ILLINOIS BUSINESS LAW JOURNAL

VOLUME 24
FALL 2018

*A PUBLICATION OF THE STUDENTS OF THE
UNIVERSITY OF ILLINOIS
COLLEGE OF LAW*

Illinois Business Law Journal

Volume 24 **2018**

ILLINOIS BUSINESS LAW JOURNAL

VOLUME 24 2018

CONTENTS

NOTES

VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

TOUCHING THE UNTOUCHABLES: REGULATING THE INTERNET OF THINGS INDUSTRY IN LIGHT OF THE EUROPEAN UNION'S UPCOMING E-PRIVACY REGULATION

❖ NOTE ❖

Clinton Oppong *

I. INTRODUCTION

Sometimes things seem all too familiar when what we see on television becomes perceptible in our lives. *Spoiler alert!* Facebook's sharing of its user data with Cambridge Analytica[1] reminds many of the plot of Westworld,[2] HBO's acclaimed television series set in a theme park called Westworld where "guests" (humans) interact with robots and play along in a storyline crafted by the Westworld corporation. The goal of the 'Westworld' corporation however is not merely to create an alternative world where guests can choose to pursue a second life; collecting data on guests is the core of Westworld's business model, and viewers and guests alike are oblivious as to what the corporation is using the data for.[3] In reality, many of the connected devices, or Internet of Things ("IoT") devices consumers use, collect data on consumers that is sometimes sold to third parties.[4] Like Westworld, the theme park is not really the product, the

[1] *See generally* Philip Bump, *Everything You Need to Know About the Cambridge Analytica-Facebook Debacle,* WASH. POST (Mar. 19, 2018), https://www.washingtonpost.com/news/politics/wp/2018/03/19/everything-you-need-to-know-about-the-cambridge-analytica-facebook-debacle/?utm_term=.894c89e1d3cb.

[2] *See* Kevin Fallon, *'Westworld' Season 2 Secrets Revealed: Facebook Data Collection, Badass Women and More,* DAILY BEAST (Apr. 20, 2018, 1:30 AM), https://www.thedailybeast.com/westworld-season-2-takes-on-facebook-data-collection-says-creator; *see also* Anna Menta, *'Westworld' Season 2 Premiere Hints At Facebook's Data Scandal,* NEWSWEEK (Apr. 22, 2018, 9:50 AM), https://www.newsweek.com/westworld-season-2-premiere-nods-facebook-data-scandal-889503.

[3] *See Westworld: Journey Into Night* (Home Box Office Apr. 22, 2018).

[4] *See* David Knight, *Who Owns the Data from the IoT?*, NETWORK WORLD (Jan. 30, 2017, 04:00 AM), https://www.networkworld.com/article/3152837/who-owns-the-data-from-the-iot.html; *see also* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping it Secret,* N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (On mobile devices, data collected from apps are sold to third parties who "use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior.").

*J.D. Candidate, Class of 2020, University of Illinois College of Law.

product is the consumer.[5] In many cases, this data is sold without the user's knowledge or informed consent.[6]

Such practices raise consumer privacy concerns, especially with the increasing security vulnerabilities associated with the connected devices consumers use such as connected cars, smart TVs, smart home devices, smart refrigerators, smart watches or fitness trackers, baby monitors, and pacemakers, to name a few.[7] These devices are classified as Internet of Things ("IoT") devices. The process by which consumer data is obtained from IoT devices has largely been unregulated in order to foster innovation in the tech industry.[8] The European Union, recognizing the security vulnerabilities of IoT devices, and the privacy concerns they raise, is now attempting to regulate IoT devices in the upcoming ePrivacy regulation.[9]

This Note argues that because of growing security and privacy issues associated with IoT devices, it is time for the United States to implement an IoT specific regulation similar to the ePrivacy Regulation. Part I is devoted to a brief discussion on what IoTs are, the breadth and scope of the upcoming ePrivacy regulation and how the ePrivacy regulation affects the IoT Industry. Part I also briefly discusses the current regulatory landscape in the United States. Further, Part II investigates why there is a need to regulate the Internet of Things Industry because of growing security and privacy issues. Finally, Part III puts forth recommendations for regulating the internet of things industry by the federal government or Federal Trade Commission (FTC).

II. BACKGROUND

A. What is Internet of Things?

The prominence of the internet has fueled inventors and tech companies to create products that connect consumers to technology, consumers to consumers, consumers to businesses, businesses to consumers, businesses to businesses, and businesses to technology.[10] Now, the

[5] *See* Danny Bradbury, *How Can Privacy Survive in the Era of the Internet of Things,* GUARDIAN (Apr. 7, 2015, 2:00 AM), https://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things (Discussing how connected devices are inexpensive because the device is not really the product, the consumer is).

[6] *See* Valentino-DeVries, *supra* note 4 (According to the authors of the article, many of these privacy policies are often ambiguous. For example, "[a]n app may tell users that granting access to their location will help them get traffic information, but not mention that data will be shared and sold.").

[7] *See e.g.* Danny Palmer, *IoT Security Warning: Your Hacked Devices are Being Used for Cybercrime Says FBI*, ZDNET (Aug. 3, 2018, 6:17 AM), https://www.zdnet.com/article/iot-security-warning-your-hacked-devices-are-being-used-for-cyber-crime-says-fbi/; Lily Hay Newman, *An Elaborate Hack Shows How Much Damage IoT Bugs Can Do*, WIRED (Apr. 16, 2018, 1:00 PM), https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/; Mayank Somani, *Connect the Dots: IoT Security Risks in an Increasingly Connected World*, SECURITY INTELLIGENCE (May 11, 2018), https://securityintelligence.com/connect-the-dots-iot-security-risks-in-an-increasingly-connected-world/.

[8] *See* Mauricio Paez & Keriabbe Tobit, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal* Issues, 62 N.Y. L. SCH. L. REV. 217, 245 (2017) (The authors argue that one of the main reasons why there is no regulation of the IoT industry in the US is because regulators do not want to hinder the freedom tech companies have in making new products).

[9] ***See Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications),*** **COM (2017) 10 final (Jan. 10, 2017) [hereinafter *ePrivacy Regulation*], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.**

[10] *See generally, Internet of Things (IoT) History,* POSTSCAPES (Aug. 20, 2018), https://www.postscapes.com/internet-of-things-history/ (Providing a history of IoT products).

internet has helped power a new spell of connectivity that allows for connections between 'things.'[11] These 'things' refer to a wide variety of connected devices such as smart wearables (including smart watches, activity trackers and smart glasses), smart speakers, smart TVs, smart refrigerators, smart homes, smart cities, smart grids (smart metering) blood pressure monitoring devices, baby monitors, autonomous vehicles and many more.[12] This new stage of connectivity is sometimes called machine-to-machine (M2M)[13] communications.[14] There is currently no general definition for the term Internet of Things.[15] Nonetheless, the term usually refers to "the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers."[16] Computers and mobile devices are typically not categorized as IoT even though they are internet connected devices made up of sensors.[17]

The basic IoT system is not complex to understand. "A complete IoT system integrates four distinct components: sensors/devices, connectivity, data processing, and a user interface."[18] First, an IoT is embedded with sensors that "detect and capture data from the surrounding environment,[19] including the people who own the objects."[20] The captured and detected data is subsequently transmitted via satellite, WiFi or Bluetooth[21] to a cloud.[22] Finally, "that data is then analyzed for insights and intelligence that will guide decision making."[23] That is, once on the cloud the data is processed,[24] and the information obtained from the data is usually sent to an end-user if there is a display interface.[25] Where there is no display interface, the processed information performs functions automatically.[26]

[11] *See* Steven Weber & Richmond Y. Wong, *The New World of Data: Four Provocation on the Internet of Things,* PEER REVIEWED JOURNAL ON THE INTERNET (Feb. 6, 2017), available at, https://firstmonday.org/article/view/6936/5859.

[12] *See generally* Knud Lasse Lueth, *The 10 Most Popular Internet of Things Applications Right Now,* IOT ANALYTICS (Feb. 2, 2015), https://iot-analytics.com/10-internet-of-things-applications/.

[13] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,* 21 RICH. J.L. & TECH 1, 7 (Calling IoTs "machine-to-machine connectivity and communications.").

[14] Some of the connected devices are controlled through an app on an end-user's phone. For example, in the smart home context, a smart home device like a thermostat is controlled from an app that is used to regulate temperature on an end-user's phone. *See* Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security,* 31 BERKELEY TECH. L.J. 997, 998 (2016).

[15] *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Business,* 43 N. KY. L. REV. 29, 31 (2016) (Stating that there is no "unified concept" for what internet of things are).

[16] KAREN ROSE ET. AL. INTERNET SOC'Y, THE INTERNET OF THINGS: AN OVERVIEW 12 (2015) *available at* https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf; *see also* Paez & La Marca, *supra* note 15, at 31 (Defining IoT as "the growing number of everyday physical objects or 'things' that have been embedded with technology to enable them to interact with the physical environment, people, and other devices in real time.").

[17] Paez & La Marca, *supra* note 15, at 31.

[18] Calum McClelland, *IoT Explained – How Does an IoT System Actually Work?*, IOTFORALL (Nov. 20, 2017), https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7.

[19] Sensors that can detect changes in environment include: temperature sensors (like infrared sensors), proximity sensors (like ultrasonic sensors), pressure sensors, water quality sensors, chemical sensors, gas sensors, smoke sensors, level sensors, motion detection sensors, accelerometer sensors, gyroscope sensors, humidity sensors, optical sensors, and image sensors. Rita Sharma, *Top 15 Sensor Types Being Used in IoT,* FINOIT https://www.finoit.com/blog/top-15-sensor-types-used-iot/ (last visited Feb. 28, 2019).

[20] Paez & La Marca, *supra* note 15, at 31.

[21] McClelland, *supra* note 18.

[22] Paez & La Marca, *supra* note 15, at 31.

[23] *Id.*

[24] McClelland, *supra* note 18.

[25] *Id.*

[26] *See id.* (Stating that "rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules.").

IoTs promise to usher in the Fourth Industrial Revolution.[27] A 2018 study by Cisco estimates that IoT connections are expected to grow from 6.1 billion in 2017 to 14.6 billion by 2022,[28] with "1.8 M2M connections for each member of the global population by 2022."[29] In another study, Cisco also estimates that by 2020, there will 37 billion new connected devices on the market.[30] As more consumers continue to use IoTs, the economic impact of the devices will grow substantially. According to McKinsey Global Institute, IoTs could generate as much as $11.1 trillion a year by 2025.[31] These devices will "offer the potential for improved health-monitoring, safer highways, and more efficient home energy use, among other potential benefits."[32]

Businesses are also taking advantage of IoT systems.[33] Mauricio Paez and Kerianne Tobitsch maintain that the prevalence and rise of IoTs "has the promise to revolutionize the industrial sector in the United States and around the World."[34] They note that companies can use a network of IoTs composed of electronic sensors and industrial internet software among others, to analyze data that will help "guide decision-making, improve safety and organizational processes, reduce waste, promote efficiency, and lessen environmental impact."[35]

Despite the popularity of IoTs, many consumers are unaware the ability of IoTs to cache personal data, which raises privacy concerns[36] related to collecting data.[37] In some cases, the data retrieved by IoT companies can be used to formulate daily data journals of consumers and corporations.[38] Moreover, for many IoT device manufacturers, manufacturing secure devices

[27] *See* World Economic Forum, *The Fourth Industrial Revolution,* YOUTUBE (Apr. 13, 2016), https://www.youtube.com/watch?v=khjY5LWF3tg; *see also* Mark Torr, *Defining the Fourth Industrial Revolution: Where IoT Fits and the Potential,* MICROSOFT (Aug. 22, 2016), https://news.microsoft.com/europe/features/defining-the-fourth-industrial-revolution-where-iot-fits-and-the-potential/ (Agreeing with the World Economic Forum's labelling of IoTs as the Fourth Industrial Revolution because of their economic and sustainable benefits to the environment).

[28] *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*, CISCO (Nov. 26, 2018), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

[29] *Id.*

[30] CISCO, THE INTERNET OF EVERYTHING AND THE CONNECTED ATHLETE: THIS CHANGES…EVERYTHING 2 (2013), *available at* https://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.pdf.

[31] JAMES MANYIKA ET. AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS 110 (McKinsey Global Institute June 2015), *available at* https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

[32] Press Release, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*,* (Jan. 27, 2015), [hereinafter FTC Report Press Release], https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

[33] *See generally,* Insights Team, *Five Ways IoT is Reinventing Businesses Today,* FORBES (Aug. 24, 2018), https://www.forbes.com/sites/insights-inteliot/2018/08/24/5-ways-iot-is-reinventing-businesses-today/#216683b21c20.

[34] Paez & Tobit, *supra* note 8, at 218.

[35] *Id.* at 219.

[36] *See infra* section II.A.2 (Discussing privacy risks associated with IoT devices).

[37] *See Privacy and IoT: Innovative Regulation Needed to Regulate Innovation,* INTERNET OF BUS. (Dec. 2. 2016), https://internetofbusiness.com/privacy-iot-innovative-regulations/.

[38] *See* Susan Morrow, *Five Reasons Privacy and IoT Are Incompatible,* IOTFORALL (Oct. 26, 2018), https://www.iotforall.com/five-reasons-privacy-iot-incompatible/.

is an afterthought.[39] As a direct result, many of the IoT devices used by consumers are embedded with lower levels of security.[40]

B. The ePrivacy Regulation

In the EU, all citizens have a fundamental right to privacy.[41] Jane E. Kirtley and Scott Memmel note that compared to the US, "the EU prefers an omnibus approach to privacy through implementation of an overarching, blanket law regulating privacy consistently across industries, providing certain rights to EU citizens regardless of context."[42] The EU is currently in the process of implementing an overarching privacy and electronic regulation due in the second half of 2019[43] called the ePrivacy Regulation to join the already enacted General Data Protection Regulation (GDPR).[44] EU legislators intend for the ePrivacy regulation to keep up with advancements in a rapidly growing tech industry.[45] Before the regulation comes into force however, the ePrivacy Directive[46] still controls this area. Unlike a regulation, a directive requires countries in the EU bloc to implement provisions through local regulations.[47] This often leads to inconsistencies in enforcement.[48] Legislators in the EU felt that in order to ensure the protection of EU citizens' rights to privacy in an internet-based world, more stringent measures were needed.[49] Originally intended to be released in tandem with the General Data Protection Regulation (GDPR),[50] the ePrivacy regulation will become the second part of the EU's data protection reform framework.

The ePrivacy regulation is a communications data regulation.[51] The regulation is intended to apply telecommunication companies, internet service providers (ISPs) and companies that process personal data.[52] Whereas the GDPR regulates how data is protected, the new ePrivacy

[39] *See* Thor Olavsrud, *Security an Afterthought in Connected Home, Wearable Devices,* CIO (Sept. 8, 2016), https://www.cio.com/article/3117396/security-an-afterthought-in-connected-home-wearable-devices.html.

[40] *See* Andrew Tannenbaum, *Why Do IoT Companies Keep Building Devices with Huge Security Flaws?,* HARV. BUS. REV. (Apr. 27, 2017), https://hbr.org/2017/04/why-do-iot-companies-keep-building-devices-with-huge-security-flaws ("The problem is that many IoT devices are not designed or maintained with security as a priority.").

[41] *See* Charter of Fundamental Rights of the European Union, 2010 O.J. C 83/02, at 389 (Mar. 30, 2010).

[42] Jane E. Kirtley & Scott Memmel, *Rewriting the Book of the Machine: Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 492 (2018).

[43] *See* Sandra Vogel & Dale Walker, *ePrivay Regulation: What is it and How Does it Affect me?,* ITPRO (Jan. 11, 2019), https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me.

[44] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (Regulating the processing of data on EU citizens).

[45] *See ePrivacy Regulation, supra* note 9, at 10 (Stating that there is a need to regulate because "important technological and economic developments" have taken place over the last decade).

[46] *See* Council Directive 2002/58/EC, 2002 O.J. (L 201) (EC).

[47] *See* I-SCOOP, THE NEW EPRIVACY REGULATION: WHAT YOU NEED TO KNOW (i-scoop.eu), https://www.iscoop.eu/gdpr/eueprivacyregulation/#EU_ePrivacy_from_a_Directive_to_a_Regulation.

[48] *Id.*

[49] *ePrivacy Regulation, supra* note 9, at recital 1.1.

[50] *See* Natasha Singer, *The Next Privacy Battle in Europe Is Over This New Law,* N.Y. TIMES (May 27, 2018), https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html (Stating that the reason why the ePrivacy regulation was not implemented in 2018 was because of internal disagreements).

[51] *See* Giovanni Buttarelli, *The Urgent Case for a New ePrivacy Law,* EUROPEAN DATA PROTECTION SUPERVISOR (Oct. 19, 2018), https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

[52] *See* Kirtley & Memmel, *supra* note 42 at 499. It should be noted that when it comes to regulating companies that process data, the ePrivacy regulation is not unique in this task. One of the main goals of the GDPR is to regulate the processing of

regulation will regulate the privacy of communications.[53] It will "address[] in detail the confidentiality of electronic communications, and the tracking of internet users more broadly."[54] The new regulation will further prohibit the "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, persons other than the end-users,"[55] without an end-user's consent.[56]

Outside the context of IoTs, the ePrivacy regulation would apply to "Over-the-Top" (OTT) providers such as WhatsApp, Facebook, Gmail, Skype, iMessage and Netflix among others.[57] EU legislators also intend to police internet cookies to prevent unwarranted marketing by companies.[58] Further, citizens are afforded broad consent rights; specifically, the draft proposal states that end-users who have "consented to the processing of electronic communications data…shall be given the possibility to withdraw their consent at any time…and [they] must be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues."[59]

Significantly, the provisions of the ePrivacy regulation will directly apply to M2M communications or IoTs. The draft regulation states that:

> In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure *Internet of Things* in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.[60]

The scope of the regulation is broad and encompassing. Legislators intend for the regulation to apply to all companies that provide connected services or devices with end-users.[61] The provisions of the regulation will directly apply to any EU or non-EU company that provides electronic communication services to an EU citizen.[62] Just like the GDPR, the cost of noncompliance is substantial. Violating the provisions will mean fines of up to €10 million or 2% of a company's annual revenue, which ever one is higher.[63]

data. *See* Danny Palmer, *What is the GDPR? Everything you need to know about the new general data protection regulations,* ZDNET (May 23, 2018, 05:28 AM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

[53] Buttarelli, *supra* note 51.

[54] Natasha Lomas, *ePrivacy: An overview of Europe's other big privacy rule change,* TECH CRUNCH (Oct. 7, 2018), https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/

[55] *ePrivacy Regulation, supra* note 9, at art. 5.

[56] *Id.* at art. 6.

[57] *Id.* at recital 1.1.

[58] *Id.* at recital 3.4–3.5

[59] *Id.* at art. 10.

[60] *Id.* at Proposal 12.

[61] This has been one of the major areas of contention with the regulation. Companies and even the United States Chamber of Commerce view this as "overly strict" and innovation stifling. *See* Singer*, supra* note 50.

[62] *ePrivacy Regulation, supra* note 9, at art. 3.

[63] *Id.* art. 23.

C. Current Regulatory Landscape in the United States

There is currently no overarching data privacy regulatory framework in the United States that polices data control or collection from IoT devices. Whereas the EU prefers an omnibus approach to protecting privacy, the United States prefers "a patchwork quilt of privacy laws that separately limit the use of Americans' medical records, credit reports…and so on."[64] But even with patchwork quilt privacy laws, data retrieved from IoT devices may not be covered. For example, healthcare data collected from fitness wearables like Fitbit or Apple Watch may not always fall under the Health Insurance Portability and Accountability Act (HIPAA) depending on who the data is shared with.[65] If the data from fitness wearables is shared with a healthcare provider or a doctor, that information is covered under HIPAA.[66] However, "HIPAA does not apply if the tech company does not share an end-user's health data with health-care providers,"[67] because manufacturers of fitness wearables are not defined as covered entities under HIPAA.[68] This means that fitness wearable manufacturers are free to utilize healthcare data retrieved from fitness wearables in any way they see fit, including sharing and selling of such data, provided such actions are listed in the terms and conditions of the fitness wearable's shrinkwrap agreement,[69] which consumers rarely read.[70]

The fact that HIPAA does not cover health data shared with third parties is no surprise given the FTC's self-regulatory approach to the IoT industry.[71] In lieu of having in place a robust regulatory framework, the FTC encourages IoT device manufacturers to follow "best business practices."[72] Some of these best practices include: security-by-design, privacy-by-design, notice and choice, security importance employee training, defense-in-depth strategies, and continuous device software updates to combat security risks.[73] However, the commission believes that Congress should look at implementing a substantive data security and breach notification law. Such calls have largely been disregarded by Congress.[74] On the state level,

[64] Natasha Singer, *Data Protection Laws, an Ocean Apart,* N.Y. TIMES (Feb. 2, 2013), https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html

[65] *See* Pamela Greenstone, *HIPAA guidelines should evolve with wearable technology,* THE HILL (Mar. 14, 2018 5:00PM), https://thehill.com/opinion/healthcare/378450-hipaa-guidelines-should-evolve-with-wearable-technology

[66] *See Id.*

[67] *Id.*

[68] *See* Nina Kostyukovsky, *Regulating Wearable Devices in the Healthcare Sector,* AMERICAN BAR (Sept. 27, 2018), https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2014-2015/may/devices/

[69] *See* Kristen Lee, *Wearable health technology and HIPAA: What is and isn't covered,* SEARCH HEALTH IT, https://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered (last visited Feb. 24, 2019)

[70] *See generally, See* Tess Wilkinson-Ryan, *A Psychological Account of Consent of Fine Print*, 99 IOWA L. REV. 1745 (2014) (Providing an in-depth analysis on a general reading problem related to modern consumer contracting).

[71] *See generally* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 48 (Jan. 2015) [hereinafter FTC IoT REPORT], https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf

[72] *See* FTC Report Press Release, *supra* note 32.

[73] *Id.*

[74] Although there is no substantive data security regulation, there have been two bills so far that have attempted to regulate some IoT. The first is a 2017 bill introduced by U.S. Senators Warner, Gardner, Wyden and Daines that attempts to improve cybersecurity of IoT devices bought by the government. The other is a bill introduced by former Michigan Rep. David Trott, called the "Internet of Medical Things Resilience Partnership Act of 2017, aimed at increasing the security and resilience of Internet of Medical Things devices." *See* Kirtley & Memmel, *supra* note 42 at 472–73.

California is the only state to have passed an IoT specific legislation aimed at ensuring that IoT devices are secure to prevent hacks and surveillance by cybercriminals.[75]

III. ANALYSIS

In a world of constant data breaches,[76] there needs to be greater attention devoted to regulating the IoT industry. Some analysts even believe that the worst has yet to happen.[77] In the tech industry, companies view any approach to regulate as an approach that restricts their innovative freedom and hinders their ability to drive up profits. On that matter, the FTC seems to agree with the tech industry. The commission's laissez faire, self-regulatory approach to IoT device manufactures as a way of combatting consumer privacy and security risks is clearly one that is geared towards protecting commerce rather than consumers. Jan Philipp Albrecht, a European Union legislator who worked on draft regulations for the GDPR, noted that in his view, "the U.S. Chamber of Commerce and Commerce Department are mostly just following the interest of Silicon Valley."[78] The transaction costs involved with self-regulation makes it even harder for such a policy to work, "because the responsibility of IoT privacy and security falls upon several actors in the IoT industry, including manufacturers, network providers, software developers, and others, [thus,] it is difficult for the industry to develop industry-wide standards."[79]

Consumers for their part do not think that the current self-regulatory approach protects their privacy. A study by Axios found that 83% of consumers want stricter regulations and more stringent sanctions for privacy breaches, while 67% also support implementing a regulation similar to the GDPR.[80] These results are perhaps born out of the increasing security and privacy risks associated with many IoT devices.

1. Security Risks and Vulnerabilities

Security vulnerabilities of IoT devices presents one of the primary reasons why there needs to be an IoT specific regulation. Because IoT devices are connected to the internet, they are as vulnerable to cyber-attacks[81] as traditional computers, however, with IoT devices, this vulnerability is especially heightened.[82] In fact, the current IoT security vulnerabilities is

[75] *See* Adi Robertson, *California just became the first state with an Internet of Things cybersecurity law*, THE VERGE (Sept. 28, 2018), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

[76] *See generally* Mike Snider, *Your data was probably stolen in cyberattack in 2018 – and you should care,* USA TODAY (Dec. 28, 2018), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/; *See also* Andrew Colley, *More that 80 percent of companies hit with IoT breaches,* CSO (Mar. 1, 2017), https://www.cso.com.au/article/615124/more-than-80-per-cent-companies-hit-iot-breaches-study/

[77] *See generally* Sooraj Shar, *Serious IoT data breach likely by 2020, say risk professionals,* INTERNET OF BUS. (Mar. 26, 2018), https://internetofbusiness.com/iot-data-breach-third-party/

[78] Singer, *supra* note 50.

[79] Kirtley & Memmel, *supra* note 42 at 471.

[80] *See* Kim Hart, *Americans Don't trust tech companies on data privacy,* AXIOS (Apr. 23, 2019), https://www.axios.com/distrust-social-media-firms-to-protect-privacy-survey-8b95db51-f137-46e3-a239-a5f304f0ac1b.html

[81] *See* Kirtley & Memmel, *supra* note 42 at 460.

[82] *See* FTC IoT Report, *supra* note 71, at 10.

similar to security vulnerabilities of computer devices in the early days of the internet[83] where "companies all over the world rushed haphazardly into the internet 'gold rush' without adequately addressing internet security. Viruses, worms, and spam subsequently descended on users. In many ways history may be repeating itself with IoT."[84] But, unlike computer systems that are frequently updated with patches to reduce and prevent cyberattacks, "many IoT devices have not been designed to use such patches in their software, leaving security issues unresolved."[85]

This IoT software security vulnerability stems from the inadequate firmware used in manufacturing some connected devices.[86] Because "embedding adequate levels of security into IoT devices would cost more, require specialized expertise, and may even involve product redesigns to accommodate different types of processors that power the security features,"[87] businesses and consumers are disadvantaged with IoT devices that are insecure.[88] A 2017 survey conducted by Altman Vilandrie & Company found that of approximately 400 IoT companies across 19 industries, 48% have experienced a data breach.[89] HP also conducted a survey in 2014 that found that there were around 25 security flaws associated with an average IoT device.[90] More worryingly, another study conducted by IBM and the Ponemon Institute found that "80% of organizations do not routinely test their IoT apps for security vulnerabilities."[91]

The FTC recognizes the security concerns associated with IoT devices. The commission noted in its 2015 report that security risks inherent in IoT devices "could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks."[92] Since that report was published consumers and businesses have been left to bear the burden of security flaws caused by insecure firmware associated with IoT devices. In 2016, IoTs and the internet in general, experienced the largest cyber-attack in history facilitated by a malware called Mirai Botnet,[93]

[83] *See generally,* Craig Timberg, *The real story of how the internet became so vulnerable,* WASH. POST, (May 30, 2015), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?noredirect=on&utm_term=.99d79ab9bba5

[84] Matt Toomey, *IoT Device Security is Being Seriously Neglected,* ABERDEEN (Feb. 5, 2018), https://www.aberdeen.com/techpro-essentials/iot-device-security-seriously-neglected/

[85] Kirtley & Memmel, *supra* note 42 at 461. Nick Ismail of Information Age gives a good summary of this problem: "Consider the operating systems for such [devices]. How do you upgrade the OS in a wall-mounted air conditioning unit that's connected wirelessly? Or a smart light bulb? If you can't upgrade an operating system, how can you attempt to patch any vulnerabilities?" Nick Ismail, *The Internet of Things: The security crisis of 2018?* INFORMATION AGE (Jan. 22, 2018), https://www.information-age.com/internet-things-security-crisis-123470475/

[86] *See* Toomey, *supra* note 84.

[87] *Id.*

[88] *See* Gary Eastwood, *4 critical security challenges facing IoT,* NETWORK WORLD (Feb. 7, 2017, 4:39AM), https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html

[89] *See Survey: Nearly Half of U.S. Firms Using Internet of Things Hit By Security Breaches,* BUS. WIRE, (June 1, 2017, 11:36AM), https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security

[90] *See,* Matthew Sparkes, *Average Internet of Things device has 25 security flaws,* THE TELEGRAPH (July 30, 2014, 11:26AM) https://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html

[91] Tannenbaum, *supra* note 40.

[92] FTC IOT REPORT, *supra* note 71, at 10.

[93] *See generally* Josh Fruhlinger, *CCTV cameras almost brought down the internet,* CSO (Mar. 9, 2018, 3:00AM), https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

which caused much of the internet to go down in the United States.[94] The perpetrators exploited insecure firmware flaws in IoT devices to pull off this attack.[95] The attack was successfully orchestrated by using mirai infected computers to "continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting [the IoTs] with malware."[96] Outside the U.S., a more alarming scenario presented itself with a hack on a smart electronic key system at a hotel in Austria "locking guests out of their rooms until the hotel paid ransom."[97] Hackers were able to compromise the key system because of inadequate security design and maintenance.[98] In the business setting, researchers at Senrio, an IoT-focused security firm, detailed how easy it is for hackers to hack into a business through weak IoT devices like security cameras as a pathway to access other company networks.[99] In the staged attack, researchers used a software tool to scan for vulnerable unpatched company security cameras "sitting on the public internet."[100] Such compromised security cameras can be used as an entry point to attack routers, allowing hackers to easily gain access to valuable company data.[101]

Despite the prevalence of these security risks and malware attacks, in 2017, a former FTC acting commissioner stated that she wanted IoT companies to continue to formulate best industry practices among themselves.[102] This statement is problematic given IoT manufacturers lax approach to solving security flaws in the face of increased malware attacks. As Bruce Schneier, Fellow and Lecturer at Harvard Kennedy School of Government puts it, "the market is not going to provide security on its own, because there is no incentive for buyers or sellers to act in anything but their self-interest."[103] IoT manufacturers will not take device security seriously unless a regulatory framework is in place.[104]

2. *Privacy Risks*

Unlike security flaws that may be resolved through technical solutions for ensuring data is protected outside regulations, IoT privacy issues cannot seriously be tackled outside regulations.[105] So far, the FTC's market approach has failed to ensure consumer privacy is protected. Companies are more concerned about their bottom dollar and the race to put new

[94] *See* Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say,* GUARDIAN (Oct. 26, 2016, 4:42PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (Stating that the attack caused websites like Twitter, the Guardian, Netflix, Reddit and CNN to go down).

[95] *See The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History,* IOTFORALL, (May 10, 2017), https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ [hereinafter *IoT Hacking and Vulnerabilities*]

[96] *Id.*

[97] Tannenbaum, *supra* note 40.

[98] *Id.*

[99] *See* Newman, *supra* note 7.

[100] *Id.*

[101] *Id.*

[102] *See* Sam Thielman, *Acting Federal Trade Commission head: internet of things should self-regulate,* GUARDIAN (Mar. 14, 2017, 6:00AM), https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation

[103] Press Release, Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices, (Aug. 1, 2017) [hereinafter Senate IoT Bill], https://www.warner.senate.gov/public/index.cfm/2017/8/senators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

[104] *See* Toomey, *supra* note 84.

[105] *See* Bryon Meyer, *Policy and Regulation in the IoT World: Should There Be Structure?*, ELECTRONIC ENGINEERING JOURNAL (Feb. 19, 2018) https://www.eejournal.com/article/policy-and-regulations-in-the-iot-world/.

products on the market that will become the next big thing. In fact, privacy rarely gets the much-needed attention it deserves by tech companies.[106] Data maximization seems to be the norm for companies in the tech industry where the practice is "keep the information until you run out of server space."[107] These companies are free to use the information they keep in any way they want, increasing concerns about misuse of sensitive consumer personal data.

The FTC is keenly aware of the risks posed by the data maximization practices of IoT companies. In a 2015 report,[108] the FTC noted that many IoTs devices collect sensitive personal information including consumer habits, physical conditions, health information, detailed geolocation, and financial account numbers,[109] all of which can be easily compromised given the major security risks posed by IoT devices.[110] This type of data harvesting, even in cases where consumers consent, can be used to create detailed and extensive data journals of consumers.[111] Absent a robust regulatory framework that polices the data maximization practices of IoT companies, sensitive behavioral patterns of consumers may be sold to other companies who may use the data obtained for insurance, credit, and employment decisions, among others.[112] What if, for example, car sensors that warn drivers about bad driving habits are used to deny consumers car insurance based on the data journals retrieved and sold to interested parties?[113] What if data retrieved from a consumer's Apple Watch is transmitted to your health insurance provider who uses it in insurance decision-making?[114] Perhaps, these questions and many more factored into decisions by EU legislators when deciding to regulate IoTs.

In addition, the ubiquity of IoT devices raises concerns about electronic surveillance. Because of the physical configuration of IoT devices (e.g. smart speakers, some smart wearables, smart toys, smart baby monitors)[115] consumers are sometimes unaware that they are being tracked or listened to because "conveying or updating a privacy policy or consenting to terms of service is not easily possible without a screen."[116] There have been instances where consumers have caught their Amazon Echo devices listening in on their conversations without engaging the devices' Alexa voice assistant.[117] In other instances, smart toys have been known

[106] *See* Rob Pegoraro, *Big tech firms still don't care about your privacy,* WASH. POST (Jan. 28, 2019), https://www.washingtonpost.com/outlook/2019/01/28/big-tech-firms-still-dont-care-about-your-privacy/?utm_term=.aee1b646a752 (Pointing out the simple steps that tech companies can take to protect privacy that they are currently neglecting).

[107] *Id.*

[108] FTC IOT REPORT, *supra* note 71, at 14–18.

[109] *Id.* at 14.

[110] *See Infra* section II.A.1 (Discussing security risks posed by IoT devices)

[111] *See* FTC IOT REPORT, *supra* note 71, at 15. (For example, the report noted that "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics…smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; level of exercise; and types of physical activity or movement").

[112] *Id.* at 16.

[113] *See* Bradbury, *supra* note 5.

[114] *See* FTC IOT REPORT, *supra* note 71, at 15-16 (Recognizing the risks posed by data journals retrieved from wearable fitness trackers).

[115] *See* Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier,* 51 U.C.D.L. REV. 475, 483 (2017)

[116] *Id.*

[117] *See e.g.* Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation,* N.Y. TIMES (Mar. 25, 2018), https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html; Will Oremus, *Terrifyingly Convenienty*, SLATE (Apr. 3, 2016, 8:04PM)

to listen in on conversations,[118] even prompting the FBI to release a report[119] warning consumers the security risks associated with some smart toys.

Relatedly, if IoT devices like the Amazon Echo can listen in on conversations, how long will it take before cyber criminals take advantage of security vulnerabilities inherent in some devices allowing them to eavesdrop on the private lives of consumers? Again, what if law enforcement agencies are able to tap IoT devices "leading to warrantless surveillance or illegal searches and recordings in violation of common law, privacy, and Fourth Amendment rights[?]"[120] As Laura DeNardis and Mark Raymond note "the private data collection of everyday objects and activities heightens opportunities for government surveillance of . . . everyday activities, whether for law enforcement, domestic or foreign intelligence gathering, or politically motivated tracking of dissidents and media."[121]

Some courts seem to be embracing the fact that devices like the Amazon Echo listen in on conversations. For example, a Judge in New Hampshire demanded Amazon hand over audio recordings that may help solve a murder case.[122] This raises questions about just how much information IoT devices retrieve, and how easy it may be for law enforcement agencies to gain access to consumer data that consumers had no knowledge was being collected. So where will the margin be drawn? "Will data be used for just violent crimes, or will law enforcement eventually want to pore over data for parking violations and minor misdemeanors?"[123]

There are more questions than answers, and without a robust framework that is geared towards targeting privacy risks associated with IoT devices, the widespread use of these connected devices may herald in a new era where an individual's privacy expectation is nothing but a relic. "Left unchecked, IoT devices could allow intrusive surveillance into the private spheres of individuals' lives."[124]

IV. RECOMMENDATIONS

Proponents of having no regulation of the IoT devices have raised concerns with EU legislators[125] that any regulation will lead to less innovation in the tech industry. Some have argued "that freedom to harvest personal data is needed in order to develop new technologies, such as artificial intelligence tools."[126] Others have argued that the regulation will make it too

http://www.slate.com/articles/technology/cover_story/2016/04/alexa_cortana_and_siri_aren_t_novelties_anymore_they_re_our_terrifyingly.html.

[118] *See* Elisabeth Leamy, *The Danger of giving your child 'smart'toys,* WASH. POST (Sept. 29, 2017), https://www.washingtonpost.com/lifestyle/on-parenting/giving-your-child-internet-connected-smart-toys-could-be-dumb/2017/09/29/a168218a-a241-11e7-8cfe-d5b912fabc99_story.html?utm_term=.9785bec5b592

[119] *See Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children,* FBI (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx

[120] Kirtley & Memmel, *supra* note 42, at 466.

[121] DeNardis & Raymond, *supra* note 115, at 482.

[122] *See* Chavie Lieber, *Amazon's Alexa Might be a key witness in a murder case,* VOX (Nov. 12, 2018 5:00 PM), https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data

[123] *Id.*

[124] Poudel, *supra note* 14, at 1013.

[125] *See* David Meyer, *Inside the ePrivacy Regulation's furious Lobbying war,* IAPP: PRIVACY ADVISOR, (Oct. 17, 2017), https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/ (European Legislator, Jan Philipp Albrecht noted that the tech industry has been engaged in a massive lobbying, with some in the industry going as far to say that the ePrivacy regulation will be the death of apps and free services online).

[126] Buttarelli, *supra* note 51.

costly for IoT manufacturers to produce new products.[127] But the security[128] and privacy risks[129] pointed out in this Note, highlight the need for an IoT specific regulation. Despite FTC recommendations,[130] IoT devices continue to be attacked by hackers. Without a robust mandatory regulatory framework, IoT manufacturers will not prioritize security and consumer privacy.

Moreover, the inherent lack of transparency of the data maximization practices of many firms in the tech industry amplifies the need for regulation.[131] Will it truly hurt companies to tell consumers if and when their data is being collected and what their data is being collected for? In most cases this will give companies the opportunity to develop consumer trust and openness. Surveys show that consumers are worried about privacy[132] and will take their business elsewhere if companies do not take security concerns seriously. For example, a survey conducted by PricewaterhouseCoopers (PWC) found that 85% of consumers will stop doing business with companies "if they have concerns about its security practices."[133] IoT device manufacturers should be cognizant of consumer perceptions and welcome an IoT specific regulation as a chance to develop trust and openness with consumers.

In the event that federal regulators decide to formulate an IoT specific regulation they should consider four key provisions as part of any regulatory framework: (1) Security by design and default, (2) Privacy by design and default, (3) Data Breach Notification, and (4) Sanctions.

1. *Security by Design and Default*

Security by design and default should be required for all IoT devices. This will require security to be embedded into every IoT device at the outset. Regulators should start at targeting security issues at the engineering level. This must include requiring IoT devices to have a minimum level of security. Here regulators can use the Senate bill authored by U.S. Senators Warner, Gardner, Wyden and Daines as a starting point in formulating a framework for all IoT devices on the market, and not just IoT devices purchased by the government.[134] The bill required IoT manufacturers to ensure that government purchased IoT devices are "patchable, do not include hard-coded passwords that can't be changed, and are free of known security

[127] *See* Bruce Gustafson, *Economic Impact of the prosed European ePrivacy Regulation,* DEVELOPERS ALLIANCE, (May 25, 2018), *available at,* https://webcache.googleusercontent.com/search?q=cache:7BV9IPTp0xMJ:https://www.orange.com/en/content/download/46903/1368006/version/2/file/Economic%252Bimpacts%252Bof%252Bthe%252Bproposed%252BEuropean%252BePrivacy%252BRegulation.pdf+&cd=9&hl=en&ct=clnk&gl=us&client=safari

[128] *See infra* section II.A.1.

[129] *See infra* section II.A.2.

[130] *See* FTC IOT REPORT, *supra* note 71, at 10.

[131] *See* Valentino-DeVries et al., *supra* note 4.

[132] For example, a survey conducted by Park associates on consumers who use smart home technologies found that "88% feel negatively about companies using their personal data to figure out when they are likely to be home." *See* Nicholas Shields, *New aurvey shows consumers are wary of smart devices invading their privacy,* BUS. INSIDER (Apr. 26, 2018), https://www.businessinsider.com/survey-says-consumers-have-privacy-concerns-with-smart-home-devices-2018-4

[133] PRICEWATERHOUSECOOPERS, CONSUMER INTELLIGENCE SERIES: PROTECT.ME, (2017), https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

[134] *See* Senate IoT Bill, *supra* note 103.

vulnerabilities."[135] Patching presents the biggest security vulnerability with IoT devices.[136] Regulators should look at requiring IoT devices to have built-in firmware that allows devices to be patched to ensure that software is frequently updated to prevent future cyber-attacks.

Elimination of hard-coded passwords that are set at the factory stage will also help curb security concerns.[137] Regulators should ensure IoT manufacturers design products that allow consumers to change factory set passwords.[138] In the event that certain IoT devices do not allow consumers to change factory default passwords, regulators should require IoT manufacturers to set passwords that are uniquely identifiable to the manufacturer. Giving consumers the opportunity to change passwords or requiring device manufacturers to use unique password credentials will further help alleviate security issues related to insecure web interface, insecure cloud interface, insecure mobile interface, and insufficient authentication.[139] The Mirai botnet attack[140] for example was made possible because the system of IoT devices hacked could not be patched because of existing firmware issues,[141] along with easily identifiable default passwords that were known to the hackers.[142]

2. *Privacy by Design and Default*

Like security by design and default, regulators must ensure that privacy is embedded at every stage of the data collection, data storage, and data sharing process. Data minimization and not maximization should be required for all companies in the IoT industry. This will mean implementing a provision similar to article 5 of the draft proposal of the ePrivacy regulation that prohibits "listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, persons other than the end-users" without an end-user's consent.[143] If a consumer consents, federal regulators should consider requiring IoT device manufacturers share consumer data journals with the consumer periodically, as well as allowing consumers the opportunity to have their data erased if collection practices are being used outside the purpose for which consent was giving.[144] Consumers should further be afforded broader consent rights and must be given the opportunity to retract their consent periodically if they do not consent to the data collection or data sharing practices of IoT device manufacturers.[145] Finally, it is also imperative that regulators clarify whether data journals of consumers retrieved from IoT devices can be obtained by courts and law enforcement without the consumer's consent.

[135] *Id.*

[136] *See* Xu Zou, *IoT devices are hard to patch: Here's why – and how to deal with security,* TECH BEACON, https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security (last visited Feb. 14, 2019).

[137] *See* Tannenbaum, *supra* note 40 (Stating that "many IoT devices share default user names and passwords that are well known and can be found with a quick Google search").

[138] *Id.*

[139] *See* Ashwin Pal, *The Internet of Things (IoT) – Threats and Countermeasures,* CSO, https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ (last visited Feb. 18, 2019).

[140] *See infra* section II.A.1.

[141] Fruhlinger*, supra* note 93.

[142] *IoT Hacking and Vulnerabilities*, *supra* note 95.

[143] *ePrivacy Regulation, supra* note 9, at art. 5.

[144] GDPR, *supra* note 44, at art 17.

[145] *ePrivacy Regulation, supra* note 9, at art. 10.

3. *Data Breach Notification*

To ensure transparency and trust with consumers and government officials, federal regulators should consider data breach notification requirements to both federal regulators and consumers. Regulators should require that IoT device manufacturers implement data breach notification protocols, similar to standards set by the EU in the GDPR.[146] For example, in the event of a data breach, companies are required to notify EU regulators within 72 hours of a data breach,[147] and must describe the gravity of the data breach,[148] names and contacts of consumers affected,[149] the consequence of the data breach,[150] and the measures taken to mitigate the effects of the data breach.[151] Since many of the IoT device manufacturers do business in the EU, it is possible that most of them already have systems in place to fall in compliance with the GDPR. Federal regulators should look into extending similar protocols to IoT companies who do business with American consumers.

4. *Sanctions*

To ensure full compliance with security and privacy safeguards, any regulation must consider levying administrative sanctions or fines. Here, regulators should look to other jurisdictions around the world that have data protection and privacy regulations to formulate sanctions that are necessary to ensure full compliance. For example, in France, sanctions include formal notices, warnings, injunctions and fines (under local laws and GDPR).[152] Across the EU, under the GDPR and ePrivacy regulations, failure to comply with the provisions of the regulations may lead to fines of €20 million or 4% of a company's annual revenue[153] and €10 million or 2% of a company's annual revenue respectively.[154]

V. CONCLUSION

It is time for federal regulators and the FTC to rethink self-regulation of IoT device manufacturers. In the FTC's 2015 report on the privacy and security concerns in a connected world, the FTC staff stated that, they do "not believe that the privacy and security risks, though real, need to be address through IoT-specific legislation at this time."[155] It has now been four years since that report was released. Since then, there has been an increase in IoT malware attacks that have compromised consumer security and privacy. Now more than ever, is the time for federal legislators to formulate a regulatory framework designed to police the IoT industry.

[146] *See* GDPR, *supra* note 44, at art. 33.

[147] *See Id.* at art. 33(1).

[148] *See Id.* at art. 33(1)(a).

[149] *See Id* at art. 33(1)(b).

[150] *See Id* at art. 33(1)(c).

[151] *See Id* at art. 33(1)(d).

[152] *See* Danhoe Reddy-Girard, *French Data Protection Rules,* 46 INT'L L. NEWS 11, 13–14 (2017).

[153] GDPR, *supra* note 44, at art. 83.

[154] *ePrivacy Regulation, supra* note 9, at art. 3.

[155] FTC IOT REPORT, *supra* note 71, at 48.

VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

ANOTHER BRICK IN THE WALL: THE *ILLINOIS BRICK* CO-CONSPIRATOR EXCEPTION'S TREATMENT BY UNITED STATES CIRCUIT COURTS

❖ NOTE ❖

Preslav Mantchev *

I. INTRODUCTION

The Supreme Court's 1977 ruling in *Illinois Brick Company v. Illinois* profoundly shaped private antitrust enforcement at the federal level in the United States. Yet, the Supreme Court's avoidance of subsequent questions stemming from its *Illinois Brick* ruling has created a circuit split regarding plaintiff standing in cases involving anticompetitive behavior by multiple co-conspirators. This Note examines the origins of this "co-conspirator" exception to *Illinois Brick* and analyzes the differences in the exception's treatment by circuit courts across the United States in order to promote a clearer, more-uniform application of the legal theory going forward.

II. BACKGROUND

The co-conspirator exception, along with all other exceptions to the *Illinois Brick* doctrine, arises under the Clayton Act of 1914.[1] The Clayton Act adds enforcement power to the Sherman Act of 1890 and together the two statutes comprise the United States' federal antitrust framework.[2] Specifically, section 4 of the Clayton Act provides that "any person who shall be injured in [their] business or property by reason of anything forbidden in the antitrust laws may sue therefor in any district court . . . ."[3] The provision thus allows a private right of action for businesses who deal with antitrust violators.[4]

[1] Illinois Brick Co. v. Illinois, 431 U.S. 720, 723 (1977).

[2] *See* 3 Federal Antitrust Law § 18.2 (2018).

[3] 15 U.S.C. § 15(a) (2012).

[4] Meagan P. VanderWeele, *In re ATM Fee Litigation: Ninth Circuit Uses Illinois Brick to Build a High Wall for Indirect Purchasers*, 12 DEPAUL BUS. & COMM. L.J. 121, 122 (2013).

*J.D. Candidate, Class of 2020, University of Illinois College of Law.

On its face, section 4 appears to permit claims by any party who can establish cause-in-fact between their injury and a defendant's antitrust violations. However, like in other legal relief frameworks such as tort law, a requisite degree of proximity is implied when a party claims antitrust damages against a defendant.[5] Given this implication, who has standing to sue for damages under American antitrust law, then?[6] The Supreme Court shed light on this question in the following case trilogy.[7]

Hanover Shoe v. United Shoe Machinery Corp. was a prelude to *Illinois Brick.* The case involved a shoe manufacturer alleging the defendant's "practice of leasing and refusing to sell . . . important shoe machinery" amounted to unlawful monopolization.[8] Plaintiff claimed damages for overcharges it absorbed in leasing the machinery from defendant.[9] Meanwhile, the defendant argued that plaintiff "suffered no legally cognizable injury" since the illegal overcharges were passed onto the plaintiff's customers in the form of higher shoe prices.[10] The Supreme Court held this cost shifting does not prevent damage recovery by plaintiff, who was a direct purchaser of defendant's machinery.[11]

Almost a decade later, *Illinois Brick Company v. Illinois* expanded on *Hanover Shoe*'s analysis. Plaintiffs in *Illinois Brick* included the State of Illinois and various municipalities who, unlike Hanover Shoe Company, did not purchase directly from the defendants.[12] Rather, plaintiffs were three levels removed as the defendant manufacturers sold bricks to masonry contractors, who then submitted bids to general contractors, who furthermore submitted project bids to the plaintiff municipal clients.[13] Thus, the Supreme Court considered whether a plaintiff can collect damages "in the context . . . in which the plaintiff, an indirect purchaser, seeks to show its injury by establishing pass-on by the direct purchaser . . . ."[14] The majority answered "no," citing risks of duplicative recovery and the immense difficulty of trying to apportion damages.[15] Nevertheless, the opinion acknowledged two exceptions to the general rule preventing recovery by indirect purchasers: "where 'an overcharged buyer has a pre-existing cost-plus contract'" with a seller,[16] and "where the direct purchaser is owned or controlled by its customer."[17]

The Supreme Court later reinforced its *Hanover Shoe* and *Illinois Brick* decisions in *Kansas v. Utilicorp United*. The case involved consolidated claims by both petitioner and respondent

[5] *See, e.g.*, SAS of Puerto Rico v. Puerto Rico Tel. Co., 48 F.3d 39, 43 (1st Cir. 1995).

[6] *See* Christopher T. Casamassima & Tammy A. Tsoumas, *The Illinois Brick Wall: Standing Tall*, 20 COMPETITION: J. ANTI. & COMP. L. SEC. ST. B. CAL 67, 67 (2011) ("Put simply, *Illinois Brick* addresses who can sue for damages under the Sherman Act.") [hereinafter Casamassima].

[7] *See* Hanover Shoe v. United Shoe Mach. Corp., 392 U.S. 481, 489 (1968) ("[W]hen a buyer shows that the price paid by him . . . is illegally high . . . . his right to damages is not destroyed."); Illinois Brick Co. v. Illinois, 431 U.S. 720, 726 (1977) ("[T]he issue is presented in the context of a suit in which the plaintiff, an indirect purchaser, seeks to show its injury by establishing pass-on . . . ."); Kansas v. Utilicorp United, Inc., 497 U.S. 199, 204 (1990) ("We must decide who may sue under § 4 . . . .").

[8] Hanover Shoe, 392 U.S. at 483.

[9] *Id.* at 483.

[10] *Id.* at 487-88.

[11] *Id.* at 493-94.

[12] *See* Casamassima, *supra* note 6, at 67.

[13] Illinois Brick Co. v. Illinois, 431 U.S. 720, 726 (1977).

[14] *Id.* at 726.

[15] *Id.* at 730-32.

[16] *Id.* at 724 n.2 (quoting Hanover Shoe v. United Shoe Mach. Corp., 392 U.S. 481, 494 (1968)).

[17] *Id.* at 736 n.16.

against a common set of defendants, a pipeline company and several gas producers.[18] Respondent had sued its suppliers alleging a conspiracy to inflate gas prices.[19] Petitioners, meanwhile, had filed their own suit against the defendants and claimed respondent's complaint lacked standing because respondent had passed on the inflated costs to Kansas citizens.[20]

Petitioners also asked for an exception "allow[ing] indirect purchaser in suits involving *regulated public utilities* that pass on 100 percent of their costs to their customers" and argued that *Illinois Brick*'s policy concerns were minimal in such a scenario.[21] The Supreme Court disagreed.[22] Recognizing the policy rationales behind *Hanover Shoe* and *Illinois Brick* may not always apply uniformly, *Utilicorp* nonetheless reinforced the Supreme Court's "belief that ample justification exists for our stated decision not to 'carve out exceptions to the direct purchaser rule for particular types of markets.'"[23]

Thus, the Supreme Court made clear that only an antitrust violator's direct purchasers may sue the violator for antitrust damages. Claims by indirect purchaser plaintiffs are blocked by the "*Illinois Brick* wall"[24] unless the direct purchaser had a cost-plus contract with the defendant, or the plaintiff owned or controlled the direct purchaser.[25] This is where the clarity ends, though. Despite having opportunities,[26] the Supreme Court failed to formulate a clear rule addressing situations where multiple parties coordinate uncompetitive behavior across multiple levels of a supply chain. Put differently, the Supreme Court declined to specify who can sue for damages when direct purchasers conspire with their supplier to violate antitrust law and injure others down the supply chain with inflated prices. Circuits have responded by formulating their own approaches to govern the standing of indirect purchasers who claim damages against co-conspirators. These approaches, discussed below, have been dubbed as a third, "co-conspirator" exception to *Illinois Brick*'s general indirect purchaser bar. Proper understanding of this exception is crucial in a modern outsourcing economy where supply chains consisting of independent contractors have largely replaced single, vertically integrated enterprises.[27]

III. Analysis

Circuits' treatment of the co-conspirator exception varies considerably. The Fourth and Ninth circuits construe the exception narrowly, applying it only in cases involving price-fixing by defendants. On the other side of the continuum, the Seventh and Eighth circuits construe the exception more liberally. A third group of circuits have illustrated the exception's procedural

[18] Kansas v. Utilicorp United, Inc., 497 U.S. 199, 204-05 (1990).

[19] *Id.* at 204.

[20] *Id.* at 204-05.

[21] *Id.* at 208. (*emphasis added*).

[22] *Id.*

[23] *Id.* at 216 (quoting Illinois v. Illinois Brick Co., 431 U.S. 720, 744 (1977)).

[24] *See* Kendall v. VISA U.S.A., Inc., 518 F.3d 1042, 1049 (exemplifying the "brick wall" metaphor).

[25] Illinois Brick, 431 U.S. at 724, 736.

[26] *See, e.g.*, Shamrock Foods Co. v. Arizona, 729 F.2d 1208 (9th Cir. 1984), *cert. denied*, 469 U.S. 1197 (1985); Iowa Beef Processors, Inc., v. Meat Price Investigators Ass'n (*In re* Beef Industry Antitrust Litig.), 607 F.2d 167 (5th Cir. 1979), *cert. denied*, 452 U.S. 905 (1981).

[27] *See generally* Simon Loertscher & Michael H. Riordan, *Make and Buy: Outsourcing, Vertical Integration, and Cost Reduction*, 11 Am. Econ. J.: Microeconomics 105, 105 (2019) (citing Josh Whitford, The New Old Economy: Networks, Institutions, and the Organizational Transformation of American Manufacturing (2005)).

requirements in a price-fixing context without expressly precluding its applicability to other uncompetitive behavior. Several other circuit courts of appeals have not considered the exception, thus allowing for wide commentary by district courts. Despite their contrasting rules, jurors on both ends of the continuum have also questioned the propriety of referring to uncompetitive conspiracies as an *Illinois Brick* "exception."[28]

A. The Fourth and Ninth Circuits – Strict Construction

The early 2000s' antitrust lawsuits involving Microsoft are widely remembered for their transformative effects on the internet browser and software industry.[29] In the Fourth Circuit, these proceedings also allowed the jurisdiction to formulate its narrow construction of the co-conspirator exception in *Dickson v. Microsoft*.[30] *Dickson* involved plaintiffs alleging a "hub-and-spoke" conspiracy between Microsoft and original equipment manufacturers.[31] The *Dickson* court acknowledged other circuits' treatment of the co-conspirator exception but elected to follow "the more narrow proposition that *Illinois Brick* is inapplicable to a more particular type of conspiracy – price fixing . . . ."[32] Since plaintiff alleged the co-conspirators' licensing agreements had restrained trade rather than set the resale price of software, plaintiff's claims were barred by *Illinois Brick*.[33]

The Ninth Circuit, meanwhile, first recognized the co-conspirator exception in *Arizona v. Shamrock Foods*.[34] In *Shamrock Foods*, plaintiffs alleged two types of "wholesale price-fixing conspiracy."[35] They "contend[ed] that the dairy producers conspired [1] among themselves *and* [2] with the grocery stores to raise and stabilize the *retail* price of dairy products to maintain more profits for all [co-conspirators]."[36] Thus, the defendants in *Shamrock Foods* were "both suppliers to and direct horizontal competitors with the [co-conspirator] grocery stores."[37] The Ninth Circuit favored plaintiffs based on their first theory and held *Illinois Brick* does not prevent claims against horizontal competitors engaged in price-fixing.[38] Furthermore, in dicta,[39] the court opined that "[e]ven if the plaintiffs were claiming a [vertical] conspiracy, we

[28] *See* Crayton v. Concord EFS, Inc. (*In re* ATM Fee Antitrust Litig.), 686 F.3d 741, 750 (9th Cir. 2012) ("As the district court aptly noted, this co-conspirator exception is not really an exception at all."); *see also* Paper Sys., Inc. v. Nippon Paper Indus. Co., 281 F.3d 629, 631-32 (7th Cir. 2002) ("The right to sue middlemen that joined the conspiracy is sometimes referred to as a co-conspirator 'exception' to *Illinois Brick* but it would be better to recognize that *Hanover Shoe* and *Illinois Brick* allocate the first non-conspirator in the distribution chain the right to collect 100% of the damages.").

[29] *See, e.g.*, Richard Blumenthal & Tim Wu, *What the Microsoft Antitrust Case Taught Us*, N.Y. TIMES (May 18, 2018), https://www.nytimes.com/2018/05/18/opinion/microsoft-antitrust-case.html.

[30] 309 F.3d 193, 215 (4th Cir. 2002).

[31] *Id.* at 198.

[32] *Id.* at 215.

[33] *Id.* at 199-200, 216.

[34] *See* Arizona v. Shamrock Foods Co., 729 F.2d 1208 (9th Cir. 1984); *see also* Casamassima, *supra* note 6, at 73 ("The exception traces its roots to a 1984 Ninth Circuit case, *Arizona v. Shamrock Foods Company*.").

[35] Shamrock Foods, 729 F.2d at 1211.

[36] *Id.* at 1210-11. (*emphasis added*).

[37] *Id.* at 1210.

[38] *Id.* at 1211.

[39] Casamassima, *supra* note 6, at 73.

[still] would hold that *Illinois Brick* is no bar . . . ."[40] This dicta created ambiguity in the ruling and hindered lower courts' subsequent application of the exception.[41]

In 2012, however, the Ninth Circuit decided *In re ATM Fee Antitrust Litigation*, which provided a more-robust discussion of the exception. *In re ATM Fee* reinforced how *Shamrock Foods* limited the co-conspirator exception's applicability to cases involving price-fixing.[42] In its ruling, the Ninth Circuit also clarified that regarding alleged vertical price-fixing conspiracies, plaintiffs' claims could only get past the *Illinois Brick* wall if "[d]efendants have conspired to fix the [final] price that [p]laintiffs paid directly."[43] Since the plaintiffs in *In re ATM Fee* alleged that defendants had conspired to set interchange fees (paid by banks) rather than the foreign ATM fees included in their final statements, their claims failed to overcome *Illinois Brick*'s indirect purchaser bar.[44]

Thus, in the Fourth and Ninth Circuits, the *Illinois Brick* wall stands formidably vis-à-vis plaintiffs wielding the co-conspirator exception. Here, the wall's narrow, selective openings only allow the passage of co-conspirator claims involving a fixed, final price.

B. The Seventh and Eighth Circuits – Simple Permissiveness

The Seventh Circuit's co-conspirator rule is articulated in *Paper Systems v. Nippon Paper Industries*.[45] Widely discussed by other jurisdictions,[46] *Nippon* involved defendants accused of conspiring to reduce fax paper output in order to raise the product's market price.[47] The Seventh Circuit favored the plaintiffs with a simple catch-phrase: "The first buyer from a conspirator is the right party to sue."[48] Thus, plaintiffs can collect damages from manufacturers and intermediaries simply if "conspiracy and overcharges can be established."[49] This approach does not require the fixing of a final price unlike the Fourth and Ninth Circuit rule. The Seventh Circuit instead "restrict[s] *Illinois Brick*'s influence by allowing an exception when the direct purchaser conspires with the seller, even though the price illegally set is an upstream cost that is passed-on to plaintiffs."[50]

The Eighth Circuit, meanwhile, articulated an approach similar to *Nippon* in its recent decision of *Insulate SB v. Advanced Finishing Systems*.[51] While discussing plaintiffs' antitrust standing, the Eighth Circuit reinforced an earlier ruling "that indirect purchasers may bring an antitrust claim if they allege the direct purchasers are 'party to the antitrust violation' and join

[40] Shamrock Foods, 729 F.2d at 1211.

[41] *See* Casamassima, *supra* note 6, at 74 ("More than twenty-five years later, the impact of the dicta in *Shamrock Foods* remains a subject of debate [in the Ninth Circuit].").

[42] Crayton v. Concord EFS, Inc. (*In re* ATM Fee Antitrust Litig.), 686 F.3d 741, 749 (9th Cir. 2012).

[43] *Id.* at 751.

[44] *Id.*

[45] 281 F.3d 629 (7th Cir. 2002). *See also* Fontana Aviation, Inc. v. Cessna Aircraft Co., 617 F.2d 478, 481 (7th Cir. 1980) (previewing the *Nippon* rule through dicta).

[46] *See* Dickson v. Microsoft Corp., 309 F.3d 193, 214-15 (rejecting *Nippon*); *In re* ATM Fee, 686 F.3d at 755 n.7 (arguing *Nippon* "contradicts [*Utilicorp*]'s admonition" against creating further exceptions to *Illinois Brick*). *But see, e.g.*, Laumann v. NHL, 907 F. Supp. 2d 465, 481-82 (S.D.N.Y. 2012) (favoring *Nippon*).

[47] Nippon, 281 F.3d at 631. Note how this behavior differs from price-fixing.

[48] *Id.*

[49] *Id.* at 632.

[50] Crayton v. Concord EFS, Inc. (*In re* ATM Fee Antitrust Litig.), 686 F.3d 741, 755 n.7 (9th Cir. 2012).

[51] 797 F.3d 538 (8th Cir. 2015).

the direct purchasers as defendants."[52] Although the insufficiency of plaintiffs' factual pleadings ultimately doomed their claim,[53] *Insulate SB* reveals the Eight Circuit, like the Seventh Circuit, prefers a broad application of the co-conspirator exception that extends beyond price-fixing. Plaintiff's initial complaint alleged that anticompetitive dealing arrangements between an equipment manufacturer and its distributors "forced [plaintiff] to pay an artificially high price."[54]

Overall, in the Seventh and Eighth circuits, the *Illinois Brick* wall remains fairly open to plaintiffs wielding the co-conspirator exception. It permits claims against a wide variety of uncompetitive behaviors, not just price-fixing. Accordingly, the resulting price inflation need not directly set the final price payed by the plaintiff.

C. The Middle Ground (Beef) Circuits

The following circuits "have not expressly required the alleged conspiracy to be one for price-fixing . . . ."[55] At the same time, this group has lacked opportunities to apply the exception outside of the price-fixing context.[56] Furthermore, several circuits in the group have reprimanded plaintiffs for failing to undertake procedural due diligence.[57]

The Fifth Circuit issued the earliest opinion in the group through its *In re Beef Industry Antitrust Litigation* ruling.[58] *In re Beef* involved consolidated claims by cattle ranchers alleging price-fixing at the retail level created a price depression that was "passed up the chain of distribution."[59] Plaintiffs argued two theories on appeal: First, that retailers had engaged in a horizontal conspiracy to fix the price of beef; Second, that retailers conspired with meatpackers in a vertical price-fixing conspiracy.[60] Plaintiffs prevailed on the first theory as the court found a functional equivalent of "cost-plus contracts" existing between the middlemen and price-fixing retailers.[61] However, the Fifth Circuit dismissed plaintiffs' "allegations . . . alleging vertical conspiracy."[62] Plaintiffs had failed to name the alleged co-conspirator middlemen as defendants in the original complaints despite having many opportunities to amend during trial.[63] Thus, the Fifth Circuit refused to apply the co-conspirator exception "absent joinder of the packers and slaughterhouses" because doing so could expose defendant retailers to an unfair risk of "overlapping liability."[64]

[52] *Id.* at 542 (quoting Campos v. Ticketmaster Corp., 140 F.3d 1166, 1170-71 nn.3-4 (8th Cir. 1998)).

[53] *Id.* at 546.

[54] *Id.* at 541.

[55] Marrero-Rolón v. Autoridad De Energía Eléctrica De P.R., 2016 U.S. Dist. LEXIS 193917, at *11 (D.P.R. 2016).

[56] *Id.* at *11.

[57] *See* Jewish Hospital Ass'n v. Stewart Mechanical Enterprises, 628 F.2d 971, 977 (6th Cir. 1980); *see also In re* Beef Indus. Antitrust Litig., 600 F.2d 1148, 1163 (5th Cir. 1979).

[58] *In re* Beef, 600 F.2d at 1148.

[59] *Id.* at 1153. *See also* Lowell v. Am. Cyanamid Co., 177 F.3d 1228, 1231-32 (11th Cir. 1999) (clarifying *In re Beef*'s factual background).

[60] *Id.* at 1153, 1160.

[61] *Id.* at 1163-66.

[62] *Id.* at 1163.

[63] *Id.* at 1161, 1163.

[64] *Id.* at 1163.

Similar reasoning guided the Sixth Circuit's decision in *Jewish Hospital Ass'n v. Stewart Mechanical Enterprises, Inc*.[65] The case involved an alleged conspiracy among contractors "to fix the price of mechanical (plumbing, heating, air-conditioning and sheet metal) work" on a hospital addition.[66] On appeal, the Sixth Circuit rejected plaintiffs' attempt to argue a vertical conspiracy.[67] "The problem with [plaintiff's] argument [wa]s that the Hospital ha[d] never pleaded the existence of a vertical conspiracy nor alleged facts sufficient to sustain such an allegation."[68] Thus, both the Fifth and Sixth circuits "reject[] . . . belated attempt[s] to argue the existence of a vertical conspiracy."[69] In doing so, they articulate a requirement which appears to be implicit in at least one of the circuits discussed earlier.[70]

The Eleventh Circuit, meanwhile, was carved out of the Fifth Circuit in 1981.[71] *In re Beef* still carries weight in the Eleventh Circuit as do other Fifth Circuit pre-split decisions.[72] But, the Eleventh Circuit refined *In re Beef*'s co-conspirator rule in *Lowell v. American Cyanamid*.[73]

Lowell involved plaintiff farmers who "appealed a district court order dismissing [their] antitrust complaint for failure to join middlemen dealers as defendants pursuant to [*Illinois Brick*]."[74] The Eleventh Circuit reversed the district court by distinguishing plaintiffs' claims from those in *In re Beef*.[75] Unlike the *In re Beef* ranchers, *Lowell*'s plaintiffs alleged only "a vertical conspiracy with no allegations of 'pass-on.'"[76] The scheme between American Cyanamid and its dealers set the product price directly billed to farmers.[77] Thus, farmers did not have to join the middlemen but could sue American Cyanamid directly.[78] The Eleventh Circuit emphasized that "*In re Beef* is consistent with the rul[ing]."[79] The two decisions' consistency is rooted in the earlier distinction: *In re Beef* involved an alleged horizontal conspiracy which passed-on price depression to the farmers, while *Lowell* involved a vertical scheme which directly set the farmers' final price.[80] The Eleventh Circuit reasoned *Illinois Brick*'s policy concerns simply do not apply to the latter type of conspiracy.[81] What distinguishes *Lowell* from *Nippon*, however, is its silence on whether the farmers would still win if American Cyanamid conspired with distributors to reduce product output, for example.

[65] Jewish Hospital Ass'n v. Stewart Mechanical Enterprises, 628 F.2d 971, 977 (6th Cir. 1980).

[66] *Id.* at 972.

[67] *Id.* at 977.

[68] *Id.*

[69] *Id.*

[70] *See* Insulate SB, Inc. v. Advanced Finishing Sys., 797 F.3d 538, 542 (8th Cir. 2015) ("[I]ndirect purchasers may bring an antitrust claim if they allege the direct purchasers are 'party to the antitrust violation' *and* join the direct purchasers defendants.") (*emphasis added*).

[71] *See* Fifth Circuit Court of Appeals Reorganization Act of 1980, Pub. L. No. 96-452 (1980).

[72] Bonner v. Prichard, 661 F.2d 1206, 1207 (11th Cir. 1981).

[73] Lowell v. Am. Cyanamid Co., 177 F.3d 1228, 1228 (11th Cir. 1998).

[74] *Id.*

[75] *Id.* at 1231-33.

[76] *Id.* at 1230.

[77] *Id.* at 1228-29.

[78] *Id.* at 1233.

[79] *Id.* at 1232.

[80] *Id.*

[81] *Id.* at 1232-33.

Lastly, the Third Circuit provides the most-liberal construction of the co-conspirator exception outside of the Seventh and Eighth circuits through its rulings in *Howard Hess Dental Labs v. Dentsply International* and *In re Linerboard Antitrust Litigation*.[82]

Hess involved consolidated appeals arising from both price-fixing and exclusive dealing conspiracy allegations against an artificial tooth manufacturer and its distributors.[83] The Third Circuit dismissed one set of plaintiffs because they failed to join the dealers who were "immediately upstream,"[84] in what the court viewed as "effectively a horizontal price fixing conspiracy at the dealer level . . . ."[85] Taken at face value, this holding shows the Eleventh Circuit's procedural stringency is in line with *In re Beef* and *Jewish Hospital*. The second set of plaintiffs, meanwhile, had antitrust standing according to the Third Circuit but only with respect to their retail price-fixing claims.[86] But, their exclusive dealing claims could only proceed if the co-conspirator middlemen were barred from suing the manufacturer due to their "totally complete" involvement in the conspiracy.[87] The Third Circuit reached this result by electing to adopted a "'limited' general" co-conspirator exception, which it juxtaposed to the Seventh Circuit's "general" exception in *Nippon*.[88] The Third Circuit was unsatisfied with *Nippon*'s lack of explanation and delineation of the "general" co-conspirator exception's limits.[89]

Through *In re Linerboard*, however, the "'limited' general" exception still maintains substantial breadth. Here, the Third Circuit ruled that output agreements by co-conspirators constitute price-fixing under the co-conspirator exception.[90] Furthermore, the court reiterated there is no bar against plaintiffs who directly purchase from an offender a product incorporating an ingredient whose price had been fixed.[91]

Thus, the Third Circuit illustrates procedural stringency similar to the Fifth, Sixth, Eight, and Eleventh Circuits. The Third Circuit rule also resembles the Seventh and Eighth Circuit more than other circuits in this group given how it broadly construes the co-conspirator exception by inconspicuously applying the exception to behavior beyond price-fixing.

In sum, the middle ground circuits have lacked opportunities to evaluate claims under the co-conspirator exception outside of a price-fixing context. Only one circuit, the Third, has accommodated anticompetitive behavior beyond price fixing into the exception albeit under the guise of equating such behavior to price fixing. Together, these circuits underscore the importance of plaintiffs joining co-conspirators as defendants during pleading in order to maximize the durability of their antitrust claim, especially when alleging vertical conspiracies involving pass-on. Plaintiffs should be diligent if they attempt to pass the *Illinois Brick* wall with a co-conspirator exception in the Third, Fifth, Sixth, and Eleventh circuits. While the Third Circuit provides some openings, other parts of the wall remain obscured.

[82] 424 F.3d 363 (3d Cir. 2005); 305 F.3d 145 (3d Cir. 2002).

[83] Howard Hess Dental Labs, Inc. v. Dentsply Int'l, Inc., 424 F.3d 363, 366 (3d Cir. 2005).

[84] *Id.* at 371.

[85] *Id.* at 378 n.12.

[86] *Id.* at 378.

[87] *Id.* at 383-84.

[88] *Id.* at 379 n.13.

[89] *Id.*

[90] Winoff Indus. v. Stone Container Corp. (*In re* Linerboard Antitrust Litig.), 305 F.3d 145, 159-160 (3d Cir. 2002).

[91] *Id.* at 159.

D. The First, Second, and Tenth Circuits – A Clean Slate

The circuits in this last group have yet to issue binding precedent governing *Illinois Brick*'s co-conspirator exception. Until that occurs, our analysis is limited to developments at the district court level and appellate courts' treatment of other *Illinois Brick* exceptions.

The Second Circuit Court of Appeals has not addressed the co-conspirator exception.[92] In *Laumann v. NHL*, however, the Southern District of New York discussed the exception in a recent class action suit against two professional sports leagues for allegedly conspiring with regional sports networks and multichannel video distributors to inflate the price of "out-of-market" game broadcasts.[93] The district court unequivocally favored the Seventh and Third Circuit precedent after juxtaposing it to the Fourth and Ninth circuits' approach.[94] Thus, in *Laumann*, the Southern District of New York held that since the middlemen – regional sports networks and multichannel video distributors – were "alleged to be participants in the conspiracy, the first purchasers who are not part of the conspiracy 'are entitled to collect damages . . . .'"[95] The parties in *Laumann* ultimately settled before any issues involving plaintiffs' antitrust standing were appealed to the Second Circuit.[96] Accordingly, the Second Circuit Court of Appeals will have to wait before ruling on whether to affirm *Laumann*'s affinity towards the Seventh and Third Circuit constructions of the co-conspirator exception.

The First Circuit Court of Appeals has not addressed the co-conspirator exception, either.[97] This void, however, has allowed for extensive commentary on the exception's merits by the District Court of Puerto Rico.[98] In *Marrero-Rolón v. Autoridad De Energía Eléctrica De Puerto Rico*, the District Court of Puerto Rico examined a complaint alleging the island's power agency corruptly conspired with petroleum dealers to burn substandard fuel at inflated prices for electric ratepayers.[99] Magistrate Judge Silvia Carreño-Coll criticized *Dickson* and *In re ATM Fee*, characterizing the rulings as "mis- or over-interpretation[s] of *Utilicorp*'s and *Illinois Brick*'s caution against creating exceptions for specific markets . . . ."[100] Judge Carreño preferred to follow the Seventh Circuit's *Nippon* approach instead like the Southern District of New York did in *Laumann*.[101] The District of Puerto Rico affirmed Carreño's approach in an interlocutory appeal one year later.[102]

Lastly, the Tenth Circuit's construction of other *Illinois Brick* exceptions may provide clues about its potential treatment of co-conspirator claims. In *Zinser v. Continental Grain Co.*, the

[92] Laumann v. NHL, 907 F. Supp. 2d 465, 481 (S.D.N.Y. 2012).

[93] *Id.* at 471.

[94] *Id.* at 483.

[95] *Id.* at 482 (citing Paper Sys., Inc. v. Nippon Paper Indus. Co., 281 F.3d 629, 632 (7th Cir. 2002).

[96] *See* Garber v. Office of the Comm'r of Baseball, 2016 U.S. Dist. LEXIS 18011 (S.D.N.Y. 2016) (approving parties' proposed settlement).

[97] *See* Marrero-Rolón v. Autoridad De Energía Eléctrica De P.R., 2015 U.S. Dist. LEXIS 134211, at *35 (citing Sullivan v. NFL, 34 F.3d 1091 (1st Cir. 1994)). [hereinafter Marrero I]. The cited precedent only addresses damage recoveries by party within a conspiracy.

[98] *See* Marrero I, *supra* note 97 at *33-40; *see also* Marrero-Rolón v. Autoridad De Energía Eléctrica De P.R., 2016 U.S. Dist. LEXIS 193917, at *11 (D.P.R. 2016) [hereinafter Marrero II].

[99] Marrero I, *supra* note 97, at *6-10.

[100] *Id.* at *35 n.23.

[101] *Id.*

[102] Marrero II, *supra* note 98, at *10 ("The court's holding as to this issue is consistent with the approach used by the Seventh Circuit . . . .").

Tenth Circuit compared plaintiffs' "cost-plus" exception claims to those *In re Beef*.[103] While doing so, the *Zinser* court noted "exceptions to Illinois Brick are exceedingly narrow in scope, and . . . should be few in number. . . . [A]ny exception should not be given an expansive application, lest it swallow the rule and become the rule itself."[104] The Tenth Circuit reiterated this prescription eight years later in *In re Wyoming Tight Sands Antitrust Cases*.[105] Thus, the Tenth Circuit's treatment of *Illinois Brick*'s cost-plus exception suggests the court will likely favor a limited construction of the co-conspirator exception like the Fourth and Ninth Circuits.

Overall, the First, Second, and Tenth Circuits have a clear foundation for constructing their *Illinois Brick* wall vis-à-vis the co-conspirator exception. District courts have sketched some blueprints which could be influenced by appellate constructions of other *Illinois Brick* exceptions. Time will tell if the appellate courts will adopt, disregard, or modify these blueprints.

IV. Conclusion

Regardless of whether it is viewed as an exception to *Illinois Brick* or a "fundamentally different factual scenario,"[106] circuits across the United States have widely debated exactly when *Illinois Brick* bars suits by parties who allege injury from anticompetitive behavior coordinated by multiple conspirators.

Courts are conflicted on whether to consider plaintiffs dealing with a participant in an anticompetitive conspiracy as "direct purchasers" from the entire conspiracy (and therefore not subject to *Illinois Brick*'s indirect purchaser bar at all) or "indirect purchasers" from an antitrust violator who hides behind co-conspiring middlemen (but still exempt from *Illinois Brick*'s indirect purchaser bar via the co-conspirator exception). Besides nomenclature disagreements, courts are also divided on how to apply the co-conspirator exception's substance. Some circuits only allow plaintiffs standing if their alleged conspiracy fixed the price they directly paid or received. Other circuits allow plaintiffs standing even if the conspirators engaged in other anticompetitive behavior which harmed plaintiffs financially (e.g., reducing output). Thus, both the theory's nomenclature and substantive applicabilition lack uniformity.

This issue can be cured in two ways. First, the Supreme Court could provide uniformity by issuing a writ of certiorari for a case disputing plaintiff's standing under the co-conspirator exception. Ideally, the Court would not only resolve the question presented, but also discuss the exception's applicability to other types of anticompetitive conspiracies and provide reasoning for its decision to favor or reject the lower Circuit. Such a broad ruling is not guaranteed, though. For instance, the Supreme Court could issue a writ of certiorari on a Third Circuit case and simply uphold the Third Circuit's equation of output agreements to price fixing without discussing the exception's substantive merits against defendants who abuse exclusive

[103] Zinser v. Continental Grain Co., 660 F.2d 754, 760-61 (10th Cir. 1981).

[104] *Id.* at 761.

[105] *See In re* Wyoming Tight Sands Antitrust Cases, 866 F.2d 1286, 1293 (10th Cir. 1989) (construing the "cost-plus" exception narrowly).

[106] Marrero I, *supra* note 97, at *35 n.23.

licensing agreements as in the Eighth Circuit.[107] This reactive solution also requires parties willing to absorb the extensive costs of litigating up to the Supreme Court.

Alternatively, a more-proactive solution would be for Congress to amend the section 4 of the Clayton Act and specify plaintiffs' standing in various contexts by codifying one of the circuit rules discussed earlier. Section 4 appears ripe for this kind of reform given it already restricts the amount of interest and damages certain plaintiffs may claim.[108] Amending the Clayton Act would be presumably revenue-neutral, possibly sparing the solution from recent congressional impasses.[109] Nevertheless, reforms affecting the rights of sophisticated private actors tend to be prime candidates for politicization.[110] Thus, it remains unclear whether Congress can deliver uniformity more quickly than the Supreme Court. For now, though, the litigation continues.[111]

[107] *See* Insulate SB, Inc. v. Advanced Finishing Sys.,797 F.3d 538, 541 (8th Cir. 2015).

[108] *See* 15 U.S.C. §§ 15(a)(1-3) (2019) (limiting interest amounts); 15 U.S.C. § 15(b) (2019) (limiting foreign parties' damage amount entitlements).

[109] *See generally* PEW RESEARCH CENTER, *Three Decades of Congressional Productivity, 1987-2017*, https://www.pewresearch.org/fact-tank/2019/01/25/a-productivity-scorecard-for-115th-congress/ft_18-01-09_congressproductivity/ (last visited May 15, 2019) (indicating a lower amount of substantive public laws passed by Congress in recent years).

[110] *See generally* LEE DRUTMAN, THE BUSINESS OF AMERICA IS LOBBYING: HOW CORPORATIONS BECAME POLITICIZED AND POLITICS BECAME MORE CORPORATE 73 (2015) (suggesting "Need to protect against changes in government policy . . . that could be harmful" is companies' most-important reason for lobbying).

[111] *See, e.g.*, Marion Diagnostic Ctr., LLC, v. Becton, Dickinson & Co., 2018 U.S. Dist. LEXIS 203407 (S.D.I.L. 2018), *appeal docketed*, No. 18-03735 (7th Cir. Dec. 28, 2018).

VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

REVERSE ENGINEERING: RECONCILING TRADE SECRET LAW WITH 3D PRINTING AND SCANNING

❖ NOTE ❖

Prateek Viswanathan *

I. INTRODUCTION

Trade secret laws are unprepared for 3D printing and scanning's effect on reverse engineering. These laws give inventors a cause of action if another party misappropriates their trade secret.[1] However, these inventors cannot prevent competitors from reverse engineering and using their trade secrets.[2] Reverse engineering, the study of a product to discover its trade secret, benefits society by advancing innovation and reducing prices, but does not prevent the first inventor from recouping R&D expenses before facing competition, because it costs time and money.[3] However, if reverse engineering becomes too cheap, it may cause market destructive effects; Inventors cannot rely on such trade secrecy protection,[4] and would incur societal costs by submitting too many patent applications or implementing costly reverse engineering countermeasures.[5] 3D printing and scanning can cheapen reverse engineering and

[1] *See* Defend Trade Secrets Act, 18 U.S.C. Section 1832.; *See also* UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985); *See also* Economic Espionage Act, Section 1, 18 U.S.C. Section 1831; *See also* Restatement Third of Unfair Competition, Chapter 4, Appropriation of Trade Values.

[2] *See* 765 ICLS 1065/2 (a)-(d). The Illinois trade secret statute finds that reverse engineering is a proper means of appropriation.

[3] *See* RICHARD A. POSNER & WILLIAM M. LANDES, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 365 (2003).

[4] *See* Samuelson & Schotchmer, *The Law and Economics of Reverse Engineering*, YALE LAW JOURNAL, 1595 (2002.) (providing a full treatment of reverse engineering's law and economics circa 2002.)

[5] *See* POSNER, *supra* note 3; Samuelson, *supra* note 4 (providing a full treatment of reverse engineering's law and economics circa 2002.).

*J.D. Candidate, Class of 2021, University of Illinois College of Law.

undermine trade secrecy laws in multiple industries. This method duplicates engines and medical devices in weeks,[6] but can duplicate even food compositions or circuit boards.[7]

This Note proposes requiring competitors to sell original products if they reverse engineer competing products with 3D scanning and printing. This proposal would mitigate market destructive effects by providing first inventors lead time to recoup R&D expenses. Part II of this Note provides background on 3D printing and scanning, Illinois's trade secrecy law, and reverse engineering. Part III analyzes how 3D printing and scanning may make reverse engineering market destructive and stress the patent system. Part IV proposes a localized solution by amending Illinois's statute to require originality in competing products.

II. Background

3D scanning uses electronic and light-based probes to determine the exterior and interior structure of an object and render it into a computer-readable file.[8]This technology can be applied to cars, aircraft, and other high-precision industries.[9] 3D printing, otherwise called "additive manufacturing," is a collection of techniques that build a product in layers according to a digital map, instead of removing pieces from a block.[10] These techniques have reduced reverse engineering time in industrial manufacturing,[11] prototyping,[12] in circuit boards and semiconductor chip layouts,[13] and in food manufacturing.[14] Complete reverse engineering can

[6] *See* Beau Jackson, 3DP Applications (last updated Dec. 15th, 2016 3:04 PM), https://3dprintingindustry.com/news/3d-printing-reverse-engineering-world-101166/; *See also* 3D Scanning Services, Arrival 3D, https://arrival3d.com/3d-scanning-services/ (quoting 3-5 days for a simple scan); 3D Scanning FAQs, 3D ScanCo, https://www.3dscanco.com/3d-scanning-faqs/ (quoting 2 weeks or less for any scan); General Questions, Ultimaker, https://ultimaker.com/en/resources/11721-general-questions (10 minutes for simple low-quality printing to a few hours for high quality complex products).

[7] *See* Ian Steadman, *Open Source cola and the Napster moment for the food business*, WIRED Mag. (Apr. 15, 2013), https://www.wired.co.uk/article/trade-secrets-open-source-cola. (Arguing that while barriers to chemical and food reverse engineering currently exist, they will be surmounted.); *See also* Scio Solutions, SCIO (Last updated 2017), https://www.consumerphysics.com/business/solutions/ (showing the business website of a chemical scanner, promising to determine the molecular composition – while it does not read out the recipe immediately, it shortens reverse engineering time.); See Lucas Mearian, *Desktop 3D Printer presages the future of multi-layer circuit design*, ComputerWorld (May 10, 2017), https://www.computerworld.com/article/3195839/3d-printing/desktop-3d-printer-presages-the-future-of-multi-layer-circuit-board-design.html (discussing Nano Dimensions' Dragonfly 2020, a desktop printer capable of reducing circuit board prototypes from weeks to hours); See *Loud and Clear: 3D Scanning Perfectly Reproduces Miniaturized Printed Circuit Boards for Microphone Products*, LaserDesign, *https*://www.laserdesign.com/loud-and-clear-3d-scanning-perfectly-reproduces-miniaturized-printed-circuit-boards-for-microphone-products/ (discussing the use of 3D scannings to replicate a microphone's circuit board.)

[8] Bernadini and Rushmeier, *The 3D Model Acquisition Pipeline, Computer Graphical Forum*, 2002, 1.; See also Jim Romeo, https://blog.grabcad.com/blog/2018/09/20/why-3d-scanners-are-the-hot-new-craze-in-reverse-engineering/

[9] Bernadini, *supra* note 8.

[10] Cecile J. Gonzalez, *The Engineering Behind Additive Manufacturing and the 3d Printing Revolution*, NAT'L SCI. FOUND. (Dec. 3, 2013), https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=129780 ("Additive manufacturing is a way of making 3-D objects by building up material, layer upon layer, with the guidance of a digital design.")

[11] *See* John Hagel et. Al., *The Future of Manufacturing: Making Things in A Changing World*, Del. Univ. Press., 2015 at 20 (illustrating the decrease in barriers to commercialization); *See also* Jim Romeo, *Why 3D Scanners are the Hot New Craze in Reverse Engineering,* Grabcad (Sept. 20, 2018), https://blog.grabcad.com/blog/2018/09/20/why-3d-scanners-are-the-hot-new-craze-in-reverse-engineering/, (illustrating the different applications of 3D scanners.)

[12] *See* Jackson, *supra* note 6

[13] *See supra* note 7.

[14] *See* Ian Steadman, *Open Source cola and the Napster moment for the food business*, WIRED Mag. (Apr. 15, 2013), https://www.wired.co.uk/article/trade-secrets-open-source-cola. (Arguing that while barriers to chemical and food reverse engineering currently exist, they will be surmounted.); *See also* Scio Solutions, SCIO (Last updated 2017), https://www.consumerphysics.com/business/solutions/ (showing the business website of a chemical scanner.)

range from weeks to hours, depending on the industry.[15] In addition, printer prices have dropped by an order of magnitude,[16] and have become user-friendly even to students.[17] 3D scanning and printing forces a reconsideration of the scope of the reverse-engineering defense.

Under trade secret laws, an inventor who uses reasonable efforts to keep his invention secret can sue another for misappropriating his invention if that person used improper means to obtain the secret and if the trade secret holds independent economic value by being secret.[18] For example, Illinois's Trade Secret statute defines a trade secret as:

> [I]nformation, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.[19]

Trade secret laws come from several sources. They were first developed through state common law, and then were codified in model publications such as the Uniform Trade Secrets Acts or the Restatement Third of Unfair Competition.[20] Now, state trade secret statutes follow either model. Federal statutes on trade secrets arise from the Federal Defend Trade Secrets Act of 2016[21] or the Economic Espionage Act.[22]

These sources of trade secret laws do not forbid reverse engineering.[23] The Uniform Trade Secrets Act, which informs Illinois's statute,[24] states that reverse engineering shall not be an improper means of appropriating a trade secret.[25] The original Illinois statute clause on reverse engineering reads:

[15] *See supra* note 6.

[16] Nick Bilton, *Disruptions: On the Fast Track to Routine 3-D Printing*, N.Y. TIMES: BITS (Feb. 17, 2013, 11:00 AM) http://bits.blogs.nytimes.com/2013 /02/17/disruptions-3-d-printing-is-on-the-fast-track/ (The price of 3-D printers has also dropped sharply over the last two years, with machines that once cost $20,000, now at $1,000 or less.)

[17] Laura Diamond, *Georgia Tech Opens Newest Student Makerspace*, GEORGIA TECH NEWS CENTER. (Sept. 27, 2018), https://www.news.gatech.edu/2018/09/27/georgia-tech-opens-newest-student-makerspace. (Illustrating the introduction of 3D printers to students.)

[18] *See* Defend Trade Secrets Act, 18 U.S.C. Section 1832.; *See also* UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985); *See also* Economic Espionage Act, Section 1, 18 U.S.C. Section 1831; *See also* Restatement Third of Unfair Competition, Chapter 4, Appropriation of Trade Values.

[19] 765 ICLS 1065/2 (d) (d).

[20] *See* John Thomas, *The Role of Trade Secrets in Innovation Policy*, CONGRESSIONAL RESEARCH SERVICE, (Jan 15, 2014.) at 9. (articulating the history of trade secrecy law.)

[21] *See* Defend Trade Secrets Act,18 U.S.C. Section 1839(6)(B).

[22] *See* Economic Espionage Act, Section 1, 18 U.S.C. Section 1831.

[23] *See* Craig L. Uhrich, *The Economic Espionage Act-Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 152 (2001) (Noting Reverse Engineering's acceptance by a wide variety of sources.)

[24] 765 ICLS 1065/2 (d) "Trade secret" means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.")

[25] 765 ICLS 1065/2 (a) ("Reverse engineering or independent development shall not be considered improper means."); Comments to the first section of the Uniform Trade Secrets Act indicate that reverse engineering is a proper means of appropriation. UNIF. TRADE SECRETS ACT § 1.1 (UNIF. LAW COMM'N 1985) ("Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means".)

> 'Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means. Reverse engineering or independent development shall not be considered improper means.[26]

Even in common law, the Supreme Court found in *Kewanee Oil Co. v. Bicron Corp.,* that reverse engineering is not an improper means of acquiring information.[27] Reverse engineering benefits society by fostering competition, reducing prices, and advancing science,[28] but harms society by incentivizing inventors to complicate their products to prevent reverse engineering, which may cost consumers both in prices and product safety.[29] Reverse engineering typically does not harm inventors because it costs the reverse-engineer time and money,[30] which provides the inventor lead time between when their product enters the market and when a second-comer's product enters.[31] Reverse engineering may harm inventors if it is market destructive. Market destructive reverse engineering involves (1) cheaply reverse engineering a product and (2) selling an identical copy in the same market.[32] Market destructive reverse engineering is easy and cheap enough to trivialize the first inventor's lead time.[33]

Market destructive reverse engineering incurs both benefits and costs on society. It can reduce prices quickly for consumers by reducing the cost for competitors to enter the market.[34] However, it deters the first inventor's participation in the market, because the first inventor might not recoup R&D expenses.[35]

Market destructive reverse engineering also deprives consumers of access to new technology.[36] First, market destructive reverse engineering reduces innovation in a market by (1) deterring the first inventor from sharing innovation if they cannot recoup expenses,[37] and (2) deterring the second comer's independent innovation, because a rational competitor would incur less cost by copying the first product than by inventing his own competitive product.[38] Furthermore, even if inventors participate in the market, they may increase manufacturing costs

[26] 765 ICLS 1065/2 (a)-(d).

[27] *Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 476, 472 (1974) (considering whether an Ohio trade secret law conflicted with federal intellectual property law's goals and finding no such conflict in that case.)

[28] *See* Craig L. Uhrich, *The Economic Espionage Act-Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 152 (2001) (Noting Reverse Engineering's acceptance by a wide variety of sources.); *See* RICHARD A. POSNER & WILLIAM M. LANDES, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 365 (2003).

[29] *See* Samuelson, *supra* note 4 (providing a full treatment of reverse engineering's law and economics circa 2002).

[30] *See* Shane Curtis et al., *The Fundamentals of Barriers to Reverse Engineering And Their Implementation Into Material Components,* REV. ENG. DESIGN. 245, 248 (2011) (illustrating the technical barriers that an inventor can place into a device to make reverse engineering more difficult., as well as external barriers such as access to equipment and the skill of the engineer, and also showing the depth of verification required in the process which scanning and printing may not directly address.)

[31] *See* Samuelson, *supra* note 4; *see also* Shane Curtis et al., *supra* note 30.

[32] Samuelson, *supra* note 4.

[33] *Id.*

[34] *Id.*

[35] *See* Samuelson, *supra* note 4.

[36] *See* Paul Heald, *Federal Intellectual Property Law and the Economics of Preemption*, 76 IOWA L. REV. 959, 985 (1991) (arguing that imitation is not innovation.)

[37] *See* Samuelson, *supra* note 4.

[38] *Id.*; s*ee also* Heald, *supra* note 36

through technical features that stymie reverse engineering, which extends their lead time but passes on extra costs to customers.[39]

Market destructive reverse engineering may also stress the patent system by overencouraging patent applications. Studies show that not all firms rely on patent protection in the first place, but as the possibility of reverse engineering increases, the volume of patent applications increase.[40] The United States Patent and Trademark Office evaluates each patent application under stringent standards: "utility" evaluates if the invention is patentable subject matter,[41] "novelty" evaluates if the invention has already been disclosed to the public,[42] and "nonobviousness" evaluates if a person of ordinary skill in the art could make this invention from existing prior art without undue experimentation.[43] An overworked Patent Office spends less time on each patent application, increasing the probability of false allowances or rejections.[44] False allowances create anti-competitive consequences for the market, while false rejections decrease the inventor's economic viability.[45]

III. Analysis

3D printing and scanning threatens to make reverse engineering "market destructive" in multiple industries, therefore deterring innovation and increasing the likelihood of Patent Office mistakes. 3D printing and scanning can currently replicate products cheaply in different industries: machines,[46] semiconductor chips layouts,[47] and recipes.[48] This cheap replication may deter the first inventor's innovation if it trivializes his or her lead time.[49] With such cheap replication, second inventors may incur fewer costs in copying products than designing their own.[50] If the first inventor still participates in the market, they may input technical features only to complicate reverse engineering, passing on the related costs to the consumer.[51]

[39] *See* Shane Curtis et al., *supra* note 30.

[40] *See* Petra Moser, *Why Don't Inventors Patent?*, Nat'l Bureau of Econ. Research, Working Paper No. 13294 (2007). (Moser studies over 7000 inventions in the United States and Britain between 1851 and 1915. She finds that as reverse engineering an invention becomes more feasible, inventors are more likely to turn from secrecy to patent protection); *See* Alexandra K. Zaby, *Losing the Lead: The Patenting Decision in the Light of the Disclosure Requirement*, 19 ECON. INNOVATION & NEW TECH. 147, 159–60 (2010) ("In an industry sector with a high propensity to patent, such as [p]harmaceuticals[,] the easiness of reverse engineering is rather high so that the effective headstart of an inventor is low."); *See also* Jay P. Kesan, *Economic Rationales for the Patent System in Current Context*, George Mason L. Rev. 897, 901 (2015) (Summarizing studies concluding that firms do not rely solely on patents and indeed may capture the value of their invention through lead time and secrecy).

[41] 35 U.S. Code § 101 (process, machine, manufacture, or composition of matter)

[42] 35 U.S. Code § 102

[43] 35 U.S. Code § 103 ("A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.")

[44] *See* Christopher R. Leslie, *The Anticompetitive Effects of Unenforced Invalid Patents*, 91 Minn. Law. Rev. 101, 106, (discussing reasons why invalid patents exist based on the time each examiner spends in examining, and the sources therein).

[45] *See* Joan Farre-Mensa et. Al., *What is a Patent Worth? Evidence from the U.S. Patent Lottery,* (Dec. 22, 2018) (showing that patents awarded do correlate with start-ups survival) at 8; *see in general* Leslie, *supra* note 44.

[46] *See supra* note 6.

[47] *See supra* note 7.

[48] *See* Steadman, *supra* note 7.

[49] *See* Samuelson, *supra* note 4.

[50] *Id.*

[51] *See* Shane Curtis et al., *supra* note 30.

In addition, 3D Printing and scanning may stress the patent system by increasing the number of patent applications. As discussed earlier, firms may choose to protect their inventions with secrecy instead of patent protection.[52] Economic historian Petra Moser shows that scientific breakthroughs lead to an increase in patenting because such breakthroughs make maintaining secrecy more difficult.[53] Here, 3D printing and scanning may be the scientific breakthrough that pushes more inventors to patent.

However, 3D printing and scanning may threaten inventions that firms cannot protect with patents, and therefore uninformed inventors may pursue patent protection for inventions of questionable patentability.[54] Patentable inventions must be "processes, machines, manufactures, or composition of matter."[55] While not true for all inventions, most inventions reproducible by 3D scanning and printing are patentable subject matter: semiconductor chip layouts,[56] machines[57] and food recipes.[58]

In addition, the invention must be novel[59] and non-obvious.[60] 3D printing and scanning affects both inventions that meet these requirements and inventions that do not. Patent applications on machines and semiconductors deal regularly with the novelty and non-obviousness requirements because of the depth of existing prior art. However, food recipes face greater challenges in these requirements; many food recipes are not novel or nonobvious because they have been individually developed without disclosure for long periods of times, and because most recipes are combinations of known elements with predictable results.[61]

For the above reasons, 3D printing and scanning may reduce the strength of trade secret protection and incentivize more firms to pursue patent protection. Because inventors may apply for more patent applications for both patentable and questionably patentable inventions, the Patent Office will receive more applications to sort through and will thus be more likely to make mistakes.[62] A patent wrongfully denied may cost a business its livelihood, while a patent wrongfully issued will have anticompetitive effects.[63]

[52] S*ee* Moser, *supra* note 40 at 18 (describing the patenting rate across different industries).; *See also* Jay P. Kesan, *Economic Rationales for the Patent System in Current Context*, GEORGE MASON L. REV. 897, 901 (2015) (Summarizing a number of studies concluding that firms do not rely solely on patents and indeed may capture the value of their invention through lead time and secrecy); *See also* John Thomas, *The Role of Trade Secrets in Innovation Policy*, CONGRESSIONAL RESEARCH SERVICE, (Jan 15, 2014.) at 13 (discussing reasons to choose trade secrecy over patent protection, such as the delay in examination and lack of foreign protection provided by patents .)

[53] S*ee* Moser, *supra* note 40.

[54] *See* UNITED STATES PATENT AND TRADEMARK OFFICE, *Can Recipes be Patented?*, INVENTOR'S EYE, (Jun. 24, 2013).

[55] 35 U.S.C. § 101 (listing the categories of patent eligible subject matter).

[56] The chip layouts are also protected under the Semiconductor Chip Protection Act which imposes sui-generis protection on maskworks and forbids layout copying. The process and manufacturing behind the individual chip layouts are themselves patentable.

[57] Machines are by definition in the list in 35 U.S.C. § 101.

[58] Recipes are patentable subject matter as "composition of matter". *See also Can Recipes be Patented?*, *supra* note 54; *See also* Gene Quinn, The Law of Recipes: Are Recipes Patentable?, IP WATCHDOG (2012), https://www.ipwatchdog.com/2012/02/10/the-law-of-recipes-are-recipes-patentable/id=22223/;

[59] 35 U.S.C. § 102

[60] 35 U.S.C. § 103

[61] Food patents are difficult on novelty and non-obviousness grounds, especially if the recipe is merely the predictable sum total of individual parts. *See Can Recipes be Patented?*, *supra* note 54. *See also* Quinn, *supra* note 58.

[62] In *Kewanee,* the Supreme Court, in facing a trade secret federal preemption issue, discussed the potential consequences of eliminating trade secret protection, including the likelihood of inundating the Patent Office with more applications. Further discussion is infra. *Kewanee* (wheat and the chaff comment); *See also* Leslie, *supra* note 44.

[63] *See* Joan Farre-Mensa et. Al., *What is a Patent Worth? Evidence from the U.S. Patent Lottery,* (Dec. 22, 2018) (showing that patents awarded do correlate with start-ups survival) at 8; *See in general* Leslie, *supra* note 44.

3D Printing and scanning threatens to disrupt trade secrecy in many industries, and thus requires careful legal treatment to maintain competition while incentivizing innovation.

IV. RECOMMENDATION

This Note proposes modifying Illinois's trade secret statute by amending the reverse engineering clause to limit market destructive reverse engineering.

The original Illinois statute reads:

> Improper means includes theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means.[64] Reverse engineering or independent development shall not be considered improper means.[65]

This Note proposes amending the reverse engineering clause to below:

> Reverse engineering, for the purpose of duplicating any manufactured product or product part by use of 3D scanning or printing, and for the purpose of selling a same or similar product to consumers, shall not be considered an improper mean, if the reverse engineer or another incorporates the results of such conduct into an original design sold or distributed to consumers.

The clause, "for the purpose of duplicating any manufactured product or product part by use of 3D scanning or printing," targets one element of market destructive reverse engineering by limiting 3D scanning and printing to maintain the inventor's lead time.

The other two clauses target the other element of market destructive reverse engineering. First, "for the purpose of selling a same or similar product to consumers," limits enforcement of the statute to competitors selling copies of products. Second, "if the reverse engineer or another incorporates the results of such conduct into an original design sold or distributed to consumers," requires an original design, as in the Semiconductor Chip Protection Act,[66] to incentivize the second comer's own innovation. The original design itself must also be made for sale or distribution. "Reverse engineer or another" indicates that a competitor that hires another to reverse engineer the device, and then manufactures the product copy themselves, would still be required to incorporate the trade secret into an original design.

This proposal addresses only some of the intellectual property issues caused by 3D printing and scanning. Furthermore, this proposal addresses only some of the trade secrecy issues posed by 3D printing's speed, low cost, and accessibility. It should mitigate costs to innovation from the cheapness and speed at which products can be copied by 3D scanning and printing, but in

[64] 765 ICLS 1065/2 (a).

[65] 765 ICLS 1065/2 (a)

[66] This definition of "originality" is borrowed from 17 U.S.C. 1301 (b)(1) in the Semiconductor Chip Protection Act. While "original" is a generic term, courts interpreting the Semiconductor Act have relied on finding adequate paper trails and found differences between substantially identical and substantially similar, ultimately finding that even a copying of a portion of someone else's work counted as copying.

limiting protection to avoid federal preemption, this proposal leaves unaddressed the potential of recreational inventors to reverse engineer a product and disclose its secrets.

Even if this proposal is limited, it may compare favorably to other possible solutions to limit 3D printing's intellectual property problems. For instance, design patents protect the form of manufactured products, but these applications may still overwork the patent system and would only protect inventions reliant on visual forms. Illinois has unfair competition laws targeted at knockoffs, but the inventor would only be liable if they created a risk of "confusion and misunderstanding."[67] Copyrights might be extended to protect the computer-readable file resulting from 3D scanning, but enforcement challenges might make this avenue less desirable for inventors.[68] Digital Rights Management (DRM) software may be included in 3D printers to check if the user has rights to the design, but DRM applications in other contexts have been unpopular due to degrading functionality.[69] Congress might also create more copyright-like *sui-generis* rights for product categories,[70] but such rights would be industry-specific and inefficient when 3D scanning and printing can affect many industries. An originality requirement on using 3D scanning and printing for reverse engineering would target each industry without overworking the patent system or affecting 3D printer customers.

This proposal would not deter all reverse engineering, because it is targeted only towards market participants who introduce identical products quickly. It would have differing effects on recreational inventors, reverse engineering firms, and direct competitors to the inventor of the original product.

This proposal would target only some recreational inventors. A recreational inventor owns a 3D scanner and printer for recreation, not for business purposes. If this person uses that technology to reverse engineer, he poses two kinds of risks: (1) disclosing the invention to another, or (2) building and selling individual copies.

This proposal would not target recreational inventors who disclose the secret to another, because they do not reverse engineer for the purpose of selling a same or similar product. This inventor contributes to society by reverse engineering a product, driving down costs, and advancing science through disclosure. Furthermore, they do not trivialize the first inventor's lead time because the recreational inventor does not introduce a competing product.

This proposal would target recreational inventors who build and sell copies, because they reverse engineer for the purpose of selling a same or similar product and do not include an original design. While the recreational inventor benefits society by driving down costs, he or she trivializes the first inventor's lead time,[71]and has not advanced science through disclosure. These inventors may be targeted by Illinois's unfair competition laws, but only if they created a risk of "confusion and misunderstanding" with the original product.[72]

[67] 815 ILCS 510/2 Section 2 (a)(2) ("causes likelihood of confusion or of misunderstanding as to the source…").

[68] Menell, 3D Printing & US Copyright Law, 2016 at 4; See also John Hornick, Anti-Copying Technology for 3D Printing: A Survey, 3DPrint.com, (May 30, 2018), https://www.finnegan.com/en/insights/anti-copying-technology-for-3d-printing-a-survey.html

[69] *See* John Newman, *Digital Rights Management for 3D Printing?,* DE247 DIGITAL ENGINEERING, (Oct. 12, 2012), https://www.digitalengineering247.com/article/digital-rights-management-for-3d-printing/. ***See also*** **U.S. Patent 8,286,236.**

[70] *See* the Vehicle Hull Protection Act and the Semiconductor Chip Protection Act discussed *infra* in the footnotes of the Federal Preemption section.

[71] *See* Samuelson, *supra* note 4.

[72] 815 ILCS 510/2 Section 2 (a)(2) ("causes likelihood of confusion or of misunderstanding as to the source…").

This proposed statute would not affect reverse engineering firms. Reverse engineering firms are defined as firms that specialize in receiving products and reverse engineering them for clients. The statute does not target these firms because while they can reverse engineer very quickly, with domain expertise and specialized equipment, they don't sell competing products, let alone identical ones.[73] While they may indirectly contribute to reducing an inventor's lead time, that harm is outweighed by the societal good they perform by reverse engineering.

This proposed statute would target direct competitors if they reverse engineer and release copies quickly for profit. A direct competitor is an inventor who reverse engineers to sell competing products. Direct competitors are most able and inclined to incorporate trade secrets into competitive products – recreational inventors may not have as much base knowledge, and reverse engineering firms are not marketing their own products.[74] If able to copy on the cheap with 3D scanning and printing, direct competitors can compete with the original inventor on the same scale before the inventor recoups R&D expense, likely deterring the inventor's further innovation, limiting their own innovation, and over-incentivizing patent applications. Therefore, any statute restricting reverse engineering should be focused on the activities by direct competitors.

Because this proposal is a state-level modification, it may risk federal preemption. Historically, statutes restricting reverse engineering risk federal preemption if they conflict with federal intellectual property goals[75] or upset the balance between intellectual property protection and free competition.[76] In brief, this statute would support patent law's goals of advancing science by disclosure in return for limited monopolies, by providing limited protection to inventors with questionably patentable inventions and freeing those inventors to apply for patents only on potentially breakthrough inventions.[77] Even if this statute deters disclosure, it coheres with patent law because the protection it provides would be similar to the "prior commercial use defense" offered by recent patent law, which allows an inventor to defend against a claim of infringement by a later inventor who secured a prior patent on the invention – the first inventor's protection against infringement claims is not contingent on disclosure.[78]

[73] *See supra* note 6.

[74] *Id.*

[75] *Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470, 472 (1974) (considering whether an Ohio trade secret law conflicted with federal intellectual property law's goals and finding no such conflict in that case); See in general Sharon Sandeen, *Kewanee Revisited: Returning to First Principles of Intellectual Property Law to Determine the Issue of Federal Preemption*, 12 INTELLECTUAL PROPERTY L. REV. 299 (2008)., for a modern treatment of intellectual property preemption; *See* Paul Heald, *Federal Intellectual Property Law and the Economics of Preemption*, 76 IOWA L. REV. 959, 985 (1991) (articulating an economic treatment of intellectual property preemption.)

[76] *See Sears, Roebuck & Co. v. Stiffel Co.,* 376 U.S. 225, 230–31 (1964) and *Compco Corp. v. Day-Brite Lighting, Inc.,* 376 U.S. 234, 235 (1964). *See also Bonito Boats, Inc. v. Thunder Craft Boats, Inc.,* 489 U.S. 141, 161 (1989). (holding that a trade secret law perpetually banning a method of reverse engineering was preempted by patent law). The proposed statute does not ban the use of 3D scanning and printing to reverse engineering products but requires that the knowledge be incorporated in original products.

[77] Kewanee differentiates between questionably patentable and patentable inventions. The Court wants more clearly patentable applications, and fewer questionably patentable applications, on the assumption that more questionably patentable applications would lead to more invalid applications. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 488 (1974) ("those who might be encouraged to file for patents by the absence of trade secret law will include inventors possessing the chaff as well as the wheat. Some of the chaff—the nonpatentable discoveries—will be thrown out by the Patent Office, but in the meantime society will have been deprived of use of those discoveries through trade secret-protected licensing."); *See in general* Leslie, *supra* note 44.

[78] 35 U.S. Code § 273(a). An inventor may defend against a subsequent patent owner's infringement suit if the inventor had used that subject matter in connection with internal commercial use.

This proposal would not interfere with other federal intellectual property laws either. Congress has used copyright law to limit market destructive reverse engineering by imposing an originality requirement on certain reverse engineering activities.[79] Furthermore, current trade secret federal laws do not preempt state laws.[80]

This Note's proposal would weigh free competition more heavily than intellectual property protection, because the monopoly is dramatically limited – an originality requirement on one method of reverse engineering only for that exact product. Competitors would still be able to participate in the market by selling competing products, and recreational inventors and reverse engineering firms would be free to disclose the trade secret should they discover it.[81] Furthermore, by providing protection for questionably patentable inventions, the statute minimizes the workload of the Patent Office, and thus the costs of either wrongful patent rejections or issuances.[82]

V. Conclusion

Reverse engineering is a social good, because it advances science. However, cheap reverse engineering deters innovation and can over-incentivize patent applications, stressing the Patent Office with anti-competitive consequences. 3D scanning and printing can be market destructive because it can be done cheaply, quickly, and by anybody. Adding an originality requirement to Illinois' reverse-engineering clause, limited to 3D scanning and printing methodologies by competitive sellers, would mitigate the harm of market destructive reverse engineering without inhibiting scientific progress.

[79] Vessel Hull Design Protection Act, 17 U.S.C. Section 1301 (a) (1) (2) (protected hulls from plug-molding) and Vessel Hull Design Protection Act, 17 U.S.C. Section 1302 (1) (requiring designs to be original to receive protection); See also Semiconductor Chip Protection Act, 17 U.S.C Section 906 (a) (2) (limiting enforceability if the semiconductor is reverse engineered and the results of such conduct are incorporated into an original product).

[80] Defend Trade Secrets Act (18 U.S.C Section 1838) and Economic Espionage Act (18 U.S.C. Section 1838) don't preempt, much to scholars' chagrin; *But see* Craig L. Uhrich, *The Economic Espionage Act-Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 152 (2001) (The EEA does not explicitly provide a defense of reverse engineering, and Urlich argues that the EEA's ambiguity regarding reverse engineering's legality chills the activity.)

[81] Reverse engineering, for the purpose of duplicating any manufactured product or product part by use of 3D scanning or printing, and for the purpose of selling a similar product to consumers, shall not be considered an improper mean if it incorporates the results of such conduct into an original design sold or distributed to consumers.

[82] *See* Leslie, *supra* note 44.

VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

WHAT HAVE YOU DONE FOR ME LATELY? HOW THE 'VALUE OF A STANDARD' SHOULD BE APPORTIONED IN FRAND LICENSING ROYALTIES

❖ NOTE ❖

Matt Pham *

I. INTRODUCTION

The Northern District of Illinois has been at odds with other circuit courts on how to best deal with FRAND licensing, and how to best constrain the intellectual property rights of inventors whose patents have been unduly empowered by their adoption into industry standards.[1] Most courts have now held that a FRAND royalty "must be premised on the value of the patented feature, not any value added by the standard's adoption of the patented technology."[2] Although well-intentioned to mitigate patent holdup risks, this rule of law misses the mark on how a standard adds value to a technology and vice versa. Indeed, there is good reason to believe both the former and the latter occur, but limited discussion has gone into delineating the two. Considering that technologies are not arbitrarily selected, the value of a standard is likely to have been enriched by the inherent properties of its adopted technologies, justifying the standard's inclusion within the technologies' royalties. The inclusion of a standard's value thus does not necessarily factor in any wrongful holdup value and would, to the contrary, mitigate any patent holdout concerns.

Part II of this note will layout the general framework of how technologies come to be adopted within a standard. Part III of this note will apply the framework of part II to explain how technologies contribute to the value of a standard and justify the standard's inclusion in a FRAND royalty rate. Part IV of this note will show how the actual contribution of SSOs to a standard's value can be distinguished to justify a lower FRAND royalty rate.

[1] *In re Innovatio IP Ventures, LLC Patent Litig.*, No. 11 C 9308, 2013 WL 5593609, at *1 (N.D. Ill. Oct. 3, 2013).

[2] *Ericsson, Inc. v. D-Link Sys.*, 773 F.3d 1201, 1232 (Fed. Cir. 2014).

*J.D. Candidate, Class of 2021, University of Illinois College of Law.

II. BACKGROUND

A. How Standardization Occurs

Industries gain significant advantages when they standardize their practices.[3] However, the administrative costs to facilitate the cooperation among many firms to do things a certain way may be too high to justify obtaining the benefits of interoperability, utility, and network effects. Standard Setting Organizations (SSOs) attempt to reduce these administrative costs by acting as the standard instituting body of their respective industry.[4] The institution of a standard through an SSO is an example of *de jure* standardization. SSO Standards are usually determined through industry members voting and ultimately collectively selecting a standard, including all the technologies to be adopted by the standard.[5] An SSO then enforces its standard by applying obligatory forces onto its members.

In the absence of *de jure* standardization, standards are still instituted *de facto*. Standards arise spontaneously from competitive forces that compel firms to voluntarily adhere to a specific way of doing things. The strongest force bringing about de facto standardization is dominance.[6] The market may be so loyal to or familiar with a dominant firm's design, process, or strategy that other firms are compelled to follow the dominant firm's lead to survive. De facto standardization therefore differs from SSO standardization in that the former selects a standard on the basis of market response, while the latter determines a standard based on voting among industry members.

B. FRAND Apportionment and the Value of the Standard

The difference between de jure and de facto standardization reflects a distinction that is important but not yet captured in current FRAND analysis. Among the many considerations of FRAND analysis is the question of whether the standard's value should make up part of the FRAND royalty. District Courts have issued different rulings on this matter,[7] and there is further contention on the international stage.[8] These FRAND analysis cases have adopted an all or nothing approach to this question, holding either that the value of a standard should be included or not at all. This dualistic approach reflects the broader question of whether to look at FRAND licensing at a time before the standard was instituted (ex-ante) or after (ex-post).[9]

The argument against including the value of a standard is motivated in part by the higher level objective of FRAND licensing to reverse the higher royalties SEP owners are purported

[3] Knut Blind, *The Economics of Standards: Theory, Evidence, Policy* (2004).

[4] Wang Ping, *A Brief History of Standards and Standardization Organizations: A Chinese Perspective,* East-West Center Working Papers, Econ. Series, 117.

[5] *Id.*

[6] Ping, *supra* note 4.

[7] *See* Judge Holderman, holding "a court should consider the importance of the patent portfolio to the standard, considering both the proportion of all patents essential to the standard that are in the portfolio, and also the technical contribution of the patent portfolio as a whole to the standard." in *In re Innovatio IP Ventures, LLC Patent Litig.*, *supra* note 1, eventually held to the contrary in Ericsson.

[8] *Unwired Planet v. Huawei*, High Court of Justice Chancery Division Patents Court (2017).

[9] Joseph Farrell et al., *Standard Setting, Patents and Hold-Up,* 74 ANTITRUST L.J. 603 (2007).

to command by virtue of patent holdup.[10] The existence of a standard provides systemic structures that help exclude technologies that are not within the standard. As such, including the value of the standard – to the ex-ante proponent – would reflect the wrongful circumstances that FRAND licensing is attempting to correct.[11]

In spite of holding true to the motivations behind FRAND, the ex-ante approach overlooks any possibility that a patented technology may have very well added value to a standard or contributed to the standard's success. Without any action from SSOs, technologies can intrinsically add value to a standard through superior interoperability,[12] being the preferred technology of consumers, and increasing a standard's adoption.[13] Examples of non-SSO contributions to the value of a standard can be seen in incremental improvements to a pre-existing standard, such as the IEEE's transition from 2G to 4G networks;[14] as well as through de facto standardization, where technologies partly become standardized due to being the technical preference of consumers.[15] Conversely, the ex-post perspective overvalues what a patented technology does for a standard's value. Here, the contributions of an SSO in suppressing design diversity, and the marketing that goes into increasing a standard's adoption, are all unjustly included in an ex-post FRAND royalty.[16]

Because a FRAND licensing agreement should reflect the incremental value added by the patented technology, both ex-ante and ex-post approaches do not serve FRAND royalty calculations well. Patented technologies non-arbitrarily add value to a standard based on aspects of their technical superiority. Still, it is important to note that technologies are not the sole contributor to a standard's value in light of the contributions of design diversity suppression and non-technological factors. The following parts will elaborate on how exactly technologies contribute to a standard's value and how SSOs may still command lower FRAND royalties in spite of this.

III. Analysis

The selection phase is not the genesis of a standard. Standards are akin to customary codes of behavior and expectations that come about through collectivized establishment.[17] Before any selection occurs, a set of options must be created. It is likely that certain technological options that may be adopted into a standard are superior to others. It is also likely that the very prospect of instituting a standard may not have arisen until a technological option presented itself. As a result, there should be some scrutiny when asking if the very act of selecting and instituting a standard – whether they be de jure SSOs or de facto end users – wholly contributes to instituting and adding value to a standard. As such, technologies themselves probably have more of a hand

[10] Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking,* 85 TEX. L. REV. 1991 (2007).

[11] *Supra* note 9.

[12] Gregory Sidak, *Apportionment, FRAND Royalties, and Comparable Licenses after Ericsson v. D-Link,* 2016 U. Ill. L. Rev. 1809**.**

[13] James M. Utterback and William J. Abernathy, *A Dynamic Model of Product and Process Innovation,* Omega 3(6) (1975) 639-656.

[14] *See* Sidak, *supra* note 12.

[15] *See* Utterback, *supra* note 13.

[16] Janusz Ordover and Allan Shampi*, Implementing the FRAND Commitment,* the Antitrust Source (2014).

[17] *See* Ping, *supra* note *4.*

to play in creating a standard, which supports the idea that SEPs contribute significantly to the value of a standard.

The functions of SSOs are not necessary to innovate and produce standards. Interoperability, network effects, and economies of scale are all advantages that incentivize private entities to innovate with the goal of standardizing among each other without the intervention of SSOs.[18] Non-dominant firms are happy to conform to a standardized landscape because a standard clearly delineates the norms to follow in order to enter, remain, and innovate in an industry.[19] Conversely, dominant firms are also willing to have others conform to their standard because of the increased licensee base and further establishment of their industry dominance.[20] Indeed, recent research is now suggesting that patent holdup is not as rational and profitable for SEP owners compared to simply participating in patent licensing.[21] This observation shows that standards obtain value far before any action is done by SSOs. Natural market incentives appear to be one of these sources that contribute to a standard's value, mainly by innovating new technologies that make standardization more feasible or viable.

Even in the case of de jure standardization, SSOs do not supplant technologies' contributions to a standard's value. In theory, purely de jure standards would be instituted before any precedential capital, infrastructure, or recognition is established (any sort of pre-existing standardized conditions must have been the result of some de facto standardization or prior de jure standardization).[22] Adopting technologies that do not reduce these costs of creating this foundational establishment would create deadweight losses, and the benefits intended by standardization would be reduced. On the other hand, adopting technologies that make a standard more effective and easier to implement would be more sensible and in the interest of both consumers and SSOs. As a result, it is likely that SEPs, regardless of being adopted de jure or de facto, were adopted by SSOs because of their added value to the developing standard.

For the reasons discussed above, there is more to a standard than just its implementation by SSOs or induction by end users. To create a standard, adoptable technologies that make the cost of implementing a standard lower than the benefits of standardization need to be created. Standard implementers such as SSOs play no part in creating these adoptable options.[23] It is the natural incentive to innovate around standardization that brings about the value adding technological options. With this value already added, SSOs and other standard instituting mechanisms add their own value by merely discovering or promoting certain technologies.[24] The following part will elaborate on the role SSOs play in discovering and promoting SEPs in a standard, and explain how these contributions can lower a FRAND royalty rate in place of a complete bar of including a standard's value.

[18] Urs Gasser and John Palfrey, *When and How ICT Interoperability Drives Innovation,* Berkman Center Research Publication 2007-2008.

[19] *Id.*

[20] *Id.*

[21] J. Gregory Sidak, *Holdup, Royalty Stacking, and the Presumption of Injunctive Relief for Patent Infringement: A Reply to Lemley and Shapiro,* 92 MINN. L. REV. 714, 735 (2008).

[22] Blind, s*upra* note 3.

[23] *Id.*

[24] *Id.*

IV. Recommendations

With the inclusion of a standard's value in an SEP's FRAND royalty rate, there may be concerns on what, if not the value of a standard, an SSO may leverage to justify lower FRAND royalty rates. The following recommendations will look to the advantages industry standard setting has over market standard setting that an SSO can leverage to come to better FRAND licensing agreements. As previously stated, standards can arise without SSOs. However, the resulting standards tend to be less optimal than SSO determined ones. Agents further upstream, such as SSO members, have more expertise in the technical aspects of their products than do more downstream players, such as market consumers.[25] As a result, industry members are in better positions than market consumers to decide on the best technologies to be instituted into a standard. Along with their expertise, SSO members have more incentives to select on the basis of technicality, whereas the marketplace would be swayed to standardize a technology due to consumer preferences that do not always reflect the technical superiorities of products.[26]

It is fair to suspect that conflicts of interest within an SSO, such as the ownership of patents and adversarial relationships, will make SSO selection biased. However, recent studies have shown that in spite of these conflicts, SSOs still tend to select the most efficient technological solutions for their standards.[27] According to research conducted by Northwestern University International Business Professor, Daniel Spulber, SSOs at best vote unanimously on the most efficient technology and at worst are still in majority with each other.[28] This contrasts with how most dominant firms are chosen, based on market shares hovering at most around 50%, which gives much less unanimous justification for adopting a standard.[29] Ultimately, standards that are chosen through voting among industry members tend to choose efficient technologies.

The ability to select efficient standards can be used to command lower FRAND rates while still recognizing that SEP owners are entitled to a part of a standard's value. The most straightforward argument is that, sans SSO, an industry would have incurred deadweight losses from instituting a suboptimal standard. Thus, the discount an SSO may apply would be the difference between the value of the selected standard and the value of the standard that would have been instituted de facto.

A more active application of an SSOs' advantages may prove more effective. For example, an SSO, being better equipped to determine more efficient standards than any one firm, can work an agreement to work with the SEP owner in further innovations to the standard. Assuming the SEP owner is also an SSO member, the SSO may agree to disclose and license, at a lower rate, their own innovations that build upon the SEP patented technology.

[25] Denzau A. T. and R. P. Parks, 1983, *Existence of Voting-Market Equilibria, Journal of Economic Theory,* 30(2), pp. 243-265.

[26] *Id.*

[27] Daniel F. Spulber, *Standard Setting Organizations and Standard Essential Patents: Voting and Markets.*

[28] *Id.*

[29] *Global Market Share - Statistics & Facts,* www.statista.com/topics/898/global-market-share/.

V. CONCLUSION

Patent holdup can be a major detriment to innovation if FRAND agreements cannot be reached. However, scrutiny should be applied for any justification to discount a royalty rate if the discount denies value that is rightfully the inventor's. Proceeding without caution would run the risk of disincentivizing the activities that give rise to the created value. Excluding a standard's value in a FRAND royalty, while an easy fix to lower a royalty, does not reflect what an SEP owner is actually entitled to and disincentivizes inventors from innovating from an interoperability standpoint.

Recognizing that licensing agreements in a patent lockup situation can be unfair and unreasonable, there must be a way to justify of reaching a royalty rate lower than the pre-FRAND licensing agreement. One possible solution comes from leveraging SSOs' superior abilities to create efficient standards and sharing their potential benefits with the SEP owner. This solution begins to strike the balance between mitigating the unduly power that an individual SEP owner may have over its collective industry and maintaining the incentives for individual SEP owners to innovate within the realms of interoperability.

VOLUME 24 FALL 2018

ILLINOIS BUSINESS LAW JOURNAL

RIDESHARING & REGULATION: HOW RIDESHARING APPS ARE REGULATED AND HOW THEY SHOULD BE REGULATED

❖ NOTE ❖

Dawson Oler *

I. INTRODUCTION

Taking a taxi in 2019 feels so archaic. Ever since apps like Uber became commonplace, the way we are transported has radically changed; tasks like hailing a taxi seem like stories our grandparents told us about the "good old days." However, every time we request an Uber, it has been allowed to take advantage of lenient regulations that the taxi industry could only dream of. Apps like Uber consider themselves "technology companies," which frees them from the strict regulations they might face if they were considered a "taxi company."

This note will discuss the question of whether Uber should be legally classified as a technology company or a private taxi company. Uber should be classified as a taxi company because although they consider themselves merely a technological intermediary between passenger and driver, their practice is more similar to a taxi company. Like a taxi company, transportation is its main supply and without it, the service would not exist. In addition, classifying Uber as a taxi company protects consumers.

Part II of this note will provide more background into this question and how courts have grappled with it in the past. Part III of this note will analyze the way ride-sharing apps like Uber have been regulated since they first came into existence. Part IV recommends that other states follow the example of one particularly innovative state who found a solution to the question of how to regulate ride-sharing apps.

*J.D. Candidate, Class of 2021, University of Illinois College of Law.

II. BACKGROUND

Perhaps the biggest development in the transportation industry of the last decade has been the growth of ridesharing apps such as Uber and Lyft.[1] Hailed as a revolutionary innovation to mobility,[2] these apps have changed the lifestyles of those living in major cities throughout America by making transportation quicker, cheaper, and more convenient than ever. In 2017 alone, Uber gave over 4 billion rides,[3] and is available in at least 460 cities.[4]

In the beginning of Uber's service, ridesharing apps were entirely unregulated by local governments.[5] However, in 2014, Colorado became the first state to enact legislation regulating ridesharing companies (called "Transportation Network Companies," or "TNC's").[6] Since then, every state except for Oregon has enacted some form of statewide regulation over TNCs like Uber and Lyft.[7]

However, TNCs are not regulated in the same way as taxi companies.[8] For instance, the Colorado legislation is viewed as more TNC-friendly, as it allows the TNCs to self-regulate their own background checks (as opposed to taxi companies, who have to perform fingerprint background checks).[9] TNCs and taxi companies, then, are allowed to compete in the same industry, but while following different rules. It raises a fascinating question: are TNCs like Uber or Lyft distinct technology companies, subject to more specialized regulation, or are they simply a new form of taxi company (and should thus be regulated like one)?

Significant differences exist between rules for taxis and rules for TNC's. Thus, it is easy to see why TNC's have been able to flourish so quickly. Some examples of rules and regulations governing taxi companies include standards of vehicle maintenance, requirement for accessible vehicles,[10] specific licensing for all drivers,[11] the use of taxi medallions to control the number of taxi drivers,[12] and predictable rates for passengers.[13]

TNC regulations are much less coherent, with a lack of consensus across regulations. However, they typically require the drivers to have service, be a licensed driver in the state in

[1] Brad Stone, *Uber: The App That Changed How the World Hails a Taxi*, THE GUARDIAN (Jan. 29, 2017) https://www.theguardian.com/technology/2017/jan/29/uber-app-changed-how-world-hails-a-taxi-brad-stone.

[2] Katy Stenimetz, *Lyft and Uber Are 'Allies' in the Transit Revolution*, TIME (Mar. 15, 2006), http://time.com/4259615/lyft-uber-apta-mobility-study/.

[3] Johana Bhuiyan, *Uber Powered Four Billion Rides in 2017. It Wants to Do More — and Cheaper — in 2018.* RECODE (Jan. 5, 2018) (https://www.recode.net/2018/1/5/16854714/uber-four-billion-rides-coo-barney-harford-2018-cut-costs-customer-service).

[4] Kirsten Korosec, *Watch Out Uber, Lyft is Now in 300 U.S. Cities*, FORTUNE (Mar. 9, 2017) http://fortune.com/2017/03/09/lyft-300-cities/.

[5] Owain James, *Uber and Lyft Are Lobbying States to Prohibit Local Regulation*, MOBILITY LAB (July 24, 2018), https://mobilitylab.org/2018/07/24/uber-and-lyft-are-lobbying-states-to-prohibit-local-regulation/ [hereinafter James].

[6] Colo. Rev. Stat. § 40-10.1-603

[7] James, *supra* note 3.

[8] David Kemp, *Don't Regulate Uber, Deregulate Regular Taxis*, NEWSWEEK (Sept. 28, 2017) https://www.newsweek.com/dont-regulate-uber-deregulate-regular-taxis-673548.

[9] Patrick Hoge, *Colorado Becomes First State to Pass Law Embracing Uber, Lyft et al*, SAN FRANCISCO BUSINESS TIMES (June 6, 2014, 10:47 AM), http://www.bizjournals.com/sanfrancisco/morning_call/2014/06/colorado-uber-lyft.html?page=all.

[10] 35 RCNY 53-02.

[11] 35 RCNY 55-04.

[12] 35 RCNY 58-04.

[13] 35 RCNY 80-17.

which they are operating, and their vehicle must be approved by a local mechanic.[14] However, most of these statutes only require that TNCs have these policies in place; they do not have to follow any guidelines established by the state or city, as a taxi company would.[15]

In 2017, the European Court of Justice grappled with how to categorize TNCs. Elite Taxi, a group of taxi companies in Spain, brought a case against Uber for failing to attain the proper "licenses and authorizations required under the Regulation on taxi services in the metropolitan area of Barcelona."[16] Before the court could determine if Uber did not have the necessary licenses, they needed to establish that Uber needed those licenses in the first place; in other words, whether Uber was a "transportation company" or a technology company.[17] If Uber was a transportation company, they were in violation of the law and would need to be conform to the same regulations as taxi companies.[18] On the other hand, if Uber were determined to be a technology company, then they would only need to follow regulations governing electronic commerce, and the lack of licenses as alleged by Elite Taxi would be irrelevant.[19]

The court ruled that Uber would be legally considered a "transportation company" throughout the European Union.[20] The court reasoned that a company is considered a technological service if the supply which is not made by technological means is independent from the service provided (such as technological platforms for purchasing hotel rooms or booking flights).[21] Because the supply of Uber's business (transportation) is inextricably linked to the service, the court held Uber should be regulated according to regulations of other transportation companies.[22] While this ruling was a major blow to TNCs overseas, U.S. courts have not yet been confronted with the issue.

III. Analysis

Uber positions itself as a technological intermediary connecting passengers and independent drivers, and denied in a recent lawsuit that it "offer[s] a taxi service."[23] However, Uber's ex-CEO once wrote that Uber's goal was to "make transportation as reliable as running water, everywhere and for everyone,"[24] signifying that Uber is at least somewhat aware of its position as a major player in the current mass transportation landscape. If Uber's entire service is designed around transporting people (in lieu of services like taxis, no less), it stands to reason that they anticipated this legal problem and have prepared for it.

Regulating TNCs with other taxi regulations only protects taxi companies from competition, potentially stifling innovation.[25] Self-regulation, along with the general state-wide

[14] Colo. Rev. Stat. § 40-10.1-605.

[15] *Id.*

[16] Case C-434/15, Asociación Profesional Elite Taxi v Uber Systems Spain, SL, ECLI:EU:C:2017:981.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] Nat'l Fedn. of the Blind of Cal. v. Uber Techs., Inc., 103 F. Supp. 3d 1073, 1082 (N.D.Cal. 2015).

[24] Travis Kalanick, *Celebrating Cities: A New Look and Feel for Uber*, UBER (February 3, 2016) https://www.uber.com/newsroom/celebrating-cities-a-new-look-and-feel-for-uber-7/

[25] Deanna Dupuy, *The Regulation of Transportation Network Companies*, The Agora Journal of Urban Planning and Design 114, 116 (2017).

regulations (like the Colorado statute) is an adequate way to protect consumers while allowing for innovation.[26] On the other hand, it might be too naïve to expect TNCs--typically massive Silicon Valley ventures--to self-regulate in a way that is safe for consumers.[27] Additionally, the services TNCs provide are most similar to a taxi company, and therefore taxi regulations are the most fair way to regulate TNCs.[28]

A. TNCs and the Americans With Disabilities Act

TNCs should not be allowed to self-regulate. When TNCs self-regulate, minority groups within the community are negatively affected. For instance, one regulatory standard imposed on taxi companies is the requirement to follow the Americans With Disabilities Act ("ADA").[29] Although the ADA does not specifically require taxi companies to be accessible to be licensed,[30] most city taxi regulations have some form of requirement pertaining to accessibility.[31] TNCs are generally not required to follow these regulations, though this issue has become relevant in courts in recent years.

In 2014, plaintiffs Dan Ramos, Laura Posados, and Tina Williams filed suit against Uber Technologies, Inc. and Lyft Inc.[32] The plaintiffs alleged Uber was in violation of both the ADA and specific regulations regarding private entities offering taxi service by "not provid[ing] vehicles for-hire services to mobility impaired consumers such as Plaintiffs who require wheelchair accessible transportation vehicles or other accommodating services," and that the defendants "allow their vehicles-for-hire to deny service to the disabled."[33]

Uber filed a motion to dismiss and argued that Title III of the ADA only applies to public accommodations, a category they argue they did not belong to.[34] The court, however, pointed out that "Title III expressly applies to public accommodations and certain services operated by private entities."[35] Further, the court ruled this statute applies not only to public organizations who provide transportation, but also to private entities who provide public transportation.[36] Because the statute does not apply only to public accommodations, Uber's motion to dismiss was denied.[37]

Because taxi companies are included in that distinction of "private companies who provide public transportation," their obligation to follow the ADA is clear. Since the settlement of the *Ramos* case, TNCs have added services to accommodate passengers with disabilities.[38]

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] AMERICANS WITH DISABILITIES ACT OF 1990, 1990 Enacted S. 933, 101 Enacted S. 933, 104 Stat. 327

[30] Noel v. N.Y.C. Taxi & Limousine Comm'n, 687 F.3d 63, 73 (2d Cir. 2012).

[31] *Supra* note 6. James.

[32] Ramos v. Uber Techs., Inc., Civil Action No. SA-14-CA-502-XR, 2015 U.S. Dist. LEXIS 20914 (W.D. Tex. Feb. 20, 2015)

[33] *Id.* at 2.

[34] *Id.* at 12.

[35] *Id.* at 14.

[36] *Id.*

[37] *Id.* at 17.

[38] Mary Wisniewski, *Uber App Now Allows Wheelchair Users To Summon Rides*, CHICAGO TRIBUNE (July 20, 2017, 11:01 a.m.) https://www.chicagotribune.com/news/local/breaking/ct-uber-handicapped-accessibility-0720-20170719-story.html.

However, there have been several issues in major American cities like San Francisco[39] and New York City[40] involving passengers with disabilities unable to receive the same service as able-bodied passengers. The lack of regulation of TNCs has led to a major blind spot causing harm to disabled passengers.

B. TNCs Self-Regulation Track Record

Ignoring the track record of TNC's and their past failures to ensure safety for consumers demonstrates the need for stricter regulations like the ones taxi companies face. In 2014 alone, there were at least three instances where a driver of a TNC was alleged to have kidnapped a passenger.[41] Passengers have also alleged physical abuse by drivers.[42] As mentioned above, TNCs generally do not conduct fingerprint background checks, which all taxi companies must do before hiring a new driver. Consumers who get into an Uber or Lyft have no way of knowing that their driver has been through a rigorous background check to ensure their safety. Uber and Lyft's refusal to conduct fingerprint background checks has led major American cities like Austin to remove them from the city.[43] TNCs have determined the externalities for self-regulation are too high, and they have benefitted by not being regulated by the same standard as taxi companies.

IV. Recommendations

Massachusetts' TNC regulation has attempted to find common ground between TNCs and taxi companies. After contentious debate, Massachusetts passed legislation in August 2016 allowing the Massachusetts Department of Public Utilities the ability to conduct background checks and permanently expel drivers that they deem as unsuitable.[44] In addition, drivers were forced to pass minimum standards of insurance.[45] Most strikingly, the bill gave a 20-cent surcharge for every ride given by a TNC.[46] This bill was met with warm reception from both TNCs and taxi companies, as TNCs were no longer banned from working in busy parts of the city, such as the airport.[47] TNCs also were not required to conduct fingerprint background checks.[48]

[39] Complaint for Plaintiff, Smith v. Uber Technologies, Inc. (Cal. Sup. Ct. 2018), No. RG18894507.

[40] Ramos v. Uber Techs., Inc., 2018 77 N.Y.S.3d 296, 297 (S. Ct. 2018)

[41] Sam Frizell, *7 Dead-Serious Uber Controversies That Somehow Didn't Sink the Company*, TIME (Nov. 18, 2014) http://time.com/3592098/uber-controversy/.

[42] Mark Matthews, *Uber Passenger Says Driver Struck Him with Hammer After He Told Him He Was Going the Wrong Way*, NBC BAY AREA (Oct. 8, 2014) https://www.nbcbayarea.com/news/local/Passenger-Hit-with-Hammer-by-Uber-Driver-278596821.html

[43] Andy Jechow, Prop 1 Fails, Marking Defeat for Uber and Lyft in Austin, KXAN AUSTIN (May 7, 2016) https://www.kxan.com/news/local/austin/prop-1-fails-marking-defeat-for-uber-and-lyft-in-austin/1049801267

[44] 2016 Mass. ALS 187, §2(m)

[45] *Id.*

[46] *Id.*

[47] Shira Schoenberg, *Gov. Charlie Baker signs law regulating Uber and Lyft in Mass.*, MASSLIVE (Oct. 25, 2018) https://www.masslive.com/politics/index.ssf/2016/08/gov_charlie_baker_signs_law_regulating_uber_and_lyft_in_massachusetts.html.

[48] *Id.*

However, the bill was scaled back in 2017 due to complaints about the severity of the background checks.[49] This move was a win for TNCs, who now only need to pay the surcharge to taxi companies and can go forward with self-regulation. This essentially puts Massachusetts, who appeared to be on the forefront of TNC regulation in the country, right at square one with the rest of the country in regard to TNC regulations. These scale-backs are another example of states caving to demands by TNCs and allowing for self-regulation policies that ultimately hurt consumers. Massachusetts' first bill was forward-thinking and a major step in the right direction; their second bill came from the same way of thinking that has led to many of the drawbacks discussed in this note, including unfair competitive balance between taxi companies and TNCs, lack of protections for consumers, and a lack of accessible transportation for passengers with disabilities.

Other states should proceed with the legislation Massachusetts originally put into place. The emerging ridesharing industry should be allowed to innovate and adapt to consumers' preferences. However, the way TNCs have been able to actively participate in the transportation industry with taxi companies virtually regulation free is harmful both to the industries already in place as well as consumers because of unfair competitive balance between TNCs and taxi companies, TNCs track record of lenient self-regulation practices, and TNCs reluctance to make transportation more accessible for passengers with disabilities.

V. Conclusion

TNCs are, by their nature, taxi companies: like taxi companies, TNCs are inextricably linked to the transportation of individuals in urban areas, and TNCs are entirely dependent on the transportation industry to remain in existence. They have been able to grow in part because of relaxed regulatory standards. In order to protect consumers and the taxi industry already in place, states should pass legislation that regulate TNCs similarly to the strict regulatory standards taxi companies are currently held to. This will decrease unfair competition in the transportation industry, offer more protections for consumers, and make transportation more accessible for passengers with disabilities.

[49] Shannon Larson, *Massachusetts Relaxes Ride-Hailing Regulations, Affecting Uber, Lyft Drivers*, DAILY FREE PRESS (Sept. 13, 2017) https://dailyfreepress.com/blog/2017/09/13/massachusetts-could-relax-ride-hailing-regulations-affecting-uber-lyft-drivers/.