[21] *Id*.

D. International Factors

International licensing of patents creates opportunity for parties to participate in the well-known advantages of international commercial arbitration. Those advantages include choice of forum, choice of law, and world-wide enforcement through The New York Convention (discussed below).[22] One of the key features of the convention is that recognition and enforcement of an award can only be refused under exceptional circumstances.[23] Therefore, a party who is part of an international patent infringement dispute can rely on prosecuting the issue only once, and having that arbitration award upheld across the globe.[24]

But patents are, or at least should be, only worth as much as its government's willingness to uphold its validity. This intersection of authority between the U.S. federal government and of arbitral tribunals produces some unforeseen results.

II. *The Rise in The Use of Patent Post-Grant Proceedings*

The American Invents Act of 2011, which took effect in late 2012, increased the availability of proceedings conducted by the Patent Trial and Appeal Board ("PTAB").[25] Notably, the Act added the Inter-Partes Review to the PTAB's arsenal for review of issued patents.[26] As opposed to Post-Grant Review proceedings, which are only available within 9-months after a patent is issued, Inter-Partes Review proceedings may be initiated anytime thereafter.[27] Although the PTAB cannot decide issues of infringement, it can review and revoke issued patents that do not meet some of the Federal Law requirements of the U.S. Code—such as definiteness, novelty and obviousness.[28] The review is increasingly considered a valuable alternative to litigation and, as a result, "the first half of 2014 filings increased 125 percent over the total filings in 2013."[29] Although this increased number of yearly filings stabilized in mid-2014, it has remained at its peak, and no signs of any slow-down in 2017 appears as of yet.[30] Unless the Supreme Court intervenes that is.[31]

---

[22] *See* New York Arbitration Convention (2013), available at http://www.newyorkconvention.org.

[23] Dimock, *supra* note 1.

[24] *Id*.

[25] *See* Charles W. Shiley, *Goodbye Patent Arbitration?*, Corporate Counsel (Oct. 13, 2014), http://www.corpcounsel.com/id=1202672879326/Goodbye-Patent-Arbitration?slreturn=20150314000849.

[26] *Id*.

[27] *See* Chad M. Rink, *Post-Grant Review and Inter Partes Review*, Birch, Stewart, Kolasch & Birch, LLP (last visited Jun. 24, 2017), http://www.postgrantproceedings.com/resources/procedures/article-CMR_PGR_IPR.html.

[28] *See* Shiley, *supra* note 27.

[29] *Id*.

[30] Wilson, Sonsini, Goodrich & Rosati, *2016 PTAB Year In Review*, JDSupra at 2 (Jan. 25, 2017), http://www.jdsupra.com/legalnews/2016-ptab-year-in-review-73496/ (citing Jan. 3, 2017 Filings per year data from LexMachina).

[31] Quinn, Gene, *Supreme Court to decide if Inter Partes Review is Unconstitutional*, IPWatchDog (Jun. 12, 2017), http://www.ipwatchdog.com/2017/06/12/supreme-court-inter-partes-review-unconstitutional/id=84430/.

A. The American Invents Act Inter Partes Review

The USPTO has defined the inter partes review ("IPR") process as a "trial proceeding to review the patentability of one or more claims in a patent."[32] The IPR procedure took effect on September 16, 2012, and applies to any patent issued before, on, or after September 16, 2012.[33] The IPR begins with a third-party—oftentimes a party being charged with infringement of the patent—filing a petition with the USPTO, and making a showing that "there is a reasonable likelihood that the petitioner would prevail with respect to at least one claim challenged."[34] If the challenging party overcomes this burden, a proceeding is initiated, with a final determination guaranteed by law to be delivered within one-year of the PTAB accepting the showing and initiating proceedings.[35]

B. The Inter Partes Review as An Alternative to Arbitration

The significant increase in post-grant proceedings under the AIA is anchored in savings in speed and cost by its streamlined proceedings and mandatory quick results. Once the proceedings are initiated, they move rather quickly.[36] The patent owner has three-months to respond, direct testimony is offered by affidavit, cross-examination depositions are set, and wide-range discovery is not permitted.[37] Soon after, oral arguments are delivered and the proceedings conclude.[38] A final decision is issued within one year of institution.[39]

In addition to providing quick proceedings, review by a USPTO patent examiner—a skilled artisan in the relevant technology—and the availability of expert testimony further enhance the level of expertise involved in these patent office proceedings. IPRs are also decided by a panel of administrative law judges at the USPTO who are patent law specialists, rather than generalist District Court Judges.[40]

Similar to arbitration, the result is a quick and therefore less costly proceeding, led by a decision-maker with technical expertise. Thus, IPR proceedings are being increasingly presented as a litigation alternative to patent arbitration.[41] Some scholars go so far as concluding that, due to these latest enhancements to PTAB proceedings, patent arbitration may just "wither away and die."[42] Others argue that post-grant proceedings should instead only be seen as a complementary process to patent arbitration, and

---

[32] *Inter Partes Review*, United States Patent and Trademark Office, https://www.uspto.gov/patents-application-process/appealing-patent-decisions/trials/inter-partes-review.

[33] *Id*.

[34] *Id*.

[35] *Id*; *see also* 37 CFR Ch. 42, Subpart B.

[36] Shiley, *supra* note 27.

[37] *Id*.

[38] *Id*.

[39] *Id*.

[40] *Id*.

[41] *See generally Id*.

[42] Shiley, *supra* note 27.

that such proceedings are "not a realistic substitute for arbitration."[43] Whatever the case may be, it is an important choice that a patent licensee should consider.

Finally, an even more interesting result of IPR proceedings is the increased likelihood that a precariously issued patent may be invalidated by the PTAB.[44] As of 2014, the PTAB instituted IPR petitions for at least one challenged claim at a rate of 84 percent.[45] From those that reach a final decision on the merits, all instituted claims are invalidated or disclaimed over 77 percent of the time.[46] This significant rate of invalidation suggests that IPR promises to make a considerable impact on the rate that weaker patents now avail themselves to scrutiny.

III. *Arbitration Awards and Public Policy: Upholding Awards of Invalid Patents*

In 1958 the United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards—The New York Convention—was born out of a desire to enhance the effectiveness of international arbitration.[47] It does so by providing an international framework for the domestic enforcement of foreign arbitral awards. And although it has been widely ratified, it is only applicable to the extent enforced by the signatory countries.[48] Article IV sets out the conditions to be fulfilled by a party seeking enforcement of an award falling within the scope of The New York Convention, permitting the State to refuse enforcement of the foreign arbitral award on any of the grounds outlined therein.[49] Notably, Article V(2)(b) states that: "[r]ecognition and enforcement of an arbitral award may also be refused if the competent authority in the country where recognition and enforcement is sought finds that . . . [t]he recognition or enforcement of the award would be contrary to the public policy of that country."[50] Yet the New York Convention does not attempt to define public policy, and it leaves it to the discretion of the courts of contracting states.

With an increase in the likelihood that weak patents may be invalidated, an interesting question arises in regards to arbitration clauses in licensing agreements. Will an arbitration award be upheld when it is based on a finding of infringement of a patent that has been invalidated afterwards by the PTAB? Or will the public policy argument that only the U.S. government has the power to make patent invalidity determinations apply? In either scenario, is a licensee simply giving up too many unknown rights when adhering to patent arbitration clauses?

---

[43] Peter L. Michaelson, *Patent Arbitration: It Still Makes Good Sense*, 7 Landslide 42, 47 (2015).

[44] Brian J. Love; Shawn Ambwani, *Inner Partes Review: An Early Look at the Numbers*, 81 U. Chi. L. Rev. Dialogue 93, 107 (2014).

[45] *Id*.

[46] *Id*.

[47] Funke Adekoya, *The Public Policy Defence to Enforcement of Arbitral Awards: Rising Star or Setting Sun?*, Kluwer Law Intl 2015, Vol. 2 Issue 2 203, 222 (2015).

[48] *Id*.

[49] *Id*.

[50] *See* New York Arbitration Convention (2013), available at http://www.newyorkconvention.org.

A. The Public Policy Against Arbitrators Deciding Patent Validity

The use of patent arbitration continues to gain visibility lately, evidenced by its increasing popularity in high-stakes disputes. One recent example is *Nokia Corporation v. Samsung Electronics Co.*, in which an ICC tribunal awarded an estimated $218 million annually to Nokia in a dispute arising from a licensing agreement for the use of Nokia's phone patents.[51] Similarly, in *Tessera Inc. v. Amkor Technologies Inc.*, an ICC tribunal awarded Tessera approximately $125 million for Amkor's breach of the patent license agreement between the parties.[52] Further, an ICC Tribunal in *InterDigital v. Samsung Technologies* awarded InterDigital $134 million in a dispute concerning a licensing agreement between the parties.[53] Still, challenges to patent awards in the name of public policy continue to be raised.

The debate as to whether arbitrators can, or should be able to, decide whether a patent is invalid or not is rooted in public policy.[54] As mentioned above, some jurisdictions preclude specific subject matters from being arbitrable in the name of public policy.[55] Some notable examples include marital disputes and employment issues.[56] Although patent arbitration awards are increasingly upheld, some scholars continue to argue that the question as to whether patent disputes based on validity issues are arbitrable remains undecided.[57] In the U.S., the dispute is based on the argument that only the federal government has the power to govern how a "patent monopoly" is granted, and to what extent a patent is enforced.[58] Because of this power exclusivity, some U.S. courts have even held in the past decade that arbitration tribunals cannot declare a patent invalid.[59]

---

[51] *See* Nokia, *Nokia Receives Decision In Patent License Arbitration With Samsung Positive Financial Impact for Nokia Technologies*, Nokia Corporation (Feb. 01, 2016), http://company.nokia.com/en/news/press-releases/2016/02/01/nokia-receives-decisionin-patent-license-arbitration-with-samsung-positive-financial-impact-for-nokiatechnologies; *see also* Adam Ewing, *Nokia Drops After Patent Ruling In Samsung Case Disappoints*, Bloomberg News (Feb. 01, 2016), https://www.bloomberg.com/news/articles/2016-02-01/nokia-drops-after-patent-ruling-in-samsung-case-disappoints.

[52] David McAfee, *Tessera Awarded $125M More In IP Arbitration Against Amkor*, Law360 (May 14, 2014), https://www.law360.com/articles/538108/tessera-awarded-125m-more-in-ip-arbitration-against-amkor.

[53] Ryan Davis, *Samsung Reaches Patent Settlement With InterDigital*, Law360 (Jun. 03, 2014), https://www.law360.com/articles/544109/samsung-reaches-patent-settlement-with-interdigital.

[54] Wei-Hua Wu, *International Arbitration of Patent Disputes*, 10 J. Marshall Rev. Intell. Prop. L. [i], 409 (2011).

[55] *Id*.

[56] *Id*.

[57] *Id*.

[58] *Id*.

[59] *See Beckman Industries, Inc. v. Technical Dev. Corp.*, 433 F.2d 55, 63 (7th Cir. 1970); *see also Paladino v. Avnet Computer Techs., Inc.*, 134 F.3d 1054, 1062 (11th Cir. 1998).

Yet, this is no longer the case today.[60] Appellate courts have construed The New York Convention's public-policy exception very narrowly. Most circuits follow the statement made by the Second Circuit that, in accordance with general international choice-of-law principles, the exception applies "only where enforcement would violate the forum State's most basic notions of morality and justice."[61] The Eleventh Circuit follows a similar approach, stressing the standard's strictness.[62] Importantly, in the 2017 case of *Bayer CropScience AG v. Dow Agrosciences LLC*, the Court of Appeals for the Federal Circuit went one step further to note that any incorrect finding of patent validity by the arbitral tribunal "is an ordinary legal or factual error", and therefore is *not* a ground for disturbing an arbitral award.[63] The Court, without laying out an exact standard, explained that "an asserted policy must be clearly established to justify non-enforcement of an arbitral award."[64]

B. Bayer CropScience AG v. Dow Agrosciences LLC

In *Bayer*, the United States Court of Appeals for the Federal Circuit seemed to have further nudged the debate in favor of enforceability of patent awards over the losing party's public policy arguments.[65] The *Bayer* case started with a patent cross-licensing agreement, in which Hoechst AG (Bayer's predecessor) licensed Lubrizol Genetics, Inc. (Dow Industries' predecessor) patents on various technologies related to pat genes that are resistant to herbicides used in agriculture.[66] In 2012, Bayer terminated the licensing agreement, accusing Dow Industries (hereinafter "Dow") of materially breaching part of it, and commencing litigation in the Eastern District of Virginia.[67] Dow was granted a stay in the action based on the agreement's arbitration clause, which stated that the agreement was to be governed by and construed in accordance with French law, and that disputes were to be decided by arbitration in accordance with the Rules of Conciliation and Arbitration of the International Chamber of Commerce.[68]

During the arbitration dispute, an interesting event ensued. Bayer's Opening Memorial (opening brief), filed on September 2nd, 2013, claimed that the patent at issue was valid and had been infringed.[69]

---

[60] *See* Neumeyer, *supra* note 7 (noting the various substantial patent disputes in the past few years).

[61] *In Parsons & Whittemore Overseas Co. v. Société Generale De L'Industrie du Papier (RAKTA)*, 508 F.2d 969, 974 (2d Cir. 1974) (citing 1 Restatement (Second) of the Conflict of Laws § 117 cmt. c, at 340 (Am. Law Inst. 1971)); *see also TermoRio S.A. E.S.P. v. Electranta S.P.*, 487 F.3 928, 938 (D.C. Cir. 2007); *Karaha Bodas Co. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara*, 364 F.3d 274, 306 (5th Cir. 2004); *Slaney v. Int'l. Amateur Athletic Fed'n*, 244 F.3d 580, 593 (7th Cir. 2001); *M & C Corp. v. Erwin Behr GmbH & Co., KG*, 87 F.3d 844, 851 n.2 (6th Cir. 1996).

[62] *Indus. Risk Ins. v. M.A.N. Gutehoffnungshutte GmbH*, 141 F.3d 1434, 1445 (11th Cir. 1998).

[63] *See Bayer CropScience AG v. Dow Agrosciences LLC*, No. 2016-1530, 2017 WL 788321 (Fed. Cir. Mar. 1, 2017).

[64] *Id*.

[65] *See Id*.

[66] *Id* at 3.

[67] *Id* at 5.

[68] *Dow Agrosciences*, WL 788321 at 10 (citing 9 U.S.C. § 3).

[69] *See Dow Agrosciences,* Supplement to Joint Appendix at 2 (citing *Bayer* Mem. at ¶¶ 170, 194).

However, the very next day—September 3rd, 2013—Bayer privately filed a reissue application[70] with the USPTO for the very same patent, and, in essence conceded during reissue that the patent claims, as written, were invalid under a 2013 Supreme Court decision that challenged the validity of gene patents in the United States.[71] Under U.S. law, this reissue action legally required Bayer to "surrender" the original patent pursuant to 35 U.S.C. § 252, because the reissue patent that was sought had been narrowed in scope.[72] Still, on June 2nd, 2014, and to Dow's surprise, Bayer invoked the then reissued patent during the arbitration proceedings, arguing that the reissued patent was the same as the original patent, and Dow continued to infringe the surrendered original, and now its reissued version.[73] Over Bayer's objection, the tribunal agreed.[74]

In 2015, the arbitral tribunal entered an award, finding that (1) Dow breached the patent licensing agreement and infringed on the various claims of the agreement's original and reissued patents; (2) certain asserted claims were *not* invalid for inadequate written description or lack of enablement; and (3) certain asserted patents were also *not* invalid for obviousness-type double patenting over a previously issued patent to one of Bayer's subsidiaries.[75] The tribunal then awarded Bayer $455,459,187 in damages, including $374,731,000 in lost-opportunity damages under French law for breach of contract and $67,837,000 in reasonable-royalty damages under U.S. law for patent infringement.[76] The only voice of opposition was by Arbitrator George Berman, who dissented in part, disagreeing with the tribunal's conclusion of no double patenting.[77]

Notably, Dow concurrently pursued the other avenues available to it at the USPTO, by filing six requests for inter-partes reexamination of the allegedly infringed patents.[78] Dow relied on the same arguments made to the arbitration tribunal, namely that the patents were invalid for obviousness-type double patenting over previously issued patents to Bayer's subsidiary, and that some of the patents would have been obvious over certain prior-art references.[79] Thus, Dow argued in the PTAB that the patents it was charged with infringing were invalid. Yet in its decision on the appeal of the arbitration award, the Federal Circuit noted that "[t]hose [PTAB] proceedings remain pending in the [U.S. Patent] Office and do not

---

[70] *Info - Reissue Application*, United States Patent and Trademark Office, https://www.uspto.gov/patents-application-process/filing-online/info-reissue-application ("[a] reissue application is an application that is filed to correct an error in a patent that has not expired").

[71] *See Association for Molecular Pathology v. Myriad Genetics*, No. 12-398 (569 U.S. June 13, 2013).

[72] *See Id; see also* U.S.C. § 252 (noting that "[the] surrender of the original patent shall take effect upon the issue of the reissued patent . . .).

[73] *See Id*; *see also Dow Agrosciences*, WL 788321 at 20.

[74] *Dow Agrosciences*, WL 788321 at 6.

[75] *Id*.

[76] *Id*.

[77] *Id*.

[78] *Bayer CropScience AG*, WL 788321 at 6.

[79] *Id*.

alter resolution of [the] appeal."[80] Meaning, any finding of patent invalidity by the USPTO would have no bearing on the Court's decision to either uphold or set aside the arbitration award, which had been rendered prior to any final written decision by the PTAB.

During the Federal Circuit appeal, Dow attacked parts of the arbitral award as counter to U.S. law and policies governing double patenting and post-patent-expiration royalties.[81] In particular, Dow argued that the New York Convention's Article V(2)(b) required the court to decide, among other issues, whether enforcement of the award would violate a host of patent-law requirements and policies.[82] But the Federal Circuit did not agree.[83]

On the issue of the arbitral award, the Federal Circuit stated that "[j]udicial review of the arbitral award at issue here is very limited even if, as we assume for present purposes, the standards governing both international and domestic arbitration apply. In numerous ways, the relevant federal statutes and precedents make clear that ordinary legal or factual error is not a ground for disturbing an arbitral award like the one at issue here."[84] On the topic of public policy, the Court noted that "[a] challenger must meet related, and similarly high, standards to support a refusal to confirm an award as contrary to public policy."[85] Given these "high" standards, the Court proceeded to conclude that because "[t]he tribunal carefully scrutinized Dow's argument", any incorrect legal or factual finding did not warrant vacating the arbitral award.[86] It noted that Dow's arguments "amount to no more than allegations of ordinary legal error", determining that "[t]he tribunal's analysis shows no manifest disregard of law or other error meeting the standards for rejection of arbitral determinations."[87]

---

[80] *Id*.
[81] *Id* at 14.
[82] *Id* at 8.
[83] *Bayer CropScience AG*, WL 788321 at 8.
[84] *Id* at 10.
[85] *Id* at 13.
[86] *Id* at 14-15.
[87] *Id* at 20.

IV. *Conclusion*

Arbitration of patent disputes, domestic or international, are becoming increasingly popular among parties who engage in international business transactions. Although the public policy considerations of patent arbitration awards continue to play a role in arbitrated patent disputes, the recognized "high" standard demanded by The New York Convention to set aside arbitral awards continues to increasingly rule the day in U.S. Courts. But at the same time, due to the United States' push for patent quality, increasing avenues have become available for parties to challenge the validity of issued patents directly with the United States Patent and Trademark Office. Yet, the Federal Circuit in *Bayer* seemed to indicate that those avenues would not be relevant to parties who agreed to arbitrate because those proceedings do not alter the resolution of whether to enforce an arbitral award that includes a finding of validity.[88] This means that parties who agree to arbitrate may not be able to take advantage of increasingly popular alternative methods to dispute charges of patent infringement, such as post-grant inter-partes reviews. Therefore, patent licensees who are now presented with arbitration clauses in their patent licensing agreements may want to re-evaluate their negotiation strategies, and not be so quick to sign the dotted line.

---

[88] *Bayer CropScience AG*, WL 788321 at 6.

Who's the Patent Troll?

EDWIN GARCIA

"I'm gonna make him an offer he can't refuse."
— Don Corleone, *The Godfather*

I. Introduction

To start out, let's take up a hypothetical and consider how the following three patent owners might be situated within our current patent system: a) Intel—a multibillion dollar and multinational corporation that designs and manufactures technological components; b) Intellectual Ventures[1]—a privately held company that monetizes their large patent portfolio through non-manufacturing means; and c) Bill—a top level MIT researcher who continuously patents his work and occasionally sells some devices incorporating his inventions on the internet. In our scenario, let's further imagine that a venture capital firm invested $3 million for Bill to begin a tech startup with one of his patented inventions. Shortly after launching his product, Bill walks into your office and tells you Intellectual Ventures sent him a cease and desist letter claiming he is infringing on their patent and demanding that he pay them a license fee. What should you tell Bill to do? Can he afford to refuse Intellectual Ventures' demands and defend himself in expensive patent litigation?

Defending a patent infringement claim is certainly not cheap, and licensing offers are generally strategically calculated with the costs of litigation in mind.[2] Just proceeding through the discovery phase may exceed $1 million and going to trial would increase the cost significantly beyond that sum.[3] On one hand, litigating the claim could stifle the startup's momentum and potentially syphon all of the invested capital from the business. On the other hand, a licensing agreement would reduce Bill's costs in the short term and allow him to continue operating the business.[4] If Bill is reasonably confident that Intellectual Ventures' patent is invalid and that the startup will be profitable, however, he might conclude that a license will cost more in the long term. Hence, Bill could decide to fight back in court to preserve future earnings and deter other companies from asserting weak claims against him.

In recent years "patent trolls" gained the attention of our national media and emerged as the perceived villains of our patent system.[5] The White House,[6] Congress,[7] corporations, scholars, and even the end-users of allegedly infringed products have chimed in on the subject. As defined by Peter Detkin—who coined

---

[1] *See generally* Jaconda Wagner, *Patent Trolls and the High Cost of Litigation to Business and Start-Ups - A Myth?*, Md. B.J., September/October 2012, at 17–18 (noting Intellectual Ventures raised more than $5 billion to invest from several Fortune 500 companies and now holds a portfolio of more than 35,000 IP assets).

[2] Caroline Coker Coursey, *Battling the Patent Troll: Tips for Defending Patent Infringement Claims by Non-Manufacturing Patentees*, 33 Am. J. Trial Advoc. 237 (2009).

[3] *Id.* at 241; *see also* Wagner, *supra* note 1, at 17.

[4] *See* James Bessen & Michael J. Meurer, *Lessons for Patent Policy from Empirical Research on Patent Litigation*, 9 Lewis & Clark L. Rev. 1, 16–18 (2005) (noting that a rational defendant might settle to the threat of a weak suit for three main reasons: first because court errors are difficult to avoid in patent litigation; second because weak lawsuits may be difficult to distinguish; and third because even weak suits can impose significant costs).

[5] Gregory d'Incelli, *Has Ebay Spelled the End of Patent Troll Abuses? Paying the Toll: The Rise (and Fall?) of the Patent Troll*, 17 U. Miami Bus. L. Rev. 343, 344 (2009).

[6] Diane Bartz, *Obama urges Congress to pass anti-patent troll bill*, Reuters (Jan. 28, 2014, 9:49 PM), http://www.reuters.com/article/2014/01/29/us-usa-obama-patentidUSBREA0S07V201401 29.

[7] *See* Sam Gustin, *This Is How the Patent Trolls and Trial Lawyers Won*, TIME Mag. (May 24, 2014), http://time.com/111639/patent-reform.

the term while working as an Assistant General Counsel at Intel—a "patent troll" is "someone who tries to make a lot of money off a patent that they are not practicing and have no intention of practicing and in most cases never practiced."[8] Hence, under this definition, "patent troll" is a pejorative way to refer to nonpracticing entities (NPEs), patent assertion entities, patent monetization entities, and patent holding companies.[9] Ironically, Mr. Detkin left Intel to serve as one of the co-founders of Intellectual Ventures, a company that according to his definition is now one of the largest "patent trolls" in the United States.[10]

But what are the characteristics of NPEs? How do they affect the public? Why are they so harshly criticized? Are their critics correct? If so, what are possible solutions to the problem? How have courts and legislatures responded to the issue? This article explores those questions within the context of our hypothetical and examines the role of NPEs in an economy driven by intellectual property.[11] Part II introduces the legal structure in which NPEs operate and presents the arguments advanced by their defenders and critics. Part III explains some of the judicial responses to patent trolls. Part IV considers some of the legislative proposals to deal with the issue. Finally, Part V discusses this author's recommendations.

II. NPEs: Trolls or Dealers?

Under the U.S. Constitution, Congress has the authority to pass laws that "promote the progress of science and useful arts, by securing for a limited time to authors and inventors the exclusive right to their respective writings and discoveries."[12] Under that authority, Congress passed the Patent Act in 1952. As a matter of public policy, the Act sought to promote the public benefits derived from an invention, but also to protect the inventor's rights as a reward for his time, effort, and money.[13] By giving patent owners legal remedies for infringements, the law encourages further innovation through legal incentives.[14] With those policy objectives in mind, to determine if NPEs violate the spirit of the patent system, we must consider whether they have an adverse impact on innovation and the public benefits derived from the inventions.

Broadly speaking, there are two kinds of patent holders: practicing entities and nonpracticing entities.[15] In our hypothetical, Intel is generally a practicing entity because they manufacture products related to their patents. Conversely, Intellectual Ventures is a NPE because they profit from patents by

---

[8] D'Incelli, *supra* note 5, at 343; Todd Klein, *eBay v. MercExchange and KSR Int'l Co. v. Teleflex, Inc.: The Supreme Court Wages War Against Patent Trolls*, 112 Penn St. L. Rev. 295, 296 (2007); *see also* James F. McDonough III, *The Myth of the Patent Troll: An Alternative View of the Function of Patent Dealers in an Idea Economy*, 56 Emory L.J. 189, 192 (2006).

[9] Klein, *supra* note 8, at 295–96; Wagner, *supra* note 1, at 12.

[10] Wagner, *supra* note 1, at 12–14.

[11] McDonough, *supra* note 8, at 190.

[12] U.S. Const. art. I, § 8, cl. 8.

[13] D'Incelli, *supra* note 5, at 351–53.

[14] *Id.*

[15] *See* Colleen V. Chien, *From Arms Race to Marketplace: The Complex Patent Ecosystem and its Implications for the Patent System*, 62 Hastings L.J. 297, 320–32 (2010).

selling them, licensing them, or suing for infringement damages without producing patented products or practicing patented methods. When a NPE—like Intellectual Ventures—asserts a patent claim against entities that are actually engaged in the business of providing products or services—like Intel or Bill's startup—they are sometimes known as patent trolls. Issues associated with patent trolls have drawn attention due to a variety of factors such as: the large amount of cases; defense costs; licensing settlement costs; verdict awards; forum shopping[16]; and the perceived frivolousness of their behavior or claims in some instances.[17] To put these factors into context, let's look at some numbers.

Ninety-seven percent of all patent infringement cases settle before trial.[18] From 1970 to 2004, the number of patents issued annually by the United States Patent and Trademark Office (USPTO) rose from 67,964 to 181,302.[19] Naturally, this led to more patent infringement suits being filed.[20] Of the almost 5,200 patent suits filed in 2012, an estimated 60% of those were brought by NPEs.[21] NPEs frequently target large corporations because they have "deep pockets" and, if found liable for infringement, the damages would likely be higher due to their sales. For example, from 2009–2013 Apple, Inc. was sued for patent infringement 101 times, Samsung 152, HP 150, and AT&T 147.[22]

The median costs of litigating these claims are also quite substantial: $290,000 (discovery) to $500,000 (total) for cases with less than $1 million at risk; $1 million (discovery) to $2 million (total) for cases with $1–$25 million at risk; and $2.5 million (discovery) to $3.9 million (total) for cases with more than $25 million at risk.[23] Estimates indicate that in 2011 troll lawsuits cost the U.S. economy $29 billion

---

[16] NPEs have traditionally preferred to file suit in plaintiff-friendly forums such as the Eastern District of Texas. *See* Brian J. Love & James Yoon, *Predictably Expensive: A Critical Look at Patent Litigation in the Eastern District of Texas*, 20 Stan. Tech. L. Rev. 1, 16–20 (2017) (noting there is some statistical support for the hypothesis that judges and jurors in the Eastern District of Texas are sympathetic to plaintiffs).

[17] Christopher Hu, *Some Observations On The Patent Troll Litigation Problem*, 26 No. 8 Intell. Prop. & Tech. L.J. 10 (2014).

[18] *Id.* at 11.

[19] McDonough, *supra* note 8, at 191.

[20] *See* Sam Gustin, *This Is How the Patent Trolls and Trial Lawyers Won*, TIME Mag. (May 24, 2014), http://time.com/111639/patent-reform (stating that patent troll lawsuits tripled in a span of two years).

[21] *Cf.* Brian Fung, *Patent trolls now account for 67 percent of all new patent lawsuits*, The Washington Post (Nov. 11, 2014, 10:00 PM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/15/patent-trolls-now-account-for-67-percent-of-all-new-patent-lawsuits (explaining NPE's share of all patent lawsuits filed increased from 28% to 67% in just 5 years).

[22] Matthew K. Blackburn, *Address Abusive Patent Litigation by Reducing Innocent Infringement*, 6 Landslide 38, 39 (2014).

[23] Bessen, *supra* note 4, at 2; *see also* Hu, *supra* note 17, at 10–11 ("The median cost of defending a troll case ranges from $1.25 million for cases with $10 million or less at stake, to $2.4 million for cases with $10 to $25 million at stake, to $4 million for cases with $25,000,000 or more at stake.").

in direct losses due to damages awards, attorney fees, and court costs.[24]

The game of patent litigation is certainly costly, and the size and resources of the player makes a big difference. Most of the patents are issued to large entities.[25] And when these large entities go to war they win more often than the little guy. Large-entity plaintiffs win 53.1% of the cases whereas small-entity plaintiffs only win 12.3% of theirs.[26] Whether this result is driven because large entities have better patents or more resources is beside the broader point: Goliath wins most of the times. But where do NPEs fit within the patent litigation world?

A. NPEs as Patent Trolls

Given the costs and macroeconomic implications of the issue, NPE critics contend that patent trolls disrupt the public policy goals of the Patent Act. They call attention to the huge financial losses associated with troll suits,[27] the damaging effects on innovation, and the burdens to the public.[28] They argue trolls diminish innovation by reducing the funds available for research and development, and also burden the public because companies pass on the cost of litigation to consumers by increasing prices.[29] Moreover, critics maintain that notions of fairness support their position.[30] For instance, if Intellectual Ventures sues Intel for patent infringement, who has more leverage? Undoubtedly, Intellectual Ventures' cost-benefit analysis will differ from Intel's.

NPEs appraise patents based on potential damages for infringement, the probability of litigation success, and the likelihood of settling the claim or licensing the technology. Aside from those factors, NPEs also evaluate their patents using revenue projections for products accused of infringement. In addition, unlike NPEs, practicing entities have to weigh the risks to their existing product distribution and manufacturing operations. Because of these inherent differences in their positions, critics assert that the current system gives patent trolls an unfair advantage during pre-trial negotiations, which leads to abusive behavior and frivolous claims.[31]

NPEs have also been criticized particularly strongly when they attempt to assert patent infringement

---

[24] Gustin, *supra* note 20; Adina Sivaraman, *The Shield Act: A Good Attempt at Curbing Patent Trolls That Leaves Us Wanting More*, 7 J. Bus. Entrepreneurship & L. 209, 210 (2013).

[25] Bessen, *supra* note 4, at 12 (71% of patents issue to large firms).

[26] John R. Allison et. al., *Patent Quality and Settlement Among Repeat Patent Litigants*, 99 Geo. L.J. 677, 690 (2011).

[27] The financial losses argument focuses on the costs that practicing entities bear by: paying for attorney fees that they can rarely recover even if they win; the court costs associated with litigation, including hiring experts to testify about the technology/product; the lost profits they might incur if they have to halt production or sales in light of the suit in order to minimize possible awards; and the damages paid to the defendants if the suit is unsuccessful.

[28] David Lee Johnson, *Facing Down the Trolls: States Stumble on the Bridge to Patent-Assertion Regulation*, 71 Wash. & Lee L. Rev. 2023, 2031–33 (2014).

[29] Blackburn, *supra* note 22, at 40.

[30] Klein, *supra* note 8, at 296.

[31] D'Incelli, *supra* note 5, at 347–48.

claims against end-users instead of manufacturers.[32] For example, let's imagine Bill owns a coffee shop and offers free Wi-Fi services to his customers through a router made by Intel. If Intellectual Ventures asserts that the router made by Intel infringes on their patent, should they be allowed to sue Bill? End-users and customers are vulnerable against patent trolls since they typically lack the resources to adequately consider the validity of the threats or defend themselves. Hence, there has been an overwhelming movement to restrict this kind of behavior. In fact, even State governments have stepped in and enacted laws to impede NPEs from going after end-users before there is a final judgment against the infringing manufacturers.[33]

B. NPEs as Patent Dealers

Despite the heavy criticism against patent trolls, some argue that NPEs are actually beneficial to society. To illustrate, let's go back to our hypothetical. If Bill had received the demand letter from Intel instead of Intellectual Ventures, would he be better off? Not really. In fact, he might be in a worse position. Bill would still have to consider all the same costs and risks of defending the claim, yet not have the option to settle for a license. While NPEs have strong incentives to license their patent portfolio because they do not sell products, competing practicing entities such as Intel might decide it is best to enjoin Bill's startup all together to protect its market share and projected revenues. In other words, Intel might decide it is better to drive Bill out of business rather than offering him a license. So how do NPEs help people like Bill?

One view is that NPEs perform a valuable market-making function that appreciates the value of patents and promotes innovation.[34] They see the NPE business model simply as a natural step in the progression to an idea economy.[35] Having companies such as Intellectual Ventures in the market increases the demand and transferability of patents while providing a new revenue source for people like Bill. In this way, NPE's role as patent dealers,[36] as opposed to trolls, serves as a valuable option for individuals who may lack the resources to effectively commercialize their patents, which in turn enhances the liquidity and worth of patents as assets.[37]

Accordingly, by giving independent inventors leverage against infringing large corporations, NPEs help the patent market work more efficiently.[38] For example, if Intel infringes on Bill's patent instead, and Bill makes a demand, Intel could assess the risks and conclude that he poses no real threat of litigation given his financial position. This causes a market failure because if independent inventors

---

[32] Johnson, *supra* note 28, at 2032–33.

[33] *See infra* Part IV.B.

[34] Robert P. Merges, *The Trouble with Trolls: Innovation, Rent-Seeking, and Patent Law Reform*, 24 Berkeley Tech. L.J. 1583, 1599 (2009).

[35] McDonough, *supra* note 8, at 189.

[36] *Id.* at 200.

[37] Wagner, *supra* note 1, at 19; *see also* McDonough, *supra* note 8, at 205–20.

[38] McDonough, *supra* note 8, at 205–20.

cannot realistically protect their property rights and recoup their investment costs, it creates inconsistencies between the incentives of market participants, which could stagnate growth and innovation.[39] However, if Bill sells his patent to Intellectual Ventures, effectively assigning them his right to sue, he would receive compensation for his invention from Intellectual Ventures, which in turn is better positioned to assert a valid claim given its resources and expertise. The role of NPEs as patent dealers alleviates this market failure because a claim made by Intellectual Ventures creates a credible threat of litigation for Intel. This in turn promotes innovation since it allows Bill to receive money for his first patent and move on to create other inventions. Finally, NPE defenders also contend that there is no legitimate reason to legally discriminate between a firm that embeds its innovation in manufactured products, and one that sells its innovations in disembodied form—a pure idea shop.[40]

III. The Courts

A. Injunctions

In asserting patent infringement claims, the right of exclusion granted through injunctive orders is one of the most powerful patent remedies that can be imposed against an infringer.[41] The Patent Act authorizes courts to grant injunctions "in accordance with the principles of equity to prevent the violation of any right secured by patent, on such terms as the court deems reasonable."[42] Let's go back to one of our hypothetical examples, if Intellectual Ventures sues Intel for patent infringement and wins, would the court issue a permanent injunction? The case of *eBay v. MercExchange* helps us answer this question.[43]

In *eBay*, the jury originally ordered eBay to pay MercExchange (a NPE) $29.5 million in damages for a patent infringement claim regarding eBay's "Buy It Now" feature.[44] Up to this point in time, courts had recognized a presumption favoring permanent injunctions in patent cases. However, in this case, the district court employed the traditional four-factor test governing requests for injunctive relief, and declined to grant one.[45] On appeal, the Federal Circuit granted the injunction, but the Supreme Court reversed the decision and remanded the case. In a unanimous decision, the Supreme Court dismissed the general presumption rule and established the standard for obtaining permanent injunctions against a defendant in patent cases.[46] Under the four-factor test, courts consider: (1) whether the plaintiff would face irreparable injury; (2) whether the plaintiff has remedies available at law to compensate for the injury; (3) whether an injunction would further public interests;

---

[39] *See id.*

[40] Merges, *supra* note 34, at 1599.

[41] McDonough, *supra* note 8, at 197 (arguing that limiting the right to exclude could weaken the foundation of the U.S. economy).

[42] D'Incelli, *supra* note 5, at 352.

[43] *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006).

[44] *eBay*, 547 U.S. 388.

[45] *eBay*, 547 U.S. 388.

[46] John M. Golden, *"Patent Trolls" and Patent Remedies*, 85 Tex. L. Rev. 2111, 2113–15 (2007).

and (4) whether the balance of hardships between the plaintiff and defendant warrants an injunction.[47]

The *eBay* decision significantly impaired a NPE's ability to obtain a permanent injunction under the new test.[48] In a concurring opinion, Justice Kennedy argued injunctions should not be granted when "firms use patents not as a basis for producing and selling goods, but, instead, primarily for obtaining licensing fees."[49] Accordingly, post-*eBay* decisions reflect the emergence of a market competition requirement where it is practically necessary to commercialize the patent in the marketplace in order to obtain an injunction.[50] Because NPEs now have an extra legal hurdle to overcome, injunction threats from NPEs are no longer as effective against practicing entities, thereby altering pre-trial leverage dynamics. As a result, in our example, if Intellectual Ventures won the suit it would likely receive a damage award or license without an injunction.

B. Fee Shifting

Given the high costs of patent litigation and the alleged frivolousness of some infringement claims, it is not surprising that shifting attorney fees is a big concern in this area. Under § 285 of the Patent Act: "The court in exceptional cases may award reasonable attorney fees to the prevailing party."[51] Two recent Supreme Court decisions considered the meaning of this section and replaced some of the rules previously set out by the Federal Circuit.

First, in *Octane Fitness v. Icon Health and Fitness*, the court clarified its interpretation of what qualifies as an "exceptional" case. Before *Octane Fitness*, the Federal Circuit interpreted "exceptional" narrowly, meaning instances where suit is "so unreasonable that no reasonable litigant could believe it would succeed."[52] The defendant had to prove these elements with clear and convincing evidence. Under the *Octane Fitness* standard, an "exceptional" case refers to one that "stands out from others in the weakness of a party's litigating position, or in the unreasonable manner in which the case was litigated."[53] Second, in *Highmark Inc. v. Allcare Health Management System*, the court limited the power to review fee awards on appeal.[54] *Highmark* took away the Federal Circuit's discretion to consider fee-shifting appeals de novo and restricted it to an abuse of discretion standard.[55]

Combined, *Octane Fitness* and *Highmark* expanded the discretion of district courts to award attorneys' fees and decreased the possibility that such decisions will be overturned. This seems to be a judicial response to lower the amount of abusive litigation by increasing the risks of asserting a frivolous claim.

---

[47] *eBay*, 547 U.S. at 391–93.

[48] Golden, *supra* note 46, at 2113–15.

[49] *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 395–97 (2006) (Kennedy, J., concurring).

[50] Golden, *supra* note 46, at 2113–15; *see also* Benjamin H. Diessel, *Trolling for Trolls: The Pitfalls of the Emerging Market Competition Requirement for Permanent Injunctions in Patent Cases Post-eBay*, 106 MICH. L. REV. 305, 309–10 (2007).

[51] 35 U.S.C. § 285 (1952).

[52] *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749 (2014); *see also* Steven Seidenberg, *Troll Alert Federal Circuit Gets Reined in over Patent Fees in Infringement Suits*, A.B.A. J., July 2014, at 19.

[53] *Octane Fitness*, 134 S. Ct. at 1749.

[54] *Highmark Inc. v. Allcare Health Mgmt. Sys., Inc.*, 134 S. Ct. 1744 (2014).

[55] *See id.*

C. Venue

Under 28 U.S.C. § 1400(b), patent infringement actions "may be brought [1] in the judicial district where the defendant resides, or [2] where the defendant has committed acts of infringement and has a regular and established place of business."

For nearly 30 years, under the Federal Circuit's precedent, corporations were deemed to reside in "any judicial district in which it is subject to personal jurisdiction."[56] Since patent infringement cases typically involve products sold around the country, this meant that corporations were considered to reside nearly anywhere. This, in turn, allowed plaintiffs to file suit in plaintiff-friendly forums such as the Eastern District of Texas. That is, forums where cases proceeded to trial often and where plaintiffs tend to win large damage awards.[57]

But recently, the Supreme Court addressed venue for patent cases in what could be viewed as an attempt to curb forum shopping. In *TC Heartland LLC v. Kraft Foods Grp. Brands LLC*, the Supreme Court rejected the Federal Circuit's precedent and held that a corporation resides only in its state of incorporation.[58] While *TC Heartland*'s holding is a significant blow to forum shopping, its overall impact remains uncertain as courts now turn to the scope of § 1400(b)'s "regular and established place of business" prong.[59]

IV. The Federal and State Governments

In an effort to reduce the negative effects of abusive litigation by patent trolls, several suggestions have been advanced both at the Federal[60] and State level. In 2011, Congress enacted the America Invents Act (AIA). Concerned by frivolous assertions, the Act limited the joinder of defendants[61] and changed

---

[56] *VE Holding Corp. v. Johnson Gas Appliance Co.*, 917 F.2d 1574, 1578–80 (Fed. Cir. 1990) *abrogated by TC Heartland LLC v. Kraft Foods Grp. Brands LLC*, 137 S. Ct. 1514 (2017) (holding that 28 U.S.C. § 1391(c), as amended, applied to § 1400(b) and therefore redefined the meaning of the term "resides.").

[57] Love, *supra* note 16, at 16–20 (noting the Eastern District of Texas is statistically less likely to grant motions to transfer or motions for summary judgment in defendants' favor, so cases are disproportionally more likely to go to trial and result in a favorable outcome for the patentee).

[58] 137 S. Ct. 1514, 1520 (2017).

[59] In *Raytheon Co. v. Cray, Inc.*, No. CV 2:15-CV-01554-JRG, 2017 WL 2813896, at *7–14 (E.D. Tex. June 29, 2017) (Gilstrap, J.), the court attempted to provide guideposts to examine the venue analysis under the "regular and established place of business" prong. In doing so the court noted four non-dispositive factors: (1) physical presence; (2) defendant's representations; (3) benefits received; and (4) targeted interactions with the district. *Id.* After considering these factors the court found that defendant had a regular and established place of business in the Eastern District of Texas and, therefore, denied its motion to transfer venue. *Id.* at *14.

[60] *See generally, Patent Progress's Guide to Federal Patent Reform Legislation*, PatentProgress.org, http://www.patentprogress.org/patent-progress-legislation-guides/patent-progresss-guide-patent-reform-legislation/#Innovation (last visited July 9, 2017) (outlining different bills introduced to Congress to deal with some aspects of the patent troll issue).

[61] Before the AIA patent trolls sued multiple companies in a single lawsuit on the ground that deciding the scope of the patent was enough to join defendants together, even if the acts of infringement were unrelated. Robin Feldman, Tom Ewing, Sara Jeruss, *The AIA 500 Expanded: The Effects of Patent Monetization Entities*, UCLA J.L. & Tech., Fall 2013, at 1, 43.

the standard of review for business-method patents.[62] This limited a patent troll's ability to aggregate defendants, but trolls adapted by filing multiple individual suits. Next, we examine the impact of two different types of statutes, one at the federal level and the other at the state level.

A. The Innovation Act

The Innovation Act is one of the federal legislative proposals aimed at reducing abusive patent troll litigation by seeking to reform the rules for fee shifting, pleadings, and discovery.[63] The Act was introduced to Congress in 2013 and again in 2015, but failed to become law on both occasions. Though the Act has not been reintroduced since then, its proposed changes are nonetheless worth examining as it was one of the most ambitious legislative attempts to address patent trolls. Overall, the Act sought five significant changes.

First, it sets stricter pleading requirements.[64] At the time the Act was introduced, plaintiffs only had to identify the infringed patent and give a general description of the infringing actions by the defendant.[65] Under the proposed Act, a complaint would have to include, *inter alia*, "asserted claims, accused products, all theories of direct and indirect infringement; standing to assert [the patent]; principal business of party alleging infringement; prior litigation involving the [patent], [and] any licensing term or pricing commitment for the [patent]."[66] Because trolls commonly purchase broad and vaguely written patents to assert general complaints, this would have foreseeably decreased baseless claims by raising the level of specificity required in complaints.[67]

Second, the Innovation Act would replace the standard for shifting attorney fees.[68] As noted in the analysis of *Octane Fitness* and *Highmark* above, courts only shift legal fees in exceptional cases. The proposed Act establishes a general rule that awards legal fees to the prevailing party unless the court determines there are substantial justifications or special circumstances warranting an exception. This loser-pays type of solution is popular among lobbyists and academics because it modifies the economics of

---

[62] Wagner, *supra* note 1, at 16; Johnson, *supra* note 28, at 2053.

[63] *See Patent Progress's Guide to Federal Patent Reform Legislation*, PatentProgress.org, http://www.patentprogress.org/patent-progress-legislation-guides/patent-progresss-guide-patent-reform-legislation/#Innovation (last visited July 9, 2017).

[64] *See* Innovation Act, H.R. 9, 114th Cong. § 3(a) (2015), https://www.congress.gov/114/ bills/hr9/BILLS-114hr9rh.pdf.

[65] *Law applied in patent infringement actions*, 6 Pat. L. Fundamentals § 20:121 (2d ed.).

[66] *See id.*

[67] Before 2015, the Federal Circuit had held that Form 18 in the Appendix of Forms of the Rules of Civil Procedure controlled in the event of a conflict in pleading requirement between the Form and *Twombly* and *Iqbal*. *See K-Tech Telecomm., Inc. v. Time Warner Cable, Inc.*, 714 F.3d 1277, 1283 (Fed. Cir. 2013). But changes to the Federal Rules of Civil Procedure, which took effect on December 1, 2015, abrogated Form 18. *Lyda v. CBS Corp.*, 838 F.3d 1331, 1337 n.2 (Fed. Cir. 2016).

[68] *See* Innovation Act § 3(b), *supra* note 64.

the system to further deter weak claims. But the downside is that such a rule might be overly inclusive and have an unintended chilling effect on otherwise valid assertions of patent infringement.

Third, the Act limits the scope of discovery.[69] Currently, courts grant discovery requests based on whether they are relevant to the cause of action. The Act seeks to constrain the scope of discovery in cases where the court has not ruled on claim construction. In those situations, it would permit requests only pertaining to information necessary to consider the meaning of the terms in the patent. Overall, because practicing entities actually make products and are directly engaged in the business they are more likely to have more documents to produce, thus making discovery requests more costly to practicing entities than they are for NPEs. Hence, this change attempts to alleviate some of those financial burdens.

Fourth, the Act expands the kind of information that must be disclosed.[70] The Act essentially provides that any entities with a financial interest in the patent must be disclosed. This information can be important as it helps ascertain the motivations behind an assertion and the level of due diligence exerted by a plaintiff in investigating the validity of its infringement claim. For example, let's say Intellectual Ventures sues Intel for patent infringement. If Intellectual Ventures was required to disclose that it has a licensing agreement with IBM—one of Intel's competitors—this could affect how Intel decides to respond. As a result, this requirement furthers ownership transparency by limiting the type of information that NPEs can withhold about their patent rights.

Lastly, the Act adds an end-user exception.[71] Patent trolls have been heavily criticized for suing customers that purchase products from manufacturers that allegedly infringe on the troll's patent. This proposal would stay actions against the end users until a decision against the infringing manufacturer is made.[72] It would also bind the end-users to the court's rulings with respect to the common issues between end users and the manufacturers.

---

[69] *See* Innovation Act § 3(d), *supra* note 64.

[70] *See* Innovation Act § 4, *supra* note 64.

[71] *See* Innovation Act § 5, *supra* note 64.

[72] Notably, courts routinely stay customer suits until the action against the manufacturer has been resolved. *Spread Spectrum Screening LLC v. Eastman Kodak Co.*, 657 F.3d 1349, 1357 (Fed. Cir. 2011) (explaining the customer-suit exception and pointing out that the guiding principles of the exception are efficiency and judicial economy).

B. State's efforts — Vermont

A common patent troll tactic involves sending multiple identical letters to small entities threatening litigation.[73] These letters generally make vague claims and offer licensing terms that would cost less than defending the lawsuit, all while cautioning that if payment is not received by a certain date, suit will follow. State governments seem to be particularly concerned with the use of these bad faith demand letters[74] by patent trolls and have enacted statues to deal with the issue. Federal district courts have "original jurisdiction of any civil action arising under any act of congress relating to patents, plant variety protection, copyrights, and trademarks."[75] Consequently, any State legislative action in this specific area of the law will have to deal with supremacy and federalism issues to ensure it doesn't interfere with Congressional jurisdiction to regulate the patent system.

The first State to venture into this domain and prohibit bad faith patent assertions was Vermont.[76] Fourteen other States followed and passed their own legislation based on Vermont's statute. These kinds of laws essentially test the distinction between a patent holder's right to exclude others from infringing its patents and a State's obligation to protect consumers. One is entirely under the purview of Congress while the other is akin to tort law. Hence, to determine a State's authority to regulate NPEs demand letters mailing campaigns, we must distinguish whether they are considered legal uses of patent rights or abusive business practices.[77]

Under the supremacy clause of the United States Constitution, if a state law is "opposed to, or inconsistent with, any constitutional power which Congress has exercised, then, so far as the incompatibility exists, the [state law] is nugatory and void, necessarily, and by reason of the supremacy of the law of Congress."[78] The Patent Act preempts any state laws that are inconsistent with it, however, the Federal Circuit did not find that Congress intended to occupy the field of state unfair competition law.[79] This expresses a view that the Patent Act regulates the field of granting patents, whereas state unfair competition laws pertain to commercial marketplace interactions, such as bad-faith patent assertions.

Broadly speaking, the goal behind general consumer protection laws is to protect the public by encouraging fair and honest competition. Vermont's statute provides that a "person shall not make bad faith assertion of patent infringement." To uphold those policies, the law gives the state attorney general the

---

[73] Hayden W. Gregory, *States Go After Patent Trolls-How Far Can They Go?*, 6 Landslide 2 (2014).

[74] A problem with the behavior exhibited by some of these demands letters pertains to the fact that NPEs will sometimes engage in mass mailing campaigns by sending multiple letters to a vast array of defendants. This is specifically troublesome to states when they are directed to end-users because they view it as NPEs using the economies of scale to exert undue pressure on individuals who are particularly vulnerable to cave into their demands due to their limited resources.

[75] 28 U.S.C. § 1338 (2011).

[76] Eric Goldman, *Vermont Enacts The Nation's First Anti-Patent Trolling Law*, Forbes (May 22, 2013, 2:22 PM), http://www.forbes.com/sites/ericgoldman/2013/05/22/vermont-enacts-the-nations-first-anti-patent-trolling-law/.

[77] Johnson, *supra* note 28, at 2026–27.

[78] *Gibbons v. Ogden*, 22 U.S. 1, 30 (1824).

[79] Johnson, *supra* note 28, at 2043.

authority to bring actions under a nonexclusive list of eight factors to determine if there was bad faith.[80] Let's examine those statutory factors in more detail to consider their impact.

> (1) The demand letter does not contain the following information: (A) the patent number; (B) the name and address of the patent owner or owners and assignee or assignees, if any; and (C) factual allegations concerning the specific areas in which the target's products, services, and technology infringe the patent or are covered by the claims in the patent.[81]

The logic behind this factor is similar to the one we encountered in the Innovation Act provision strengthening the pleading requirements.[82] That is, the statue seeks to encourage the disclosure of enough information for defendants to properly assess the validity of the claim before they decide whether to litigate or settle.

> (2) Prior to sending the demand letter, the person fails to conduct an analysis comparing the claims in the patent to the target's products, services, and technology, or such an analysis was done but does not identify specific areas in which the products, services, and technology are covered by the claims in the patent."[83]

While the first factor looks at whether there was sufficient information provided in the demand letter, this factor concentrates on whether a plaintiff undertook a diligent examination of the infringement claim *before* sending the letter. In other words, it looks at what the plaintiff did to reach the conclusion that the defendant infringed his patent.

> (3) The demand letter lacks the information described in subdivision (1) of this subsection, the target requests the information, and the person fails to provide the information within a reasonable period of time.[84]

This essentially seeks to promote disclosure of information when requested by a defendant. For example, let's suppose Intellectual Ventures sends a demand letter to Bill that doesn't include the information outlined in factor number one. If Bill requests the information and does not receive it, it may support an inference that Intellectual Ventures failed to perform the analysis required by the second factor.

---

[80] Vt. Stat. Ann. tit. 9, § 4197 (2013).
[81] Vt. Stat. Ann. tit. 9, § 4197(b)(1) (2013)
[82] *See supra* Part IV.A.
[83] Vt. Stat. Ann. tit. 9, § 4197(b)(2) (2013).
[84] Vt. Stat. Ann. tit. 9, § 4197(b)(3) (2013).

> (4) The demand letter demands payment of a license fee or response within an unreasonably short period of time.[85] [And] (5) The person offers to license the patent for an amount that is not based on a reasonable estimate of the value of the license.[86]

Essentially these two factors consider whether the timing and the amount implicated in the demand letters are reasonable. Although there is some value in weighing these components to reach a broader conclusion that there was bad faith, I believe they encroach on a party's freedom to negotiate. The fact that a party exercises leverage through tight deadlines or high premiums does not necessarily indicate frivolousness. In a capitalist economy, patent owners should be allowed to maximize value through savvy negotiation techniques.

> (6) The claim or assertion of patent infringement is meritless, and the person knew, or should have known, that the claim or assertion is meritless.[87]

Out of all the factors laid out by the statute, this is the most analogous to the current standard laid out by the courts for fee shifting.[88] According to the Federal Circuit, "if the patentee knows that the patent is invalid, unenforceable, or not infringed, yet represents to the marketplace that a competitor is infringing on the patent, a clear case of bad-faith representation is made out."[89] Therefore, if this statute is subjected to further review by the courts, this factor could survive the pre-emption review if viewed as merely adopting the federal standard in the context of consumer protection, or it might fail if there is a desire to keep this area exclusively in the realm of federal jurisdiction.

> (7) The claim or assertion of patent infringement is deceptive.[90]

Because the Vermont legislature did not define the meaning of "deceptive," courts have to rely on their interpretations of deception according to their decisions in the context of consumer protection. This is problematic because conceivably there is a difference between (a) misleading consumers with respect to the products that they are buying, and (b) deceiving defendants through litigation or demand letters. The two are different concepts to the extent that one generally relates to what a product can do while the other focuses on legal determinations regarding the scope of a patent.

---

[85] Vt. Stat. Ann. tit. 9, § 4197(b)(4) (2013).
[86] Vt. Stat. Ann. tit. 9, § 4197(b)(5) (2013).
[87] Vt. Stat. Ann. tit. 9, § 4197(b)(6) (2013).
[88] *See supra* Part III.B.
[89] *Zenith Elecs. Corp. v. Exzec, Inc.*, 182 F.3d 1340, 1354 (Fed. Cir. 1999).
[90] Vt. Stat. Ann. tit. 9, § 4197(b)(7) (2013).

> (8) The person or its subsidiaries or affiliates have previously filed or threatened to file one or more lawsuits based on the same or similar claim of patent infringement and: (A) those threats or lawsuits lacked the information described in subdivision (1) of this subsection; or (B) the person attempted to enforce the claim of patent infringement in litigation and a court found the claim to be meritless.[91]

In short, this factor asks the court to consider previous filings or threats to sue, which could have mixed results. On one hand, it could help establish a pattern of behavior that assists courts in determining that the claimant possessed the necessary mens rea of bad faith. On the other hand, the fact that a plaintiff raised similar claims against another party does not automatically discredit their current claim and could result in unfair prejudice. For example, the rules of evidence generally exclude settlement offers from being introduced at trial because they consider them to be too prejudicial.[92] Although this evidentiary rule deals with settlement offers made to the party involved in the suit and does apply to offers made in other lawsuits, it does illustrate the point that allowing an individual to introduce settlement offers brings considerable weight.

And lastly, "(9) Any other factor the court finds relevant."[93] Evidently, this last factor is a catch-all provision that gives courts perhaps too much flexibility to weigh other elements that they find persuasive.

V. Recommendations

It can hardly be contested that patent infringement suits are complicated, costly, and have a significant impact on innovation. Although the term "patent troll" has been used as a synonym for NPEs, I believe it is important to distinguish the two.[94] That is, we should start concentrating on patent trolls as those who engage in a type of abusive/frivolous behavior and not just as a blanket term to refer unfavorably to all NPEs. As discussed in Part II, NPEs can serve a valuable role in the marketplace that actually promotes innovation and levels the playing field between large corporations and independent inventors or small entities. Since NPEs are not intrinsically harmful[95] to our economy, I believe the core issue is the bad faith assertion of frivolous patent infringement claims by owners of weak patents. Below I offer my recommendations for tackling the problems at the heart of the patent troll controversy.

---

[91] Vt. Stat. Ann. tit. 9, § 4197(b)(8) (2013).

[92] *Cf.* Fed. R. Evid. 408.

[93] Vt. Stat. Ann. tit. 9, § 4197(b)(9) (2013).

[94] Merges, *supra* note 34, at 1614 (2009) (concluding that we must delineate troll activity more precisely and shut it down through the courts).

[95] Blackburn, *supra* note 22, at 39.

First, we should increase the resources of the USPTO to reduce the possibility that weak patents are granted. Currently, most of the proposed solutions to the issue focus on demand letters and the litigation procedures. While I recognize this is important, I submit that we should also pay more attention to solutions aimed at the USPTO's examination process during the patent-granting stage. Since critics argue that part of the problem is that patent trolls seek out broad and vaguely written patents to extort licensing fees or royalties from companies under a threat of a patent infringement suit, it seems logical to spend more time ensuring that the patents being granted are less likely to be invalidated. Although this would increase administrative costs, it should also reduce the overall toll of patent infringement suits on our economy.

Second, we should heighten the level of specificity required in the pleadings for patent infringement claims. Specifically, we should require early disclosure of claim construction arguments[96] and not just infringement contentions. As discussed in the analysis of the Innovation Act[97] and the Vermont statute,[98] legislative proposals are keen to amend the law to demand more information from plaintiffs who claim their patent has been infringed. This additional disclosure is encouraged because it would allow defendants to properly assess the validity of a claim and perhaps decide it is best to settle. Similarly, this would also permit courts to determine more accurately whether the plaintiff has indeed established a prima facie case for patent infringement against the defendant.

Third, courts should shift the cost of attorney fees more often by enforcing Rule 11 and the exceptional case provision with more flexibility. Rule 11 provides that:

> by presenting to the court a pleading, written motion, or other paper . . . an attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances: (1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; (2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law; (3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and (4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.[99]

---

[96] By requiring claim construction arguments to be provided early in the process, courts can consider how each party understands the areas covered by their patents and thus rule on summary judgment motions more often which would reduce litigation costs.

[97] *See supra* Part IV.A.

[98] *See supra* Part IV.B.

[99] Fed. R. Civ. P. 11(b).

In addition, the Patent Act states that "the court in exceptional cases may award reasonable attorney fees to the prevailing party."[100] Taken together, these rules give judges the authority to shift the cost of litigation to the patent troll so that the trolls would have to consider additional risks when engaging in abusive litigation tactics. This should further discourage trolls from filing frivolous lawsuits merely to extract unreasonable licensing fees or royalties.[101]

Lastly, Congress should enact an end-user or consumer exception. In this regard, I agree with the provision examined in our overview of the Innovation Act, which stays litigation against end-users until the patent infringement claim is resolved with the manufacturer of the product. End-users or consumers are the most vulnerable to threats of litigation as they lack the knowledge or financial resources to consider the validity of a patent infringement claim. The rights of a patentee are not unduly diminished by requiring that they sue the entity who makes the product before being able to bring claims against end-users. As result, the public benefits of this end-user exception are high whereas the burden on patent owners is minimal.

Overall, it is clear that bad faith assertions of patent infringement claims have a significant economic impact; and patent owners are divided on the issue. On one side, we have practicing entities like Intel, which are manufacturing, pharmaceutical, or technological companies. And on the other side, we have NPEs, such as Intellectual Ventures, which can be independent inventors, universities, or simply companies that monetize their patent portfolio primarily through royalties and licenses. With these two kinds of patent owners in mind, caution must be practiced in making distinctions between the types of hurdles, standards, and remedies that are applicable to one or the other.[102] A patent entitles the holder to certain property rights that I believe should not be constrained according to how a patent is monetized. By extension, I submit that Justice Kennedy's concurring opinion in the *eBay* case could lead to a slippery slope of placing too much emphasis on whether the owner is competing in the market.[103] I highlight my first recommendation because it aims to solve issues dealing with patent ownership before the ownership rights accrue. In other words, by allocating more resources towards enhancing the patent application/examination process, we can proactively try to prevent the problem before it arises. This would also be neutral and make no distinctions between entities because it deals with a party who is in the process of applying to obtain patent ownership rights instead of enforcing them.

Lastly, we should be mindful of making changes that are too sweeping because the market has ways of adapting and evolving. The United States' intellectual property laws are some of the most reliable in the world, and we should explore ways to refine and harness that market. In fact, with the rise of patent trolls, we have seen the market adapt through an increase in patent portfolio defense and insurance

---

[100] 35 U.S.C. § 285 (1952).

[101] Patents are presumptively valid. So it is important to recognize that identifying whether a lawsuit is frivolous is not always an easy task.

[102] *But cf. eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 395–97 (2006) (Kennedy, J., concurring) (expressing an opinion that only market competitors should be granted permanent injunctions as a remedy in patent infringement cases; and that NPEs are adequately compensated with licensing fees because that's what their business model relies on).

[103] *Id.*

strategy.[104] The idea for patent portfolio defense and insurance is simple: if you have more patents at your disposal then you have a better chance to find one that trumps your opponent's claims.[105] Let's say Bill has this type of insurance[106] and is sued by Intellectual Ventures. Because patent infringement suits are decided according to the actual claims made in the patent, Bill could go to his insurance company and search for patents that he could then use as evidence in trial to prove the invalidity of the patents at issue in the case. For example, Google and Apple pay to have access to any of RPX's 4,900 patents to defend themselves by being able to use the patents for counterclaims. Although the payment for access to that portfolio is made with a defensive strategy, it can have the collateral benefit of encouraging innovation as the company now has a whole new addition of inventions or patents it is allowed to use.

Ultimately, I conclude that proposed solutions should focus on improving the patent examination system before they are granted and combatting patent trolls as a type of behavior—not just merely through distinctions according to how patent owners profit from their patents.

---

[104] *See e.g.,* Reed Albergotti, *For Startups Afraid of Patent Trolls, Insurance,* The Wall St. J. (Nov. 10, 2014, 8:00 AM), http://blogs.wsj.com/digits/2014/11/10/for-startups-afraid-of-patent-trolls-insurance (noting that there are companies like RPX which are dedicated to buying patents and licensing them to deter suits; and explaining that even startups now have the option to pay yearly affordable premiums to get access to their large portfolio).

[105] *See e.g.*, Debra Brubaker Burns, *Titans and Trolls Enter the Open-Source Arena*, 5 Hastings Sci. & Tech. L.J. 33, 76 (2013) (discussing how certain organizations have joined the Open Invention Network to pool their patents offensively against litigation that is brought against Linux software).

[106] Keep in mind that these "insurance" companies are generally entities that license their large patent portfolio to other companies who want to have access to those patents to serve as ammunition if a lawsuit arises.

Patents, Food Science and Veganism

BY KIMBERLY PFLUG-RODRIGUEZ

The innovative nature of cuisine has benefited from strong patent protections. The United States Patent & Trademark Office ("USPTO") has granted various utility patents as methods or compositions of matter for all types of food innovations. But recent changes in the food market may present a new challenge when it comes to protecting food innovation: veganism.

Vegan food companies stand to gain strong legal protections through patent law if they are able to satisfy the non-obviousness requirement: likely the most difficult requirement for food innovators to overcome. Altering or utilizing methods or compositions found in non-vegan foods to produce vegan food alone would not satisfy the non-obviousness hurdle.

Food-patent owners have experienced invalidations of their patents on obviousness grounds when they have tried to enforce those patents. And in their limited success, food-patent owners have often had to demonstrate that they are highly innovative or that they have produced "unexpected results."[1]

Food Patents

A patent is a form of intellectual property protection that "gives its owner the right to exclude others from making, using, offering to sell, selling, or importing the patented invention."[2] Patents are protected by federal law under the authority of the Intellectual Property clause to the United States Constitution, Article I, Section 8, clause 8.[3] Accordingly, the purpose of a patent is to serve the public interest in promoting the progress of science and the useful arts.[4]

The USPTO has designated a specific class for food inventions titled "Patent Class 426 Food or Edible Material: Processes, Compositions, and Products."[5] The most common type of patent protection for food is a utility patent, which may protect food inventions as "a process or composition of matter."[6] A utility patent for a food invention must satisfy the novelty and non-obviousness requirements that are applicable to all patents. To meet the novelty requirement, the food innovation must not have been disclosed or known to the public before the applicant's filing date.[7] If a food innovation has previously been disclosed or sold to the public, the food innovation would not meet the novelty requirement. To meet the non-obviousness requirement, a food innovation would have to be "nonobvious to a hypothetical person of ordinary skill in

---

[1] Chris Mayes, What Users Say About PatentEase Software What Users Say About PatentEase Software, http://store.inventorprise.com/content_articles.php?id=1049 (last visited Aug 14, 2017).

[2] Patent: Overview, Practical Law Practice Note Overview 8-509-4160

[3] *Id.*

[4] *Id.*

[5] Class Definition for Class 426 - FOOD OR EDIBLE MATERIAL: PROCESSES, COMPOSITIONS, AND PRODUCTS, Class Definition for Class 426 - FOOD OR EDIBLE MATERIAL: PROCESSES, COMPOSITIONS, AND PRODUCTS, https://www.uspto.gov/web/patents/classification/uspc426/defs426.htm (last visited Aug 14, 2017).

[6] Morgan P. Arons, *A Chef's Guide to Patent Protections Available for Cooking Techniques and Recipes in the Era of Postmodern Cuisine and Molecular Gastronomy*, 10 J. Bus. & Tech. L. 137 (2015)

[7] Patent: Overview, Practical Law Practice Note Overview 8-509-4160

the technical field of the invention."[8] Compositions of matter patent claims cover the different ingredients or compounds used to make a food.[9] Process patent claims are the different steps or methods used to make the food. [10]

The Growing Vegan Market

According to the vegan society, veganism is "a way of living which seeks to exclude, as far as is possible and practicable, all forms of exploitation of, and cruelty to, animals for food, clothing or any other purpose."[11] A steady increase in demand for vegan food is resulting in dramatic innovation in the vegan food market. In the UK, vegan food sales increased 1,500% in 2016.[12] In 2016, the number of Google® searches for the word "vegan" reached an all-time high with the United States among the top contributors.[13] With the rise of veganism, we also see decrease in the market for red meat. According to the most recent USDA statistics, red meat consumption declined by 25% in 2012 and continues to decline.[14] Dairy sales have also been steadily declining as dairy consumption has decreased 40% since 1970.[15] In 2016, the U.S. government "bailed out" the dairy industry by buying $20 million worth of cheese with taxpayer dollars.[16] These statistics seem to confirm the notion that Americans are steadily transitioning their meat and dairy based diets to a more plant-based one.[17]

There are numerous reasons why people are adopting a plant-based diet, including environmental, health and ethics concerns. The environmental impact of adopting a plant-based diet is evident in the rise of greenhouse gas emissions. The meat and dairy industry is responsible for 51% of "all worldwide

---

[8] *Id.*

[9] Morgan P. Arons, *A Chef's Guide to Patent Protections Available for Cooking Techniques and Recipes in the Era of Postmodern Cuisine and Molecular Gastronomy*, 10 J. Bus. & Tech. L. 137 (2015)

[10] *Id.*

[11] Definition of veganism, The Vegan Society, https://www.vegansociety.com/go-vegan/definition-veganism (last visited Aug 14, 2017).

[12] Vegan Food Sales up by 1,500% in Past Year, Rise of the Vegan, http://www.riseofthevegan.com/blog/vegan-food-sales-up-by-1-500-in-past-year (last visited Aug 14, 2017).

[13] Google Searches for 'VEGAN' Have Never Been Higher, Rise of the Vegan, http://www.riseofthevegan.com/blog/google-searches-for-vegan-have-never-been-higher (last visited Aug 14, 2017).

[14] Tony Dokoupil, The decline of red meat in America MSNBC (2015), http://www.msnbc.com/msnbc/the-decline-red-meat-america (last visited Aug 14, 2017).

[15] USDA: Milk Consumption Has Dropped a Whopping 40 Percent Since 1970, Mercy For Animals (2013), http://www.mercyforanimals.org/usda-milk-consumption-has-dropped-a-whopping-40-percent-since-1970 (last visited Aug 14, 2017).

[16] Madeline Farber, The U.S. Government Is About To Buy 11 Million Pounds of Cheese USDA to Buy 11 Million Pounds of Cheese to Combat Surplus | Fortune.com (2016), http://fortune.com/2016/08/24/usda-buy-cheese-surplus/ (last visited Aug 14, 2017).

[17] Mark Bittman, We're Eating Less Meat. Why? The New York Times (2012), https://opinionator.blogs.nytimes.com/2012/01/10/were-eating-less-meat-why/ (last visited Aug 14, 2017).

greenhouse gas emissions;" more than that caused by transportation. [18] Additionally, the meat and dairy industry is responsible for 80-90% of water consumption in the United States.[19] The water used for growing feed for cows alone comprises 56% of the water usage in the United States.[20]

Another factor contributing to the rise in vegan food is health. Many studies have shown that the top fifteen causes of death in the United States can be prevented or even reversed by adopting a plant based diet:[21] A stark difference when compared to the substantial link between the consumption of red meat and pre-mature death.[22]

Lastly, ethics have also become a motivating factor. The U.S. government has refused to enforce stricter animal cruelty laws despite decades of undercover footage of graphic animal abuse at slaughterhouses: for example, chickens that were boiled alive[23], cattle that suffer third-degree burn from branding[24], and female pigs forced to live in pork gestation crates for their entire lives[25].

Food innovation

The growing vegan market is motivating innovation in food science. In Silicon Valley, food scientists are engaged in the "perfect vegan burger" race with Impossible Foods Inc. and Beyond Meat Inc. as the frontrunners. Both companies aim to create a 100% plant based burger with the exact taste and texture of a beef burger. Impossible Foods, backed by Bill Gates, rejected a $300 million buy-out offer from Google in 2015.[26] Stanford professor and CEO of Impossible Foods, Patrick Brown, said the company rejected the offer because they wanted to "have control of our own fate."[27] Patrick Brown started the company in 2009 when he "decided to devote an 18-month sabbatical to eliminating industrial meat

---

[18] Facts and Sources, COWSPIRACY, http://www.cowspiracy.com/facts/ (last visited Aug 14, 2017).

[19] *Id.*

[20] *Id.*

[21] HOW NOT TO DIE, an instant New York Times Best Seller, NutritionFacts.org, https://nutritionfacts.org/book/ (last visited Aug 14, 2017).

[22] Harvard Health Publications, Cutting red meat-for a longer life Harvard Health, https://www.health.harvard.edu/staying-healthy/cutting-red-meat-for-a-longer-life (last visited Aug 14, 2017).

[23] Bruce Friedrich, USDA: Time to Stop the Chicken Industry From Boiling Birds Alive The Huffington Post(2014), http://www.huffingtonpost.com/bruce-friedrich/usda-time-to-stop-the-chi_b_4855990.html (last visited Aug 14, 2017).

[24] The Beef Industry, PETA, https://www.peta.org/issues/animals-used-for-food/factory-farming/cows/beef-industry/ (last visited Aug 14, 2017).

[25] Post Staff Report, Hidden-camera video shows graphic animal abuse at pig farm New York Post (2017), http://nypost.com/2017/01/31/hidden-camera-video-shows-graphic-animal-abuse-at-pig-farm/ (last visited Aug 14, 2017).

[26] Jack Millner For Mailonline, Google wants the world to go meat-free: Search giant tried to buy a veggie burger start-up for $300 MILLION Daily Mail Online (2015), http://www.dailymail.co.uk/sciencetech/article-3177026/Google-wants-world-meat-free-Search-giant-tried-buy-veggie-burger-start-300-MILLION.html (last visited Aug 14, 2017).

[27] Jason Del Rey, Here's why fake-meat startup Impossible Foods wouldn't sell to Google Recode (2016), http://www.recode.net/2016/6/1/11836120/impossible-foods-meat-sell-google (last visited Aug 14, 2017).

production, which he determined at the time to be the world's largest environmental problem."[28] Since then, Impossible Foods has received $300 million in funding and has released a plant based burger that is currently available in select restaurants in the United States.[29]

Beyond Meat was founded in 2009 by Ethan Brown, who wanted to solve the problems of "climate change, animal welfare, natural resources, and human health" by creating the perfect plant based burger.[30] Tyson foods, one of the biggest U.S. meat producers, invested an "undisclosed amount" for a 5% stake in Beyond Meat in 2016. The Beyond Burger is currently available at Whole Food Stores nationwide.[31]

At these companies, innovation is still in its nascent stages. Currently, Impossible Foods is working to develop blood substitutes and connective tissue to hold burgers together in a way that mimics real meat. [32] This is a hard problem, and Impossible Burger is the first to admit it. Allen Henderson, a food scientist at Impossible Burger recently stated that: "[T]here's a lot more to discover. Every plant species contains 20,000 to 40,000 proteins in its genome, any one of which could have surprising functions once separated from the rest of the plant."[33] Developing mock meat requires experiments that lead to constant unexpected results. As Allen Henderson observed:

> I'm learning a lot about how proteins do or don't play well together. . . . The rules are turning out to be very different than we thought . . . . They do things that are completely unexpected. I have over a decade of training as a biochemist, and I'm still like, Why did that just happen?[34]

Early case law

Early case law suggested that food inventions and innovations could not receive patent protection because it would be harmful to the food industry. One of the first cases that discussed the topic was *In re White*[35] In *In re White,* the Court observed that "it is a matter of common knowledge that new recipes for cooking and for the production of food products are constantly being developed by adding or eliminating

---

[28] Rowan Jacobsen, The Biography of a Plant-Based Burger Pacific Standard (2016), https://psmag.com/the-biography-of-a-plant-based-burger-31acbecb0dcc#.3qobqgqxe>. (last visited Aug 14, 2017).

[29] Connie Loizos, Impossible Foods just raised $75 million for its plant-based burgers TechCrunch (2017), https://techcrunch.com/2017/08/01/impossible-foods-just-raised-75-million-for-its-plant-based-burgers/ (last visited Aug 14, 2017).

[30] Madeline Stone, How a startup that makes fake meat from plants caught the attention of Bill Gates and the founders of Twitter Business Insider (2015), http://www.businessinsider.com/how-a-startup-that-makes-fake-meat-from-plants-caught-the-attention-of-bill-gates-and-the-founders-of-twitter-2015-7 (last visited Aug 14, 2017).

[31] Fast Company Staff, Why Beyond Meat Is One Of The Most Innovative Companies Of 2017 Fast Company(2017), http://www.fastcompany.com/3067490/why-beyond-meat-is-one-of-the-most-innovative-companies-of-2017 (last visited Aug 14, 2017).

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] In re White, 39 F.2d 974, 975 (C.C.P.A. 1930)

well known ingredients or treating them in ways differing from former practice. To hold all these patentable would unsettle the arts of cooking and of preparing food products."[36] Many interpreted the reasoning in the case to suggest food could not receive patent protection in general and to do so would be damaging to the art of cooking.

A modern interpretation of the reasoning behind disallowing food patents in *In re White* is based on the nonobviousness doctrine.[37] The nonobviousness doctrine assesses whether a skilled artisan would have been motivated, through the art existing at and before the time of the alleged invention, to invent the subject matter of the alleged invention. Nonobviousness may be demonstrated by exhibiting "new and unexpected, surprising or far superior results, when compared with previous inventions and knowledge in the particular area of the invention."[38] Fortunately, subsequent case law did not follow the interpretation that food, in general, is un-patentable. Instead, case law developed a high standard for the non-obviousness requirement, as discussed in the next section. The court in *Publications Int'l v. Meredith,* explicitly held that food inventions are patentable when holding that food was not copyrightable: "there can be no monopoly in the copyright sense in the ideas for producing certain foodstuffs. Nor can there be copyright in the method one might use in preparing and combining the necessary ingredients. Protection for ideas or processes is the purview of patent."[39] *Publications Int'l* essentially held that, for the first time, a method of combining ingredients was patentable.

High standard for non-obviousness

Case law has demonstrated a high standard for non-obviousness. In *General Mills v. Pillsbury,*[40] the United States Court of Appeals for the Eighth Circuit[41] examined the validity of a cake mix patent owned by Pillsbury. General Mills argued that the cake mix was invalid because it was obvious. The court agreed that changing a pre-existing food recipe by adding or omitting an ingredient did not satisfy the non-obvious requirement: "It is conceded that all of the ingredients going into the cake mixes of each of the parties are old with the possible exception of the chemical leavening ingredients."[42]As a result, the patent was held as invalid because the addition of the chemical leavening ingredients, which were found in the prior art, was insufficient to pass the nonobviousness requirement. The Court held that:

> all of the elements used in plaintiff's cake mix batter were old and known. The means of creating carbon dioxide gas by use of soda and acids was known and understood at lease since Glabau's writings in 1931 . . . . We hold that the subject matter of plaintiff's patent

---

[36] *Id.*

[37] Merges, Robert P. *Patent Law and Policy: Cases and Materials*. Charlottesville, VA: Michie, 1997. Print.

[38] Pressman, David. *Patent It Yourself*. Berkeley, CA: Nolo, 2008. Print.

[39] *Publications Int'l, Ltd. v. Meredith Corp.*, 88 F.3d 473, 481 (7th Cir. 1996)

[40] *Gen. Mills, Inc. v. Pillsbury Co.*, 378 F.2d 666, 671 (8th Cir. 1967)

[41] This case was decided by the Eighth Circuit because the Federal Circuit, which now decides all appeals of patent cases, had not yet been formed. The United States Court of Appeals for the Federal Circuit was created in 1982. "Federal Circuit US Court of Appeals Case Law." *Justia Law*, law.justia.com/cases/federal/appellate-courts/cafc/.

[42] *Id.*

> would be obvious at the time of the invention in view of the prior art to a person having ordinary skill in the pertinent art[43]

The *General Mills* case established the standard that the addition or omission of an ingredient to an existing recipe was obvious to a person having ordinary skill in the art, and it therefore did not result in an unexpected result. The failure to demonstrate an unexpected result established a heightened nonobviousness requirement.

The high standard for nonbviousness has also posed obstacles for companies after they have successfully obtained food patents. An example of this happened when the The Smuckers Company tried to enforce and expand a patent on a peanut butter and jelly sandwich concoction.[44] Smuckers argued Ablie's Foods, Inc. was infringing their patent and sent the company a cease and desist letter.[45] Albie responded by filing a declaratory judgment in an effort to invalidate the patent. The patent was re-examined and Smuckers simultaneously prosecuted two closely related applications in the effort to expand the scope of its peanut butter and jelly patent. The original patent was cancelled and the two related applications were rejected. The rejected applications were appealed to the Board of Patent Appeals and Interferences who affirmed the rejections.[46] The Board rejected the applications due to obviousness objections. The Board cited prior art that was used during the litigation of the patent reexamination. Therefore, successfully obtaining a food patent is not the final hurdle of the nonobvious standard. Nonobviousness obstacles may exist after obtaining patents for food companies.

Successful food patents

The USPTO has issued several food patents. Some examples of successful recipe patents include a dissolvable tablet with nutritious ingredients used for astronauts,[47] additives to enhance the flavor of chocolate[48],and a microwaveable sponge cake.[49]

Focusing on the microwavable sponge cake, prior to its invention, the technique used for making sponge cakes was baking in a conventional oven. Microwaves were not used because uneven heating would result in a "stale or tough" end product.[50] The innovative aspect of the food invention used "mesophase

---

[43] *Id.*

[44] Emily Cunningham, Protecting Cuisine Under the Rubric of Intellectual Property Law: Should the Law Play A Bigger Role in the Kitchen?, 9 J. High Tech. L. 21 (2009)

[45] Thomas C. Folsom, Designing Food, Owning the Cornucopia: What the Patented Peanut Butter & Jelly Sandwich Might Teach About Gmos, Modified Foods, the Replicator, and Non-Scarcity Economics, 8 Akron Intell. Prop. J. 53, 55 (2015)

[46] *Id.*

[47] U.S. Patent No. 6,149,939 A

[48] Chris Mayes, What Users Say About PatentEase Software What Users Say About PatentEase Software, http://store.inventorprise.com/content_articles.php?id=1049 (last visited Aug 14, 2017).

[49] U.S. Patent No 6,410,074 B1

[50] *Id.*

gels" which facilitated the sponge cake's baking in a microwave in a manner that was similar to baking in an oven. A sponge cake baked in a microwave with "mesophase gels" would also taste similar to a sponge cake baked in an oven. The use of mesophase unexpectedly resulted in a microwaveable sponge cake that enabled the granting of a patent.

One piece of prior art to the microwavable sponge cake included a "reduced calorie chemically leavened cake batter." [51] The reduced caloric quality of the cake batter was achieved in part by adding "gel mesophase." [52] It can be interpreted that the link between using mesophase gels to reduce calories in cakes and to create a microwavable sponge cake was an unexpected result.

An additional example of a highly innovative method is a patent for "controlling cookie geometry".[53] Using varying fats in the "shortening component of the cookie dough" controls the spread of a cookie.[54] Prior to the invention, methods employed to control excessive spread had limitations. For example, corn was used to decrease spread, but it made the cookies "hard and gritty." [55] Using certain proportions of fat to successfully control cookie geometry is not found in the prior art. Again, link between fat proportions and cookie spread can be interpreted as leading to an unexpected result, which allowed for a successful food patent.

Conclusion

Given the state of patent protection for food, it is likely that vegan food companies like Impossible Foods and Beyond Meat will continue to receive legal protections in the form of food patents. Impossible Foods has already successfully obtained a patent covering technology "to use leghemoglobin in plant based meat".[56] And with over 100 patents pending, it is likely Impossible Foods, and companies like it, will successfully obtain more food patents. Therefore, strong patent protection for food patents will help food research companies invest more in innovation of vegan food technology and help the vegan food industry continue to grow.

---

[51] U.S. Patent No 5,534,285

[52] *Id.*

[53] U.S. Patent No 5,374,440

[54] *Id.*

[55] *Id.*

[56] Plant-Based Impossible Foods Raises Another $75 Million: Bill Gates Invests Again, Latest Vegan News, http://www.plantbasednews.org/post/plant-based-impossible-foods-raises-another-75-million-bill-gates-invests-again (last visited Aug 14, 2017).

Demystifying the Algorithm in Employment Hiring Disparate Impact Cases*

BY CRYSTAL ARAUJO

* *I would like to gratefully acknowledge Susan Freiwald, Associate Dean at the University of San Francisco, School of Law, for her guidance on this article. I would also like to thank my parents Leticia and Javier Araujo and my daughter Sophia Araujo for all their support.*

I. Introduction

Employers are increasingly relying on the benefits of automated algorithms, because the amount of information and quick results.[1] These tools or processes can have an adverse effect on protected classes under Title VII of the Civil Rights Act of 1964.[2] This existing legal framework does not address the technological advances and algorithms used to make hiring decisions. Generally, in employment discrimination cases, the plaintiff must first prove either disparate treatment or disparate impact. In disparate impact cases, the employee/plaintiff already has a higher evidentiary burden to prove with traditional hiring practices. Today, it is nearly impossible to prove any form of discrimination in hiring practices when an algorithm is the decision maker. To increase transparency, Congress should adopt a recording system for algorithms used in hiring decisions and make these reports available to the public.

As more companies and agencies rely on algorithms to make critical hiring decisions, the algorithm cannot remain a "black box" of unknown processes.[3] Congress should pass legislation to implement a self-reporting and record-keeping system. This self-reporting system would create a database of algorithmic formulas used in hiring decisions to be made available to interested parties such as applicants, employees, researchers, and the general public. The use of algorithms requires a greater level of transparency and accountability than we have now. New legislation would set a standard and guidelines for disclosure and transparency for both public and private sectors. The collection of these records would also assist employers in the hiring decision by promoting a better understanding of their workforce and its demographics.

This Paper is divided into three parts. Part I provides background information pertaining to big data and algorithms used for hiring decisions. Further, it identifies the growing reliance on algorithms for hiring purposes and outlines Title VII of the Civil Rights Act. Part II identifies the risk of violating Title VII that employers face when relying on algorithms to make hiring decisions. Part III gives an overview of European Union law and previously introduced United States House bill H.R. 451, both of which present two different approaches to addressing the issue described in Part II. It also includes a legislative recommendation that would create a self –reporting database for algorithms used for hiring purposes.[4]

---

[1] David J. Walton, *Big Data's Potential Disparate Impact Problem,* Law360 (Aug. 21, 2014), http://www.law360.com/articles/568911/big-data-s-potential-disparate-impact-problem

[2] *See* Civil Rights Act of 1964, 42 U.S.C. § 2000(e) (1964).

[3] *See* Viktor mayer-schonberger & Kenneth Cukier, Big Data 5 (2013).

[4] *See* Application, Privacy, Protection, and Security (APPS) Act, H.R. 4517, 114th Cong. (2d Sess 2016).

A. Background

The advancement of technology has brought many opportunities for efficiency and precision with everyday tasks and decisions.[5] There are currently many different online platforms driven by data, such as in shopping, social media, and search engines.[6] The opportunities for both companies and consumers to efficiently strike a bargain has led to an overwhelming use of these systems.[7] As globalization dominates all markets and the employment sector, companies and organizations have adopted and invested in algorithms to stay competitive.[8] The vast amount of information intertwined with the power of algorithms has caused some concern about the autonomy algorithms have to make decisions.[9]

In recent years, the Federal government has highlighted the benefits and concerns of relying on technology and big data. In 2014 and 2015, the Obama Administration released two extensive reports on big data and its implications.[10] Around the same time, the Federal Trade Commission (FTC) and the Equal Employment Opportunity Commission (EEOC) also held conferences and produced reports on big data and its potential to discriminate.[11] All these reports identified the employment sector as a potential area for concern.

There is a concern between the benefits algorithms can provide employers and the hidden harms of these automated systems. Algorithms and big data can be used to either promote or inhibit fairness in the hiring process depending on how they are used.[12] In late 2016, EEOC Chair Jenny R. Yang provided the following comments during the "*Growing Use of Algorithms to Make Employment Decisions,"* panel:

> Big Data has the potential to drive innovations that reduce bias in employment decisions and help employers make better decisions in hiring, performance evaluations, and promotions. At the same time, it is critical that these tools are designed to promote fairness and opportunity, so that reliance on these expanding sources of data does not create new barriers to opportunity.[13]

---

[5] *See supra* note 3, at 5.

[6] *Id.*

[7] *See* Walton, *supra* note 1.

[8] Executive Office of the President of the United States, Big Data: Seizing Opportunities, Preserving Values, iii (May 1, 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf . [hereinafter Seizing Opportunities].

[9] *See* Walton, *supra* note 1.

[10] *See Id.*, *see also,* Executive Office of the President of the United States, Big Data and Differential Pricing (February 2015), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf . [hereinafter Differential Pricing].

[11] Press Release, Equal Employment Opportunity Commission, Use of Big Data Has Implications for Equal Employment Opportunity, Panel Tells EEOC (Oct. 13, 2016) (on file with author) [hereinafter EEOC Press Release].

[12] *Id.*

[13] *Id.*

The question many agencies, both private and public, are asking is: can algorithms discriminate unfairly? To answer the question, an understanding of algorithms and the data used by these systems is essential.

1. Algorithms

An algorithm is a mathematical formula designed to analyze information and produce results or decisions.[14] When enabled by technology, algorithms can process more information faster and automatically. According to Claire Miller author of *When Algorithms Discriminate,* programmers and computer engineers develop and design algorithms to achieve specified results by using a series of instructions.[15] These instructions can be designed to "[g]enerate categories for filtering information, operate on data, look for patterns and relationships, or generally assist in the analysis of information."[16] Unfortunately, an algorithm often becomes a "black box," because the automatic results cannot easily be traced back to the original instructions or the information behind those instructions.[17]

An advanced algorithm is designed to give automatic results based on the evolution of data collected. Advanced algorithms are also known as "machine learning" algorithms.[18] In *Big Data's Potential Disparate Impact Problem*, authors Solon Barocas and Andrew Selbst state that, "[t]he algorithm 'learns' which related attributes or activities can serve as potential proxies for those qualities or outcomes of interest." [19] In other words, the algorithm learns to modify its instructions and results based on the past patterns and trends. As the algorithm collects new data from new applicants or from purchased data sets, the analysis of the decision changes and over time it becomes difficult to trace back the change. A mathematical formula alone is already difficult to understand, but when that mathematical formula evolves independently, understanding how and why the formula evolved becomes even more difficult.

Today, algorithms have a level of sophistication that advances our ability to process massive amounts of information at speeds not humanly possible. A comparison between 1954's IBM's translation system to today's Google Translate illustrates the advancement and capabilities of algorithms.[20] IBM's algorithm translated Russian to English which made understanding the language easier because it was one-word to one-word translation.[21] However, today's technology has advanced tremendously and Google Translate's algorithms use billions of pages to not only translate each word but also to predict the correct

---

[14] Federal Trade Commission, Data Brokers, A Call for Transparency and Accountability n. 36 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf . [hereinafter Data Brokers].

[15] Claire Cain Miller, *When Algorithms Discriminate*, The New York Times (July 9, 2015). [hereinafter Miller, *When Algorithms*], https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?_r=0.

[16] Seizing Opportunities, *supra* note 8, at 46.

[17] Miller, *supra* note 15.

[18] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671, 678 (2016)

[19] *Id.*

[20] Mayer-Schoenberger & Cukier, *supra* note 3, at 178.

[21] *Id.*

word usage.[22] This makes the language translation much more sophisticated, accurate and advanced.

2. Data

Data is essentially information. Before technology, information had been traditionally stored in physical hard copies that were organized in a filing or record keeping system. Each individual piece of information is known as data and the compilation of data generates data sets known as big data.[23] The types of data collected and stored can include anything shared online from personal information to a user's online interactions.[24] Individual users create data with each online interaction. [25] Today, advancements in technology enable information to be organized and recorded electronically.

In 2014, the Executive Office of the President of the United States stated, "Today, data is more deeply woven into the fabric of our lives than ever before. We aspire to use data to solve problems, improve well-being, and generate economic prosperity."[26] Technology provides users with the opportunity to interact online with a variety of applications, social media platforms, and websites.[27] Data is constantly being created, collected, shared, bought, and sold by these online tools.[28]

For decades, companies have relied on larger data sets to advance business interests.[29] Technology has allowed for these data sets to be created at a faster pace. According to President Obama's Executive Report, in 2013, people generated four zettabytes, or 4,000, 000,000,000,000,000,000 bytes or units, of information worldwide.[30] "[I]magine that every person in the United States took a digital photo every second of every day for over a month. [P]ut together would equal about one zettabyte."[31] However, larger amounts of data do not guarantee accurate results for algorithms.

The success of an algorithm and its results depend on the quality of the data.[32] It is important to have a good understanding of the data interpreted by an algorithm. Outdated, missing, or inaccurate data can significantly impact a data set and can alter a decision or result made by an algorithm.[33] An FTC's report explained the importance of data quality is based on the accuracy of the collected data.[34] The maintenance and management of data and comprised data sets are crucial for those using algorithms.

---

[22] *Id.*

[23] Differential Pricing, *supra* note 10, at 1.

[24] *Id.*

[25] *Id.*

[26] Seizing Opportunities, *supra* note 8, at 1.

[27] *See* FTC Data Brokers *supra* note 14, at 70.

[28] Seizing Opportunities, *supra* note 8, at 1.

[29] Sheri Pan, *Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze,* 30 Harv. J.L. & Tech. 239 (2016).

[30] *Id.*

[31] *Id.*

[32] *See* Walton, *supra* note 1. *See also,* Seizing Opportunities, *supra* note 8, at 1.

[33] *Id.*

[34] *See* FTC Data Brokers, *supra* note 14, at 70.

B. Algorithms Used to Hire Employees

Employers have a lot to gain from algorithms and big data. Algorithms can help businesses find efficient business models as well as determine the quality of a potential employee.[35] Technology coupled with a mathematical algorithm allows for automated decisions in contrast to the traditional hiring process. Using automated algorithms is more efficient and more cost effective because recruiters and employers can sort through more qualified applicants than they could by sorting through traditional paper applications. It is very similar to online dating sites that use algorithms to match couples.[36] An employer can create a model candidate profile and a developer can take that information to create a set of instructions to identify the ideal candidates from a pool of applicants.[37] In that way, algorithms provide substantial cost savings by making hiring efficient and by eliminating unqualified or unfit candidates.

Today, employers and recruiters can use instructions to more precisely instruct algorithms to search for the best candidate. Automated searches can look for specific skills, indications of reliability, or previous job tenure.[38] An employer can hire a programmer or engineer internally to develop an algorithm unique to the company's needs or hire a third party recruiting company dedicated to meeting employers' needs by using automated algorithms.[39] Today, new recruiting companies like Gild, Entelo, Textio, Doxa, and more established companies like Korn Ferry are all incorporating algorithms to find the ideal candidates for employers.[40] Miller argues, "[H]iring could become faster and less expensive, and their data could lead recruiters to more highly skilled people who are better matches for their companies."[41] Employers are beginning to make the switch from traditional hiring methods to automated algorithm-based recruiting and hiring.

The EEOC also recognizes the advantages of algorithms and sees them as an opportunity to meet the goals of their agency. The EEOC has stated that companies can employ algorithms to specifically prevent discrimination and promote diversity.[42] This highlights just how dependent algorithms are on the instructions. For example, in response to pressure to diversify the workforce in the Silicon Valley tech industry, companies like Twitter and Yahoo pledged to diversify their workforces. [43] These companies are trying hold their automated hiring algorithm accountable by keeping records and publishing their diversity data. This data demonstrates a company's commitment to diversity in its workforce.

---

[35] Barocas & Selbst, *supra* note 18*,* at 679.

[36] *See* Miller, *When Algorithms, supra* note 15.

[37] Claire Cain Miller, *Can an Algorithm Hire Better Than a Human?*, The New York Times (June 25, 2015) [hereinafter Miller, *Hire Better*], http://www.nytimes.com/2015/06/26/upshot/can-an-algorithm-hire-better-than-a-human.html.

[38] Barocas & Selbst, *supra* note 18*,* at 679.

[39] Seizing Opportunities*, supra* note 8, at 41.

[40] Miller, *Hire Better, supra* note 37.

[41] *Id.*

[42] EEOC Press Release, *supra* note 11.

[43] Miller, *Hire Better, supra* note 37.

The FTC's report highlights another Silicon Valley example that illustrates a change in the type of questions Google asks during its interview process.[44] Google modified its interview process to include behavioral questions because the company found issues with its historical reliance on academic grade point averages.[45] Google's goal was to minimize an interviewer's bias by changing the automated algorithm to include additional behavior questions.[46] Like Twitter and Yahoo, Google is using algorithms to achieve more diversity in its workforce.[47]

In the same manner that algorithms can be used to diversify a workforce, algorithms can also be used to employ discriminatory instructions. These biases can be explicitly or implicitly embedded into neutral instructions.[48] There is a concern about bias at every stage of creating an algorithm.[49] For example, many companies have relied on top tier university degrees as a hiring threshold.[50] This reliance exacerbates diversity problems because it excludes many members of protected classes who historically could not attend top tier schools or currently attend them in smaller percentages.[51]

Another example from the FTC's *Big Data* report shows the difficulty keeping discriminatory correlations out of business decisions.[52] Specifically, a company found that the length of employees' previous job tenure was linked to the distance the employee had lived from their previous company. Employees who lived closer to their jobs had spent longer terms at those companies. Using residency as a hiring criteria in an algorithm would ideally ensure long-term employees, but living further from the company may be tied to an employee's social class and race. In fact, "another company decided to exclude [residency] from its hiring algorithm because of concerns about racial discrimination, particularly since different neighborhoods can have different racial compositions."[53] Including or excluding certain information could significantly change the results an algorithm produces.

---

[44] Federal Trade Commission, Big Data, A Tool for Inclusion or Exclusion, Understanding Issues 7-8 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf . [hereinafter FTC Big Data].

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *See* Miller, *Hire Better, supra* note 37.

[49] FTC Big Data*, supra* note 44, at 25.

[50] *Id.* at 29.

[51] *Id.*

[52] *Id.* at 31.

[53] *Id.*

C. Title VII Employment Discrimination

The 1964 Civil Rights Act prohibits discrimination based on several protected classes, including sex, race, religion, and national origin.[54] Title VII of the Act specifically prohibits employment discrimination, including discrimination during the hiring process.[55] The EEOC enforces Title VII.[56] There are two common causes of action an applicant or employee can bring to address racial discrimination in the hiring process. The first is disparate treatment. The plaintiff in a disparate treatment case must prove the employer intentionally discriminated based on membership in a protected class.[57] The second is disparate impact. The plaintiff in a disparate impact case must prove that the employer's neutral practice disproportionally inhibited members of a protected class from being hired.[58] Once the plaintiff established a disparate impact, the employer must show there is business necessity for any such discriminatory practice. The plaintiff's burden of proof and the employer's intent are different for each cause of action.

An employer's intent to discriminate is vital for disparate treatment cases. Disparate treatment occurs when an employer treats an applicant differently based on race or another protected class.[59] An applicant who specifically was not hired based on race by an employer's explicit discriminatory treatment or practice may prove a prima facie case of disparate treatment with direct or circumstantial evidence.[60] After establishing that the plaintiff belongs to a protected class, the plaintiff must prove he or she met the hiring qualifications but was denied the opportunity because the employer had a specific discriminatory motive.[61] After an employee establishes a prima facie case, the burden of proof will shift to the employer to provide a nondiscriminatory reason for rejecting the applicant.[62] The burden reverts back to the plaintiff/applicant to prove the reason given was pre-textual.[63] In *McDonnell Douglas Corp. v. Green,* the Supreme Court described the final burden a plaintiff must meet, "In short, . . . respondent must be given a full and fair opportunity to demonstrate by competent evidence the presumptively valid reasons for his rejection were in fact a cover-up for a racially discriminatory decision."[64] In other words, a plaintiff must establish the employer's motive or intent to discriminate in a disparate treatment case. [65]

---

[54] 42 U.S.C. § 2000e-2(a).

[55] *Id.*

[56] § 2000e-4(a).

[57] § 2000e-2(a)(1).

[58] § 2000e-2(a)(1)(A).

[59] *Teamsters v. United States,* 431 U.S. 324, 335 (1977). *See also McDonnell Douglas Corp. v. Green,* 411 U.S. 792, 805 (1973).

[60] *Teamsters*, 431 U.S. at 336.

[61] *McDonnell*, 411 U.S. at 802.

[62] *Id. See also Teamsters*, 431 U.S. at 339.

[63] *Id.* at 807.

[64] *Id.* at 805.

[65] *Id.* at 807.

By contrast, intent to discriminate is not required for disparate impact claims.[66] Both parties have to meet different evidentiary burdens. Even though disparate impact cases do not require an employer's discriminatory intent, the evidentiary burden for the plaintiff is much higher than in disparate treatment cases.[67] Instead of overtly discriminatory conduct, disparate impact is a neutral practice with an adverse effect on a protected class.[68] First, a plaintiff must show that a specific impartial hiring practice caused disparate impact on a protected class.[69] The burden then shifts to the employer/defendant to rebut the plaintiff's accusations by showing the disparity does not exist or that the hiring practice is a business necessity.[70] Finally, the plaintiff can counter an employer's business necessity argument by showing it is not related to the job or that an alternate selection process exists without the same discriminatory effect.[71]

In 1971, the Supreme Court established disparate impact in the landmark decision, *Griggs v. Duke Power Co*.[72] In *Griggs*, the Court found that disparate impact may occur with "practices that are fair in form, but discriminatory in operation."[73] The employer in *Griggs* required a high school diploma or intelligence test for hiring purposes and for promotions to departments that had been historically white with higher pay.[74] Griggs argued the diploma requirement was not intentionally discriminatory however, as applied, the requirement excluded African Americans from higher paying jobs.[75] The Supreme Court found that the policy disproportionately impacted African Americans because only 12% of black males had completed high school in comparison to 34% of white males in the state of North Carolina.[76] Moreover, the Court found that, "neither the high school completion requirement nor the general intelligence test is shown to bear a demonstrable relationship to successful performance of the jobs for which it was used."[77] Since this decision, the courts have frequently found that high school diplomas and standard aptitude or intelligence tests violate Title VII if the requirements have no relation to the job or are not a business necessity.[78]

---

[66] *Griggs v. Duke Power Co.*, 401 U.S. 424, 428 (1971).

[67] *See Teamsters*, 431 U.S. at 378.

[68] *See Desert Palace, Inc. v. Costa*, 539 U.S. at 99-100 (quoting *Price Waterhouse v. Hopkins*, 490 U.S. 228, 253 (1989) and *Rogers v. Missouri Pacific R. Co.*, 352 U.S. 500, 508 n.17 (1957)).

[69] 42 U.S.C. § 2000e-2(k)(l)(A)(i).

[70] § 2000E-2(k)(l)(A)(ii).

[71] *See* McDonnell, 411 U.S. at 807.

[72] 401 U.S. 424 (1971).

[73] *Id.* at 432.

[74] *Id.* at 427.

[75] *Id.* at 431.

[76] *Id.*

[77] *Id.* at 432.

[78] Barocas & Selbst, *supra* note 18, at 702.

In disparate impact cases, a plaintiff has a higher evidentiary burden because a plaintiff must first meet the burden of a prima facie case and then rebut an employer's "business necessity" defense.[79] As part of a prima facie case, a plaintiff must establish a specific hiring practice or test that is being used by the hiring employer that caused a disparate impact. Statistical and data evidence can be used to established disparate impact among new hires by a recruiter or employer. In *Griggs,* for example, the high school diploma requirement assisted the company in continuing to hire and promote white over blacks to higher paying roles, because only one African American employee out of thirteen had been promoted since the beginning of the Civil Rights Act.[80] Later in *Wards Cove Packing Co. v. Atonio,* the Supreme Court required "a demonstration that specific elements of the petitioners' hiring process have a significantly disparate impact on nonwhites."[81]

Once a plaintiff establishes a racially discriminatory effect by means of a pre-employment test or practice, the burden shifts to the employer. The employer must then provide evidence showing the test or practice is sufficiently related to the job opening. In other words, an employer must establish a "business necessity," which is described as a practice related to the position and consistent with business demands.[82] For example, in *Albemarle Paper Co. v. Moody*, the Supreme Court gave deference to the EEOC's Guidelines which were established for employers to meet the job-related standard:

> The message of these Guidelines is the same as that of the Griggs case – that discriminatory tests are impermissible unless shown, by professionally acceptable methods, to be 'predictive of or significantly correlated with important elements of work behavior which comprise or are relevant to the job or jobs for which candidates are being evaluated.'[83]

The plaintiff retains the burden of persuasion and then must prove an alternative business practice or test that can accomplish the same business necessity without disparate impact effect.[84]

II. The Problem

With an open universe of data, programmers have the opportunity to ask a nearly infinite number of questions. To narrow that universe, programmers design algorithms to follow a specific set of instructions to meet certain objectives.[85] However, an algorithm's decisions are not objective or free of human bias, because different decision-makers influence the instructions assigned to algorithms.[86] Advanced and

---

[79] *Id.* at 701.

[80] *See Griggs*, 401 U.S. 424, *supra* note 66.

[81] *Wards Cove Packing Co. v. Atonio*, 490 U.S. 642, 658 (1989).

[82] 42 U.S.C. § 2000e-2 (k)(1)(A)(i).

[83] *Albemarle Paper Co. v. Moody*, 422 U.S. 405, 431 (1975).

[84] 42 U.S.C. § 2000e-2 (k)(1)(A)(ii).

[85] *See* Zeynep Tufekci, *Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency,* 13 Colo. Tech. L.J. 203, 206 (2016).

[86] *See* Walton, *supra* note 1.

independent algorithms cannot separate learned biases from past results or new data, unless instructed to do so.[87] These algorithms are designed to produce fast results with a huge amount of data and poor or biased data can significantly affect those results. There must be some accountability and transparency when using algorithms in hiring decisions.

Currently, without oversight or transparency, algorithms can intentionally or unintentionally eliminate individuals at any phase of an electronic hiring process. Rejected applicants are left without a notification or explanation as to the decision made by the algorithm.[88] Algorithmic decisions and analyses are unknown to the public which makes it nearly impossible for a plaintiff to meet the evidentiary standard in employment discrimination cases. This is a problem for both disparate treatment and disparate impact cases. The issue also inhibits enforcement of Title VII of the Civil Rights Act.[89] An entire protected class could potentially be eliminated from the interview process without notice or opportunity for due process, due to an algorithm and its use of data.

Algorithms and data can inherit biases that can significantly impact results.[90] Sociologists contend that historical bias is embedded in society as "institutional racism," and therefore in data sets.[91] Individual biases can impact the design of the algorithm through the instructions given to the algorithm. At the same time, historical data has embedded biases that will continue to be considered in the decision-making process unless the algorithm is instructed do otherwise. Poor data quality or mismanaged data can further perpetuate unchecked or historical biases in favor of or against certain individuals.[92] According to Dr. Lundquist, "The algorithm is matching peoples' characteristics, rather than job requirements."[93] In other words, an algorithm is focused on finding patterns in data and is not necessarily holistic or savvy enough to identify discrepancies with the data or its results.

An algorithm could simply mask intentional discrimination or embedded biases.[94] Masking is the covering of intentional discrimination by a conduct or a skills requirement that seems neutral on its face.[95] Masking could also occur unintentionally by conduct or practice that may seem necessary, but, when analyzed closely, is unrelated to the job.[96] For example, the Court in *Griggs* found the defendant's requirement of high school diplomas to mask discrimination of African Americans when applying for job promotions. Unfortunately, masking can be easily applied in algorithms. In 2014, the Obama administration stated: "The final computer-generated product or decision—used for everything from predicting behavior

---

[87] *See Id.* at 673.

[88] Pan, *supra* note 29*,* at 251.

[89] *See* Civil Rights Act of 1964, *supra* note 2.

[90] *Id.* at 676.

[91] Barocas & Selbst, *supra* note 18*,* at 673.

[92] *See* FTC Big Data, *supra* note 44, at 8.

[93] EEOC Press Release, *supra* note 11.

[94] Barocas & Selbst, *supra* note 18*,* at 692.

[95] *Id.*

[96] *Id.*

to denying opportunity—can mask prejudices while maintaining a patina of scientific objectivity" making it difficult to identify the bias or disparity.[97] In other words, the black box literally never creates the evidence that a plaintiff needs in order to prevail in disparate impact case.

A. Disparate Impact as Applied to Algorithms

For disparate impact, a plaintiff must establish a prima facie case by identifying a specific hiring practice or test that caused a disparate impact on a protected class. It is already challenging for plaintiffs to prove disparate impact in traditional hiring scenarios.[98] Without notice or access to the algorithm, or data used in making an employment decision, it is impossible to identify a violation of Title VII. As Pauline Kim explains, "[T]he ways the doctrine has been applied in the past are not well suited to address the data-driven nature of classification bias" today.[99] *Griggs* did not account for algorithms and technology, leaving plaintiffs without the necessary evidence to meet their burden.

In addition to the evidence of a specific discriminatory practice, a plaintiff must rebut an employer's "business necessity" defense. Establishing a business necessity requires evidence that the test or practice is integral to the skills needed to accomplish the job being filled. Unfortunately, "[r]eliance on algorithms will typically be a facially neutral employment practice.[100] An algorithm is often designed with business outcomes already in mind and it can easily be argued to be job related.[101] Without extensive background knowledge, a plaintiff would have difficulty identifying the exact practice that causes disparate impact. A plaintiff would have even more difficulty recommending an alternative to an unidentified business practice within a complex algorithm.

B. Hypothetical

To expand on the argument, consider the following hypothetical of a restaurant employer who is looking to hire a host or hostess to greet and seat guests upon arrival. This is a high-end restaurant, in an urban setting, that has always required a high school diploma as part of the hiring process. Additionally, a host or hostess is required to have good communication and customer service skills to qualify for the job. In this setting, the local applicant pool of Latinos and African-Americans have historically had a lower graduation rate than their white counterparts. Similar to the facts in *Griggs*, the restaurant's high school diploma requirement is neutral with unintentional discriminatory results. In *Griggs,* the Court found the high school diploma did not "measure the person for the job."[102]

The major difference between *Griggs* and the hypothetical is that the employer here has decided to automate the applicant screening process. In this example, the employer hires a developer to create an algorithm that preselects candidates for interviews based on a series of instructions developed to meet

---

[97] *See* Seizing Opportunities, *supra* note 8, at 46.

[98] Barocas & Selbst, *supra* note 18, at 692.

[99] Pauline T. Kim, *Data-Driven Discrimination at Work,* Wm & Mary L. Rev. 50 (forthcoming 2017).

[100] *Id.* at 49.

[101] *See* Barocas & Selbst, *supra* note 18, at 673.

[102] Griggs, 401 U.S. 424, 436.

the needs of the employer. Because the employer has historically interviewed only candidates with high school diplomas for the host position, the developer takes that information and can either instruct the algorithm to eliminate applicants without diplomas or prioritize applicants with diplomas. Either option will evolve the data to produce automated decisions that could significantly impact protected classes in a potential applicant pool. Based on these facts, it would be difficult for a potential plaintiff applicant to initially establish a Title VII prima facie case based on this example of a high school diploma requirement. Disparate impact requires some knowledge of the decision in order to meet the evidentiary standard.

Even though an applicant has knowledge that education information is collected, the plaintiff does not know how that information is then used and analyzed by an algorithm to make a decision. The disparate impact evidentiary standard does not account for automated algorithms and, unfortunately, a plaintiff cannot merely speculate that an algorithm may have caused a disparate impact. Even discovery may not reveal the precise evidence to prove an instruction within the algorithm caused disparate impact, because there are no accountability requirements for creating and using automated algorithms. When an automated algorithm is part of the hiring process, it eliminates accountability and the availability of information necessary for a potential plaintiff to claim a violation of Title VII.

III. Solution

Currently there is a lack of regulation and accountability from those benefitting from automated algorithm decisions. An Obama Administration big data report noted an, "asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it."[103] Without regulation, the unknown "black box," or automated algorithm, will only hide more practices. In response, last year the European Union revised its own General Data Protection Regulation ("GDPR") to address some of these concerns with a narrow explanation policy. The United States now has the opportunity to develop its own policy while working with the technology industry to continue innovation. As algorithms continue to advance our understanding through predictive measures, the United States cannot afford to wait for a solution.

A. The E.U. Solution

In 2016, the European Union ("EU") Council passed the GDPR to update the EU's laws on data usage.[104] In 2015, the directive was introduced in the European Parliament with the end goal of replacing the EU's original 1995 Data Protection Directive.[105] The 1995 Data Protection Directive guaranteed EU

---

[103] Seizing Opportunities, *supra* note 8, at 3.

[104] Conference Report, Proc. Int'l Conf. Machine Learning Workshop Human Interpretability, Bryce Goodman & Seth Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation*," New York, NY, 26– 30 (Jun. 28, 2016), https://arxiv.org/pdf/1606.08813.pdf.

[105] Council of the European Union Presidency Memo 95/46/EC, The Proposal for a Regulation of the European Parliament and of the Council on General Data Protection Regulation (Jun. 11, 2015), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf . [hereinafter EU Memo].

citizens protection from certain types of processing of personal data within the Union.[106] The GDPR regulation focuses on preserving the rights of an individual when it comes to "the collection, storage and use of personal information."[107] Author Bryce Goodman and Seth Flaxman explain, "[t]he GDPR's policy on the right of citizens to receive an explanation for algorithmic decisions highlights the pressing importance of human interpretability in algorithm design."[108] The GDPR will take effect in mid-2018.[109]

The EU recognizes the need for individuals to understand algorithms and their effects on decisions. The GDPR states that a "data subject shall have the right not to be subject to a decision based solely on automated processing."[110] Job applicants have the option to exercise their right to have a human being, such as the employer or a recruiter, consider the applicant's application, as opposed to an algorithm. An employer or recruiter would probably review these applicants through the traditional hiring process with individuals making decisions instead of an algorithm. United States employers looking to hire EU citizens for EU positions may face this request as well.

The GDPR further grants EU citizens the "right to explanation." This right will require employers and recruiters to give notice to applicants about the data collected about them and will give them access to their collected data upon request.[111] Article 15 of the GDPR requires data controllers or brokers to respond to individuals at "reasonable intervals and free of charge."[112] In addition, the GDPR outlines about a half dozen different requests a citizen can make to a data controller.[113] Producing these documents and reporting to each individual may place a heavy cost burden on companies and data controllers. Beyond the cost, another barrier to this level of transparency is that companies with automated algorithms may purposefully conceal the "decision making procedures . . . from public scrutiny."[114]

Accountability can be lost when you remove a human decision-maker and replace that role of decision-maker with an automated algorithm. Transparency is required to keep these automated algorithms accountable. Exposure of the automated decision-making process is also necessary for governments to protect their citizen's rights. In a world that heavily relies on technology and automated algorithms, the EU's GDPR is demanding on employers and recruiters as it should be to better understand the black box.

B. A Proposed U.S. Approach

A solution should reveal sufficient information for an applicant in an employment hiring disparate impact case to meet the prima facie evidentiary standard when it comes to an automated algorithm decision. Before we can completely rely on the benefits from these automated systems, we must understand how these

---

[106] *See* Goodman & Flaxman, *supra* note 104, at 2.

[107] *Id.* at 1.

[108] *Id.*

[109] *Id.*

[110] *See* EU Memo, *supra* note 105, at 109.

[111] *See* Goodman & Flaxman, *supra* note 104, at 26.

[112] *See* EU Memo, *supra* note 105, at 98.

[113] *See* Goodman & Flaxman, *supra* note 104, at 26.

[114] *Id.*

systems are designed. To understand the algorithms used for hiring, there must be greater transparency and accountability. This Paper discusses two potential solutions. First, support for legislation like H.R. 4517 for mobile applications, because H.R. 4517 addressed both transparency and accountability.[115] Second, this paper recommends the establishment of a business record system for employers to self-report automated algorithms used for hiring.

1. *H.R. 4517*

In 2016, the 114th Congress attempted to bring security and transparency to data collection through user control. [116] The *Application, Privacy, Protection, and Security Act* ("APPS Act") would have introduced transparency to the treatment and use of data and its collection.[117] The opportunity to address transparency of data usage was called "user control."[118] Unlike the EU, the APPS Act would have been the first time the U.S. would require companies to allow users to have control of their personal data. Congressman Hank Johnson, the author of the bill stated, "The Data Act would bring big data out of the shadows, creating transparency and control for consumers over their personal data, and provide consumers with the tools to correct the record and minimize collection."[119]

The APPS Act would have required application developers for mobile devices to be transparent and accountable for the data collected from their customers. The Act had several components, including requiring consent from the user, data protections, and a notice requirement.[120] Developers would have had to provide users notice of the following four categories: personal data collected, collection purpose, third party sharing, and a transparent data retention policy.[121] This notice would have provided users with the information necessary to understand how their information is being collected and used.

This bill is a step in the right direction for data policy in the United States. It can serve as a template for future data use laws in other sectors. Though the original APPS Act covered only mobile applications, the bill could be amended to reflect all data in general or specific sectors, like employment. For example, had the APPS Act requirements covered automated algorithms used in hiring decisions, the notice requirement would have revealed the information collected and its use before an applicant applied for a position. The information exposed could reveal potential violations of Title VII of the Civil Rights Act by employers or recruiters using an automated algorithm to screen applicants. This bill on data privacy should be reintroduced and passed by the current Congress.

---

[115] *See* APPS Act, *supra* note 4.

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] Hank Johnson, *Every Member of Congress Should Sign On To My Bills That Enhance consumers' Privacy & Ensure Digital Inclusion,* Huffington post (February 16, 2017).

[120] *Id.*

[121] *See* APPS Act, *supra* note 4.

2. *Proposed Law*

Demystifying algorithms will begin to reveal the black box and allow for the development of best practices and opportunities to promote diversity to meet the goals of the EEOC.[122] Congress should require employers and recruiters using automated algorithms to report the data and the algorithm used in making those decisions. This reporting system would be a business records model requiring companies to self-report the information. The government through an established agency, like the EEOC, can collect these reports for the public to view which would establish prior knowledge of the automated algorithm and the data used to make hiring decisions by specified companies. Essentially providing the public the foundation of an automated algorithm before it evolves.

The reporting system would require all employers and recruiters using automated algorithms in hiring employees to report information regarding the algorithm and data. The report would require information about all the data that interacts with the algorithm including, but not limited to, data collected, data sets, and data usage. An initial report would be required for any new automated algorithm and then every two years a report of any amendments or significant changes should be filed. The reports would be made available to the public by an already established entity, such as the EEOC, which is dedicated to this mission of equal employment. This entity would be responsible for collecting and keeping a public database of information.

These reports would be required to be developed by experts, such as the developers behind the algorithm or a third party specializing in audits of algorithm and data. Experts could translate technical language into layman's terms for better comprehension for the public to view and understand. The report would outline the algorithm instructions and the data it used to process those instructions. The EEOC's recent data audit outcomes can provide a template to the information to be gathered for reporting. The EEOC would be the best-suited agency to maintain a public database for algorithm reports since it is already dedicated to protecting equal employment.

The EEOC's three target outcomes of its own data audit could benefit employers and recruiters using data and automated algorithms for hiring purposes.[123] For example, the first target outcome would be to require an "audit standard" level of auditing of data used by automated algorithm to hire an employee.[124] A data audit could reveal missing data categories and data sets that could potentially impact algorithm results.[125] The second target outcome is maintaining the data collected by reviewing its quality.[126] This goal of this policy is to maintain data quality for accurate results. Finally, the third and final target outcome for the

---

[122] Research and Data Plan, Equal Employment Opportunity Commission, https://www.eeoc.gov/eeoc/plan/research_data_plan.cfm.

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Id.*

EEOC's data plan is to use the knowledge gained from audits to further the goals of the agency.[127] This final outcome could prompt companies to make stronger commitments to equal employment across the country.

To report their commitment to equal employment, employers and recruiters could proffer a statement showing their commitment. The statement could include aspects of the algorithm that are already working towards diversity and inclusion. Like the Google example mentioned earlier about changing algorithm instructions to include behavior questions, an algorithm could be designed to diversify a workforce by either adding or removing instructions or data.[128] Other automated algorithm based companies, including Twitter and Yahoo, are also using algorithms to achieve more diversity in its workforce. These companies are trying to keep themselves accountable by disclosing their data results to their employees and making changes when necessary.[129]

This legislative recommendation could also adopt the APPS Act's notice requirement. Notice gives users or applicants an upfront understanding of the data collected and the data used. As under the APPS Act, these reports would include the personal data collected and the purpose for its collection. Additionally, it would report which third parties have access to the data and the company's data retention policy. This portion of the report would give applicants an understating of the automated algorithm and the data collected and used in making a hiring decision.

Instead of requiring employers and recruiters to provide customized reports for each individual request like in the EU, these reports would be broad and general to cover an entire applicant pool. Reports would only be required for an algorithm's initial debut, and every other year to account for any significant changes to the algorithm by the developer.[130] Finally, by keeping the EEOC's goals in mind, this legislative recommendation includes a commitment to achieving a diverse workforce that can ultimately promote positive changes in the use of automated algorithms.

This legislative recommendation is reasonable considering that the reporting system is proactive as opposed to reactive. The report will allow employers and recruiters to demonstrate transparency and a commitment to creating a diverse workforce before applying the algorithm to applicants. This recommendation can achieve a balance between the employers' benefits in using the algorithm while protecting the equal employment opportunity of the applicant. Reporting should be reasonable for employers and recruiters because the requirement is only a one-time full general report followed by any amendments made to the original report. This system could encourage competition among companies to improve hiring systems by directly addressing diversity in the workforce. Moreover, the report information will discourage automated algorithms that create disparate impacts.

---

[127] *Id.*

[128] Miller, *Hire Better, supra* note 37.

[129] *Id.*

[130] *See* EU Memo, *supra* note 105, at 98.

III. Conclusion

To establish a prima facie case for disparate impact, a potential plaintiff faces a high evidentiary burden to prove a specific practice or conduct caused the disparate impact. To stay accountable to Title VII of the Civil Rights Act, plaintiffs should have access to the information used by automated algorithms to make hiring decisions. This self-reporting requirement is a reasonable burden for employers and recruiters to meet because it requires a one-time original report and only updates every two years as necessary to address significant modifications to the original algorithm or data. Individuals should have an opportunity to understand the data that is being collected from them and how that data is being used. To avoid violating Title VII, employers should be transparent and accountable with the data they use and store. Ideally, transparency and accountability should be required of all automated algorithms used across the board in different industries.

Today, there is an ongoing conversation among scholars and the government regarding the potential harms that data and algorithms pose to our privacy and autonomy. This legislative recommendation will broaden the discourse among the public, legislators, scholars and so on. This reporting requirement will expose the data sets used to establish the "ideal candidate" by the algorithm and its instructions, thereby giving potential plaintiffs in disparate impact cases the evidence necessary to establish disparate impact. This is a common-sense bill that could be the stepping-stone to balance the advantages of using automated algorithms and an individual's privacy and autonomy.

ACKNOWLEDGMENTS

The IPLI depends upon the generous support of many people and organizations, including our Law Firm Fellows and mentors, government institutions, George Washington School of Law, law school professors, and other members of the bar. The HNBA and Microsoft would like to thank and recognize our IPLI community.

Law Firm Fellows and Mentors

Ballard Spahr 2017
Wendy Choi
Randall Towers

Cadwalader, Wichersham & Taft 2013-2014
Tihua Huang
Dorothy Auth
Rebekka Noll
Nick Locknauth

Covington & Burling 2013-2015
Enrique Longton
Michael Chajon
Tony Lopez
Peter Swanson

Davis Wright Tremaine 2013-2017
Peter Karanjia
Richard Gibbs
Ruben Pagan
Christopher Savage
Micah Ratner
Deirdre Davis
Brian Bentcover
Karen Ross

Ferraiouli LLC 2017
Eugenio Torres Oyola

Finnegan 2013-2017
Cecilia Sanabria
Clara Jimenez
Jorge Gonzalez
Naresh Kilaru
Kara Stoll
Anand Sharma
Frank Decosta

Fish & Richardson 2013-2017
Ahmed Davis
Daniel Gopenko
Cherylyn Mizzo
Indranil Mukerji
Timothy Riffe
Kevin Wheeler
Lee Gardner
Robert Devoto
Joshua Pond
Lauren Degnan
Ricardo Bonilla
Gwilym Attwell
Martina Hufnal

Gonzalez Saggio & Harlan 2013
Houda El-Jarrah

Lowenstein Sandler 2013-2015
Miguel Alexander Pozo
Vanessa Ignacio

Merchant & Gould 2013-2017
Tim Scull
Anthony Zeuli

Morrison & Foerster 2013-2017
Hector Gallegos
Corinna Alanis

Perkins Coie 2013-2017
Qudus Olaniran
Dennis Hopkins
Justin Moon
Elizabeth Mendoza
Alberto Araiza
Maurice Pirio

Sheppard Mullin 2013-2015
Jennifer Trusso Salinas
Andre De La Cruz

Shook, Hardy & Bacon 2013-2015, 2017
Jesse Camacho
Scott Strohm
Stephen Marshall
Daniel Tishman
Jay Newman
Linhong Zhang
Terry Mahn

Sidley Austin 2013-2017
Peter Choi
Michael Franzinger
Michelle Lyons
Anne Weinberg

Workman Nydegger 2017
Jens Jenkins

Law School Partners
George Washington University School of Law
2013-2017
Dean John Whealan 2013-2017

Professor Jorge Contreras (University of Utah S. J. Quinney College of Law) 2013-2017

United States Court of Appeals for the Federal Circuit
Circuit Judge Jimmie V. Reyna
2014 – Raquel Rodriguez
2015 – Clint South and Omar Amin
2016 – Sarah Jelsema and Alex Ruge
2017 – Samhitha Medatia and Andrew Wilhelm

Government Institutions
United States Patent and Trademark Office
Teresa Stanek Rea
Janet Gongola
Mariam Mahmoudi
Dana Colarulli
Scott Weidenfeller
Debbie Cohn
Tonya Gaskins
Scott Baldwin
James House
Shira Perimutter
Nestor Ramirez
Margaret Focarino
Rebecca Eisinger
Miriam Quinn
Caridad Berdut
Vikrum Aiyer
Leonardo Villarreal-Alejandro
Krista Contino Saumby
Diego Gutierrez
Merrell Cashion
Federal Trade Commission
Edith Ramirez
Suzanne Munck
Andrew Gavil
J. Maren Schmidt

Henry Su
Maren Schmdt
John Dubianski
Neal Hannan
Marina Lao
Kara Monahan

Copyright Office
Catherine Rowland
Erik Bertin
Kevin Amer
Abioye "Abi" Oyewole
Aurelia J. Schultz
John Saint Amour
Whitney Levandusky
Stephen Want

International Trade Commission
Chief Judge Charles Bullock
Irving A. Williamson
Jeffrey T. Hsu
Clark Cheney
Anne Goalwin
Erin Joffre
Sonia Murphy
Dee Lord
Margaret MacDonald
Lucy Noyola
Randy Weinsten
Clint Gerdine

The Judiciary Committees of the US House of Representatives and the US Senate
Alexandra Givens
Aaron Cooper
Joe Keely
Stephanie Moore
Matthew Sandgren, Sr.
Jason Everett
Elaine Gin
David Greengrass
Hakeem Jeffries

White House
Daniel H. MartÍ
US Trade Representative Stan McCoy

Speakers and Members of the Legal Community

Donald Dunner
Bob Stoll
George Pappas
Judge Peter J. Reyes
Horacio Gutierrez
Daniel H. MartÍ
Harry Gwinnell
Hector Gallegos
Bob Armitage
Jill Pietrini
Krista Contino Saumby
Mark Edwards
Ian Fried
Ian Slotin
Troy Dow
Bryan Zielinski
Christine Poleski Gaona
Robert Maldonado
Dave Green

American Intellectual Property Law Association
Clara Jimenez
Lissi Mojica
Diallo Crenshaw