Journal of Law and Technology at Texas

Volume 3 2019-2020

Published by The University of Texas School of Law

First printing, 2020.

JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 3 • Spring 2019

THE EMPIRES STRIKE BACK: REASSERTION OF TERRORITORIAL REGULATION IN CYBERSPACE

PAYOLA 3.0? THE RISE OF THE INTERNET "PLAYOLA"

AND

SMART HOME TECHNOLOGY: ABUSERS ADAPT TO TECHNOLOGY QUICKER THAN LAWS DO

JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 3 • Fall 2019

Staff Editors (cont'd)

FOREWORD

As the Journal of Law and Technology at Texas (JOLTT) celebrates its fourth year, it is an exciting moment to reflect on the journal's growth and accomplishments to date. From increased membership, official university sponsorship, packed networking and fundraising events, and publication of topical content, JOLTT continues to stand out at The University of Texas School of Law for its entrepreneurial culture, its innovative perspective, and its enthusiastic editing staff.

The journal's successes are due in part to JOLTT's academic and financial supporters on- and off-campus, JOLTT's active alumni network, and JOLTT's amazing academic advisor, Professor Wendy E. Wagner. A huge thanks to all of you.

JOLTT's successes are also largely thanks to the grit and hustle of this year's editorial board: Seth Young, Melanie Froh, Jacqueline Odum, Kevin St. George, Arushi Pandya, Sarah Propst, Tracy Zhang, Daniel Michon, and Jacob Przada. This Volume 3 would not exist without you. Thank you for your hard work, energy, and determination.

Finally, a special thanks to the State Bar of Texas Computer and Technology Section for its financial support of JOLTT in the publication of this Volume 3. We look forward to our continued relationship in exploring the future of law and technology.

Sincerely,

Grace Bowers
Editor in Chief
The Journal of Law and Technology at Texas

TABLE OF CONTENTS

THE EMPIRES STRIKE BACK: REASSERTION OF TERRITORIAL REGULATION IN CYBERSPACE

Jon M. Garon*

> "Cyberpower is now a fundamental fact of global life. In political, economic, and military affairs, information and information technology provide and support crucial elements of operational activities."—Franklin D. Kramer, *Cyberpower and National Security*[1]

In cyberspace, as it was throughout the world, the most dominant political trend of 2018 was the rise of populism. Populist trends tend to be isolationist, nationalistic, and antagonistic to free trade and the free movement of capital. While analysts do not typically ascribe an anti-technology sentiment to the populist movement, much of the cyberspace technologies are controlled by U.S. multinational corporations.

The dominance of several U.S. technology companies has shifted Internet and Cyberspace regulatory policy to the forefront of battles over globalization and trade between the U.S. and China as well as the U.S. and Europe. These companies have triggered protectionist legislation throughout Europe and Asia, and their lax privacy protections have triggered additional regulation within the U.S. at the state level.

Because some of the government regulation is designed to enhance military readiness, it also serves to propel a populist agenda to promote greater militarization, which extends into cyberspace. This raises concerns regarding state-sponsored cyberterrorism and the march toward autonomous, networked cyber and kinetic weaponry that may have horrific consequences. These trends, along with the continued expansion of criminal cyberattacks, increased identity theft, and the continued expansion of corrosive, hate-filled social media sources, define the shifts in cyberspace policy and practice. This review highlights the recent trends and

---

* Dean and Professor of Law, Nova Southeastern University Shepard Broad College of Law; J.D. Columbia University School of Law 1988. These materials were prepared as part of the 2019 Winter Working Meeting of the American Bar Association, Business Law Section Cyberspace Law Committee meeting held January 24–26, 2019.

[1] CYBERPOWER AND THE LAW 1 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009).

influences on cyber law with the aim to anticipate key issues that will shape the coming year.

TABLE OF CONTENTS

I. INTRODUCTION

Both in cyberspace and throughout the world, the most dominant political trend of 2018 was the rise of populism.[2] Populist leaders "tapped into a backlash against immigration and a globalized economy that many people feel has left them behind."[3] Populist trends tend to be isolationist, nationalistic, and antagonistic to free trade and the free movement of capital.[4] While analysts do not typically ascribe an anti-technology sentiment to the populist movement, much of the cyberspace technologies are controlled by the U.S. oligopoly that includes Apple, Microsoft, Facebook, Amazon, Netflix, and Alphabet's Google, sometimes referred to as the FAAMG companies[5] or FANG companies.[6] The dominance of these U.S. companies has shifted Internet and cyberspace regulatory policy to the forefront of battles over globalization and trade between the U.S. and China as well as the U.S. and Europe.[7]

The political tailwinds propelling domestic populism have also pushed for greater limits on global companies. As a result, a political distrust of the FAAMG/FANG oligopoly has suddenly created some movement at the state level to regulate the power of these companies in the

---

[2] *See generally* Ronald F. Inglehart & Pippa Norris, *Trump, Brexit, and the Rise of Populism: Economic Have-Nots and Cultural Backlash*, (Harv. Kennedy Sch., Working Paper No. RWP16-026, 2016) https://ssrn.com/abstract=2818659.

[3] Marc Champion, *The Rise of Populism*, BLOOMBERG (Jan. 21, 2019), https://www.bloomberg.com/quicktake/populism.

[4] *See* Angelos Chryssogelos, *Populism in Foreign Policy*, OXFORD RESEARCH ENCYCLOPEDIAS (July 2017) http://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-467.

[5] Will Kenton, *FAAMG Stocks*, INVESTOPEDIA (Mar. 6, 2018), https://www.investopedia.com/terms/f/faamg-stocks.asp#ixzz5VwTdxaHs ("FAAMG is an abbreviation coined by Goldman Sachs for five top-performing tech stocks in the market, namely, Facebook, Amazon, Apple, Microsoft, and Alphabet's Google.").

[6] Will Kenton, *FANG Stocks*, INVESTOPEDIA (Mar. 18, 2019), https://www.investopedia.com/terms/f/fang-stocks-fb-amzn.asp#ixzz5VwU13A1T ("FANG is the acronym for four high-performing technology stocks in the market as of 2017 – Facebook, Amazon, Netflix and Google (now Alphabet, Inc.)").

[7] *See* Robert Hackett, *Cyber Saturday—A CEO-Felling Privacy Bill, Facebook Ad Scandals, Chinese Spy Charges,* FORTUNE (Nov. 3, 2018), http://fortune.com/2018/11/03/consumer-data-privacy-bill-wyden-facebook-ad-china-spy-charges/; Simon Johnson, *Opinion: Should Facebook be more tightly regulated?*, MARKETWATCH (Apr. 9, 2018), https://www.marketwatch.com/story/should-facebook-uber-and-other-tech-companies-be-more-tightly-regulated-2018-03-31.

marketplace.[8] Columbia law professor Tim Wu captures the essence of this distrust, stating that "we must not forget the economic origins of totalitarianism, that 'massively concentrated economic power, or state intervention induced by that level of concentration, is incompatible with liberal, constitutional democracy.'"[9]

Unfortunately, the growing fears of totalitarianism parallel earlier trends toward greater cyberspace militarization, increasing concerns around state-sponsored cyberterrorism, and a continued march toward autonomous, networked cyber and kinetic weaponry that may have negative consequences. These trends, along with a growing rate of criminal cyberattacks, increased identity theft, and the continued expansion of corrosive, hate-filled social media sources, make up the 2019 year in review for cyberspace.

There is a growing recognition of the militarization of cyberspace and the impact caused by the expansion of cyberspace beyond the Internet through network-connected devices, autonomous technologies, and artificial intelligence.[10] While this trend continues, 2018 saw the expansion of regulation of cyberspace as a trend that characterized the most comprehensive pattern of the past year.

This review highlights the recent political trends and influences on cyber law with a hope to anticipate the key issues that will shape the future of cyberspace and society.

---

[8] *See*, *e.g.*, Brian Barrett, *What would Regulating Facebook Look Like*, WIRED (Mar. 21, 2018), https://www.wired.com/story/what-would-regulating-facebook-look-like/; Tony Romm, *Why a Crackdown on Facebook, Google and Twitter Could Come From the States Before Congress*, WASH. POST (Mar. 2, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/02/as-d-c-sits-on-the-sidelines-these-states-are-looking-to-regulate-facebook-google-and-twitter/?utm_term=.8ca879c42082. *See also* Tim Wu, *Be Afraid of Economic 'Bigness.' Be Very Afraid*, N.Y. TIMES, (Nov. 10, 2018), https://www.nytimes.com/2018/11/10/opinion/sunday/fascism-economy-monopoly.html (noting "we have allowed unhealthy consolidations of hospitals … the pharmaceutical industry; accepted an extraordinarily concentrated banking industry, [and] despite its repeated misfeasance failed to prevent firms like Facebook from buying up their most effective competitors… There is a direct link between concentration and the distortion of democratic process.").

[9] Wu, *supra* note 8 (quoting lawyer and consumer advocate Robert Pitofsky).

[10] *See* Jon M. Garon, *Cyber World War III: Origins*, J. L. & CYBER WARFARE (forthcoming 2019), https://ssrn.com/abstract=3078327.

II. THE CURRENT CYBER APPROACH: FOREIGN REGULATORS LEVERAGE ANTITRUST AND DATA PRIVACY LAWS TO ADVANCE PROTECTIONISM

EU regulators are engaging in protectionist activity by enforcing antitrust laws and structuring privacy laws to reduce value of customer data for business intelligence. In particular, these regulators are enforcing non-traditionally cyber laws to limit FAAMG companies' reach and to promote EU protectionism.

a. EU Domestic Protectionism Under Antitrust Laws

Recently, EU regulators have engaged in economic warfare with FAAMG companies by leveraging existing antitrust laws and enacting new privacy laws in the cyber context. For example, in July 2018, EU regulators fined Google a record $5.1 (€4.34) billion for illegally tying features of Google Chrome to Google's Android operating system in contravention of EU antitrust laws.[11] Specifically, regulators found that Google had violated EU antitrust laws when the company:

- required manufacturers to pre-install the Google Search app and browser app (Chrome) as a condition for licensing Google's app store (the Play Store);
- made payments to certain large manufacturers and mobile network operators on condition that they exclusively pre-installed the Chrome app on their devices; and
- prevented manufacturers from pre-installing Google apps on mobile devices that also ran alternative versions of Google's Android operating system (i.e., "Android forks").[12]

EU Commissioner Margrethe Vestager, who prosecuted the case, stated that "Google has used Android as a vehicle to cement the dominance of its search engine. These practices have denied rivals the chance to innovate and compete on the merits. They have denied European consumers the benefits of effective competition in the important mobile sphere."[13]

---

[11] European Commission Press Release IP/18/4581, Antitrust: Commission Fines Google €4.34 Billion For Illegal Practices Regarding Android Mobile Devices To Strengthen Dominance Of Google's Search Engine (July 18, 2018).

[12] *Id.*

[13] *Id.*

In addition to pursuing a protectionist agenda through antitrust law, EU regulators also seek to regulate FAAMG's content. For example, the EU conditioned expansion of Netflix and Amazon streaming services to include minimum quotas of 30% European content on their platforms.[14] The plan is awaiting approval by the EU Parliament and the member states.[15] The plan also requires expanded content control, which will impact video-sharing platforms that have weak content control regarding violence or obscenity. "Online platforms will need to create a 'transparent, easy-to-use and effective mechanism to allow users to report or flag content . . . .' [Google and Facebook, in particular] will also have to take measures against content 'inciting violence, hatred and terrorism.'"[16]

Record regulatory fines and increasing content restrictions reflect a pattern of cyber regulation. The EU also fined Google $2.7 billion the prior year for favoring its shopping service.[17] EU Commissioner Margrethe Vestager is now investigating whether Amazon is leveraging data from the retailers it hosts on its site to undercut those retailers price points.[18] In a similar investigation, Vestager is also investigating anti-competition concerns regarding Apple's acquisition of Shazam and its ability to use Shazam data to unfairly promote Apple music.[19]

In contrast to Europe's veil of regulatory fairness that masks its domestic protectionism, India has been more forthright in its protectionist

---

[14] *See* Julia Fioretti, *EU Strikes Deal Forcing Netflix, Amazon To Fund European Content*, REUTERS (Apr. 26, 2018), https://www.reuters.com/article/us-eu-media/eu-strikes-deal-forcing-netflix-amazon-to-fund-european-content-idUSKBN1HX2M2.

[15] *Id*.

[16] *Id*.

[17] *See* Adam Satariano & Jack Nicas, *E.U. Hits Google With Record Fine In Software Case*, N.Y. TIMES (July 19, 2018), https://www.nytimes.com/2018/07/18/technology/google-eu-android-fine.html ("Competitors said that after Google was fined €2.4 billion, or $2.7 billion, in an antitrust case last year for favoring its comparison-shopping service in search results, the company sidestepped the rules.").

[18] Sara Salinas, *Amazon Hit By EU Antitrust Probe*, CNBC (Sept. 19 2018), https://www.cnbc.com/2018/09/19/eu-probing-amazons-use-of-data-on-third-party-merchants.html.

[19] Anita Balakrishnan, *Apple's Deal For Shazam Draws 'In-Depth Investigation' From Europe*, CNBC (April 23, 2018), https://www.cnbc.com/2018/04/23/european-commission-annouces-in-depth-investigation-into-apples-shazam-deal.html.

legislation against U.S. retailers including Amazon and Walmart.[20] The policies bar "the American companies from selling products supplied by affiliated companies on their Indian shopping sites and from offering their customers special discounts or exclusive products."[21] These regulations targeted at online retail are part of a broader protectionist pattern in India that has also targeted financial firms, data retention, and other aspects of the technology industries.[22] The movements in Asia and Europe echo the protectionist approach of the current U.S. administration, and reflect a general global shift back to protectionist regulations and me-first policies.[23]

b. EU Domestic Protectionism Under Privacy Laws

In Europe, the direct economic fines, investigations, and regulatory attacks on U.S. technology companies under antitrust law is buoyed by a strident new approach to privacy law that is structured to reduce the value of customer information for business intelligence. According to the EU, the General Data Protection Regulation (GDPR) "is the most important change in data privacy regulation in 20 years. The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond."[24] An EU-published brochure on the GDPR highlights the competitive agenda of the law, stating, "European rules on European soil: companies based outside the EU must apply the same rules as European companies when offering their goods or services to individuals in the EU."[25]

---

[20] *See* Vindu Goel, *India Curbs Power of Amazon and Walmart to Sell Products Online*, N.Y. TIMES (Dec. 26, 2018), https://www.nytimes.com/2018/12/26/technology/india-amazon-walmart-online-retail.html.

[21] *Id*.

[22] *Id*.

[23] *See* Matthew Lee, *AP Analysis: Other Nations Adjust to 'America First' Policy*, ASSOCIATED PRESS (Sept. 21, 2018), https://www.apnews.com/93c62e82b68b4561b0dfe40b5dc0e641 ("In his first several months, Trump withdrew from a trans-Pacific trade deal, the Paris climate accord and pulled the U.S. out of the U.N.'s science, educational and cultural organization.").

[24] EU GDPR, https://eugdpr.org/ (last visited Mar. 25, 2019).

[25] Directorate-General for Justice and Consumers (EC), *The GDPR: New Opportunities, New Obligations: What Every Business Needs to Know About the EU's General Data Protection Regulation* (May 25, 2018), *The GDPR: New Opportunities, New Obligations*, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf.

In May 2018, the GDPR went into effect. Within the first day, large technology companies, like Google, Instagram, WhatsApp, and Facebook, have been sued and face more than $8 billion (EUR 7 billion) in fines.[26] For example, Ireland's Data Protection Commission has sought a $1.63 billion fine against Facebook for its data breaches and its alleged failure to put proper protections in place.[27]

The GDPR effect is multifold, offering EU residents enhance privacy protection and increasing international barriers to entry.[28] "[T]he statute itself suggests another set of stakeholders: litigants, non-profit organizations, data protection professionals, and data regulatory authorities."[29]

As one GDPR guide explains, "on the face of it, the GDPR is quite a terrifying prospect."[30] The guide states that the GDPR was motivated to keep the EU "at the forefront of the modern information economy while creating a 'level-playing field' among the member countries of the EU."[31]

As an alternative to pure-protectionist motivations for GDPR, some European historians trace the origins of heightened EU data protection to the adoption of Article 8 of the European Convention on Human Rights ("ECHR") in 1953.[32] Another view posits that the European value of privacy stems from the government-led prosecution of Jews during World War II.[33] Regardless of the origins of the European privacy right, the impact has

---

[26] Chris A. Denhart, *New European Union Data Law GDPR Impacts are Felt by Largest Companies: Google, Facebook,* FORBES (May 25, 2018), https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#704f2f7f4d36.

[27] *See* Sam Schechner, *Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach*, W. S. J. (Sept. 30, 2018, 2:08 PM), https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906.

[28] *See generally* Roslyn Layton & Julian McLendon, *The GDPR: What It Really Does and How the U.S. Can Chart A Better Course*, 19 FEDERALIST SOC'Y REV. 234 (2018).

[29] *Id*.

[30] ALAN CALDER, EU GDPR: A POCKET GUIDE, SCHOOL'S EDITION 2 (2018).

[31] *Id*. at 3.

[32] *Id*. at 10 ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

[33] *See, e.g.*, Olivia Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, TIME (May 24, 2018), http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ (noting that during the 1930s, German census workers collected information on residents' nationalities, native language, religion and profession, and some historians believe IBM-subsidiary manufactured Hollerith machines were used to process this information and identify Jews).

been that EU regulations tend to focus on preventing exploitation by private parties rather than limiting state authority.[34]

The impact of the GDPR is to strengthen the power of the individual to control the private use of their data and the power of nonprofit organizations to take collective action against the holders of the data.[35] Although the GDPR is sometimes characterized as a consumer-protection law, the regulation is structured as a trade regulation designed to reduce the power of the holder of large data sets.[36] The new regulation has very explicit guidance on the processing of personal information:[37]

> 1. Processing[38] shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

---

[34] Bob Sullivan, *'La Difference' Is Stark In EU U.S. Privacy Laws*, NBC NEWS (Oct. 19, 2006, 11:19 AM), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.W_V3WOhKiUk (arguing that the difference in EU and U.S. privacy laws stems from basic premise that Europeans have a deep distrust for corporations and Americans are concerned with governmental privacy invasion).

[35] Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 78–79, 82, 2016 O.J. (L 119) 1, 80–81 [hereinafter "Council Regulation 2016/679"].

[36] *See* Layton, *supra* note 28 at 234, 236.

[37] Council Regulation 2016/679, arts. 1–3, 2016 O.J. (L 119) 1, 32–33.

[38] Council Regulation 2016/679, art. 4(2), 2016 O.J. (L 119) 1, 36 (defining "Processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction . . . .").

> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.[39]

The definition of "consent" in the GDPR is much more restrictive than in the U.S. Under the GDPR, consent means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[40] Informed consent requires that the data subject be, at minimum, aware of the controller's identity and the intended purposes of processing the personal data.[41] The GDPR Preamble states, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[42] In this way, the focus is on the trade regulation of the data holder much more than the autonomy of the individual who has data in the dataset.

In practice, this eliminates services exclusively offered to end-users who consent to data reuse, and all-or-nothing terms of service agreements. However, if the data or processing is required to provide the service, it is not subject to this general rule. For example, a consumer can use a map function without consenting to the use of tracking GPS information, but the software could not provide the user his or her location on the map without the GPS turned on. Marketing, advertising, and consumer demographic information are generally unrelated to the function of a company's services, so they cannot be required under the terms of service.[43]

---

[39] Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1, 36–37.

[40] Council Regulation 2016/679, art. 4. 2016 O.J. (L 119) 1, 33.

[41] Council Regulation 2016/679, recital (42), 2016 O.J. (L 119) 1, 8.

[42] *Id.*

[43] *Id.* at recital (43).

The GDPR overrides the notion of contractual consent by altering the terms through which a contract can be formed.[44] This operates in stark contrast to the multitude of "clickwrap" decisions in the U.S.,[45] which have shifted the bargaining power between two contractual parties for specific types of goods and services.

The greatest change triggered by GDPR may be its extraterritorial effect. "The GDPR aspires to a broad jurisdictional reach, and it is intended to cover any company, anywhere in the world, with an online presence that 'monitors the behavior' of EU data subjects."[46] The regulation provides for

---

[44] *See* Lisa V. Zivkovic, *The Alignment Between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject*, 28 TRANSNAT'L L. & CONTEMP. PROBS. 189, 211 (2018) (discussing the GDPR restrictions on lawful processing to six bases, which ultimately increases previous consent standards).

[45] *See, e.g.*, Hancock v. AT&T Co., 701 F.3d 1248, 1255 (10th Cir. 2012) (stating "Clickwrap is a commonly used term for agreements requiring a computer user to 'consent to any terms or conditions by clicking on a dialog box on the screen in order to proceed with [a] . . . transaction.'" (citing Feldman v. Google, Inc., 513 F.Supp.2d 229, 236 (E.D.Pa. 2007))); s*ee* Treiber & Staub, Inc. v. United Parcel Serv., Inc., 474 F.3d 379, 385 (7th Cir. 2007) (stating "one cannot accept a contract and then renege based on one's own failure to read it," in reference to contract dispute between plaintiff-jeweler and defendant-shipper); Serrano v. Cablevision Sys. Corp., 863 F.Supp.2d 157, 164 (E.D.N.Y. 2012) (stating that "'Clickwrap' contracts are enforceable under New York law as long as the consumer is given a sufficient opportunity to read the end-user license agreement, and assents thereto after being provided with an unambiguous method of accepting or declining the offer."); DeJohn v. The TV Corp. Int'l, 245 F. Supp. 2d 913, 919 (C.D. Ill. 2003) (stating that because the plaintiff had the opportunity to review the terms of the defendant's agreement, "failure to read a contract is not a get out of jail free card.") (applying New York law); Ronald J. Mann & Travis Siebeneicher, *Just One Click: The Reality of Internet Retail Contracting*, 108 COLUM. L. REV. 984, 990 (2008) (noting that clickwrap forms with (1) terms within a frame that the user must scroll to get to a button that must be checked to proceed, and (2) terms within a frame and button outside and below that must be checked to proceed, "are largely accepted as forcing assent to all the terms included in the contract . . . ."); Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Electronic Contracting Cases 2005-2006*, 62 BUSINESS LAWYER 195, 201–03 (2006); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 472-75 (2006) (discussing various cases where courts have enforced browsewrap licenses against businesses). *But see* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 28–32 (2d Cir. 2002) (concluding that when consumers are urged to download free software through a single button click, reference to existing license terms on a non-obvious sub-screen is insufficient to place consumers on constructive notice) (applying California law).

[46] Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers*, 68 SYRACUSE L. REV. 547, 549 (2018).

the protection of EU data subjects' data in any country where the data is found, with substantial fines for noncompliance.[47]

In practice, the GDPR will impact all companies, including FAAMG, that engage in business involving EU citizens' data. Specifically, Article 3(2) states the intended jurisdiction:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[48]

GDPR regulations present many challenges to U.S. companies. These tend to fall into three broad categories: (1) disparity in international data regulations, (2) greater consequence of data breaches, and (3) conflict in U.S. and EU constitutional principles.

First, the usage of the data will be more restricted under EU regulation than its U.S. counterpart.[49] Individuals in corporate data systems will have a much greater right to opt out of those databases, to receive much clearer and more detailed information about the use of one's information, and to require that generalized usage provisions are not used as a pretext for undisclosed third-party transfers of information.[50]

Second, the epidemic of data theft, ransomware, and disruption caused by external data breaches and internal employee misconduct may have a greater consequence for the corporate owners of the data and a higher cost for the response to each data breach.[51] Regulators application may also

---

[47] *See* Council Regulation 2016/679, arts. 82–83, 2016 O.J. (L 119) 1, 82-83 (discussing fines for non-compliance).

[48] *Id.* at recital (23).

[49] *Id.*at art. 6. *See also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 179 (2017).

[50] Council Regulation 2016/679, arts. 6–7, 2016 O.J. (L 119) 1, 46.

[51] *See* 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, 498 (2018) (stating "the GDPR requires that data breaches be reported if personal data is involved,

extend liability under GDPR to data security, data storage, and data-breach notification contractors who are involved in the breach.[52]

Third, and conceptually most challenging, is that GDPR restrictions may conflict with the U.S. fundamental right of free speech. Our constitutional right in free speech grates against EU fundamental notions of privacy, like the right to be forgotten.[53] Even Great Britain has not been amused. During testimony about the right to be forgotten, Minister for Justice and Civil Liberties, Simon Hughes, stated that "[a]nything that is impractical, impossible and undeliverable is a nonsense, and we should not countenance it."[54] Although this conflict may not be the most financially significant, it reflects the stark divide between EU and U.S. policies and political histories.

GDPR and the related right to be forgotten may have had implications in the British EU referendum (Brexit). For example, news outlet Information Age noted additional debates on "how Brexit would impact the General Data Protection Regulation (GDPR), which encompasses a number of data protection laws including Google's 'Right to be Forgotten.'"[55] As the final deadlines for Brexit loom, the extraterritoriality of the GDPR

---

such as in DDoS and ransomware cyberattacks. Companies dealing with personal data must be able to identify and deal with security breaches, in addition to creating a mandatory notification system . . . .").

[52] *Id*.; *see also Internet of Things Privacy: What GDPR Means for IoT Data*, LANNER (Oct. 20, 2017), https://www.lanner-america.com/knowledgebase/iot/internet-things-privacy-gdpr-iot-data-protection/ (discussing liability under GDPR for breaches of IoT data).

[53] *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX, ¶. 98 (May 13, 2014) (discussing instances where data subject may be entitled to have sensitive private information, like a decades-old auction related to social security debt, unlinked from his name); *see also* Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 3 (2017) (defining the "right to be forgotten" as "the right of an individual to erase, limit, or alter past records that can be misleading, redundant, anachronistic, embarrassing, or contain irrelevant data associated with the person, likely by name, so that those past records do not continue to impede present perceptions of that individual.").

[54] EUROPEAN UNION COMM., EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN'?, 2014 HL 40, ¶37 (UK) (citing Rt Hon Simon Hughes MP, Minister for Justice and Civil Liberties, 9 Jul. 2014 Parl Deb HL (2014) Q38, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-sub-f-home-affairs-health-and-education-committee/the-right-to-be-forgotten/oral/11381.html).

[55] Nick Ismail, *How Will Brexit Impact Google's Right to be Forgotten?,* INFORMATION AGE (Nov. 29, 2016), https://www.information-age.com/brexit-impact-google-right-to-be-forgotten-123463440/.

provides some answers while the lack of a Brexit agreement fuels additional uncertainty.

III. TERRITORIALITY BEYOND THE GDPR: REGULATORY AND RESTRICTIVE APPROACHES

The consequence for U.S. companies with European customers on these three areas of data hygiene will be profound, if not transformative. More important than the specifics of the regulatory compliance, however, are the implications to territoriality itself. GDPR provides an existential proof of concept that territorial boundaries can be drawn around the movement of information.[56] When these techniques are adopted by more totalitarian regimes, however, the potential for significant global tension will become apparent.

As states learn to reassert territorial controls over Internet content and extraterritorial controls over multinational corporations doing business in their territories or among their citizens, the ability to harness data for state control greatly increases. Take the case of China:

> [Chinese government] [r]eforms in 2017 and 2018 further centralized the regulatory landscape for social media and Internet platforms, including increasing the resources available to strengthen the censorship infrastructure through a central government agency. Changes in regulations and increased censorship strengthened the Great Firewall, especially through significant limitations on the use of virtual private networks ("VPN") software that allow users to access blocked information. As part of Xi Jinping's "cyber sovereignty" campaign, government regulators required state-run telecommunications firms to use technology to block VPNs and other circumvention tools. The stakes for challenging dominant state narratives increased—regulations from the Cyberspace Administration of China released in 2017 now impose real name registration requirements for users seeking to post online

---

[56] *See, e.g.*, Andrew Guerra, *General Data Protection Regulation (GDPR) Principles and Primer*, IBM, https://www.ibm.com/blogs/bluemix/?s=General+Data+Protection+Regulation+%28GDPR%29+Principles+and+Primer (June 27, 2019) ("Geo-fencing is the ability to separate workloads within a trusted compute pool, and helps solves for data sovereignty requirements. Data can only be decrypted on good, known hosts in authorized geographies.").

> content or comments, and legal liability for Internet platform providers who fail to regulate online content.[57]

General Secretary of the Communist Party of China Xi Jinping's ability to garner control of both domestic sovereignty and cyber sovereignty anticipates a new world order in which both democratic states, like EU member states, and dictatorial states, like Russia and China, will increasingly use the technologies and regulations of modern data management to control the experience for their citizens.[58]

This reassertion of state control is unsurprising. Since at least 1998, Russia has claimed that free Internet is a form of "information terrorism."[59] It spent the past two decades seeking to use the weapon to its own advantage while simultaneously attempting to stop the West from using online and cyber tools to promote democratic ideals. In 2008, at a U.N. disarmament conference, Russian Defense Ministry member Sergei Korotkov advocated that "anytime a government promotes ideas on the Internet with the goal of subverting another country's government—even in the name of democratic reform—it should qualify as 'aggression.' And that, in turn, would make it illegal under the U.N. Charter."[60]

---

[57] *See generally* Joy L. Chia, *Rights Lawyering in Xi's China: Innovation in the Midst of Marginalization*, 41 FORDHAM INT'L L.J. 1111, 1127–28 (2018) (citing Zhou Xin, *It's The Mysterious Department Behind China's Growing Influence Across The Globe. And It's Getting Bigger*, SOUTH CHINA MORNING POST (Mar. 21, 2018, 3:00 PM), https://www.scmp.com/news/china/policies-politics/article/2138196/its-mysterious-department-behind-chinas-growing); Lucy Hornby, *China's VPN Crackdown Is About Money As Much As Censorship*, FIN. TIMES (Jan. 21, 2018), https://www.ft.com/content/35eafc9a-fcf8-11e7-9b32-d7d59aace167; *China Tells Carriers to Block Access to Personal VPNs by February*, BLOOMBERG NEWS (July 10, 2017), https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february; Guójiā Hùliánwǎng Xìnxī Bàngōngshì Gōngbùle "Hùliánwǎng Fābù Pínglùn Guǎnlǐ Tiáolì" (国家互联网信息办公室公布<<互联网跟帖评论服务管理规定>>) [The National Internet Information Office Announced the "Regulations on the Management of Internet Posting Comments"], Zhōngguó Wǎngluò Kōngjiān Guǎnlǐ Jú (中国网络空间管理局) [Cyberspace Administration of China] (Aug. 25, 2017), http://www.cac.gov.cn/2017-08/25/c_1121541481.htm.

[58] *See generally* Jon M. Garon, *Revolutions and Expatriates: Social Networking, Ubiquitous Media and the Disintermediation of the State*, 11 J. INT'L BUS. & L. 293 (2012).

[59] Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* NAT'L PUBLIC RADIO (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

[60] *Id.*; *See also* Timothy L. Thomas, *The Russian View of Information War,* FOREIGN MILITARY STUDIES OFFICE (Feb. 7-9, 2000), https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/202359 (discussing various reasons driving Russia's calls at

In April 2018, Russia's Internet regulator Roskomnadzor (RKN) made a frontal assault on the Russian instant-messaging app, Telegram.[61] Nearly 19 million IP addresses were blocked in the first weeks of the campaign, which also impacted sites such as Amazon, Google, Microsoft, Mastercard, Twitch, Slack, SoundCloud, Viber, Spotify, FIFA, Nintendo, and many others.[62] Amazon and Google resisted these efforts, but only to a point.[63] Although the companies objected to the restrictions, they began enforcing their terms of service provisions to ban domain fronting, a technique that helps client websites shift their HTTPS request to a generalized service instead of a communications platform in order to avoid government shutdowns.[64] By enforcing the terms of service, the companies gave Russia exactly the assistance it needed to conduct the crackdown.

As noted in a letter by U.S. Senators Ron Wyden (D-Ore.) and Marco Rubio (R-Fla.), the decision:

> [P]revents millions of people in some of the most repressive environments including China, Iran, Russia and Egypt from accessing a free and open internet. Dissidents, pro-democracy activists, and protestors living under authoritarian regimes need access to secure communications enabled by domain fronting techniques to stay safe and organize.[65]

---

the U.N. for a "world-wide information security policy and to limit the development of information weaponry and operations.").

[61] Ingrid Lunden, *Russia's Game Of Telegram Whack-A-Mole Grows To 19M Blocked IPs, Hitting Twitch, Spotify And More,* TECHCRUNCH (Apr. 19, 2018), https://techcrunch.com/2018/04/19/russias-game-of-telegram-whack-a-mole-grows-to-19m-blocked-ips-hitting-twitch-spotify-and-more/.

[62] *Id.* (noting "[t]he technique uses HTTPS encryption to communicate with a censored web host even though it looks like it's communicating with another host like Amazon Web Services. One service is on the outside of the HTTPS request, the real domain is on the inside and censors are none-the-wiser from a technical point of view, unless they block the first domain entirely.").

[63] *Id.* (noting that Google and Amazon initially appeared to not buckle under the pressure of Russian regulators regarding IP hopping).

[64] *See* Patrick Howell O'Neill, *Lawmakers Call On Amazon And Google To Reconsider Ban On Domain Fronting*, CYBERSCOOP (July 17, 2018), https://www.cyberscoop.com/domain-fronting-ban-letter-ron-wyden-marco-rubio-amazon-google/.

[65] Letter from Senator Ron Wyden & Senator Marco Rubio, U.S. Senate, to Jeff Bezos, CEO, Amazon.com, Inc., & Larry Page, CEO, Alphabet Inc. (July 17, 2018), https://assets.documentcloud.org/documents/4609286/Wyden-Rubio-Letter-to-Amazon-Alphabet-Re-Domain.pdf.

The increase in trade and content restrictions targeting global multinational corporations is taking a toll on their ability to operate independently of state regulation. Governments such as India are also looking for increased privacy and data security regimes.[66] India continues to expand its restrictive approach, adopting aspects of both the European regulatory model and Chinese restrictive model.[67]

In addition, Thailand has attempted to join the club of totalitarian cyber regimes.[68] Pending legislation in the country would create a "new government agency sweeping powers to spy on Internet traffic, order the removal of content, or even seize computers without judicial oversight . . . ."[69] Large Internet companies are also confronting other Southeast Asian, countries, like India, Vietnam, and Indonesia, over similar proposals.[70]

China continues to make additional advances with its integration of new technologies for surveilling minority or dissident groups. For example, China now uses artificial intelligence to track its Uighur Muslim minority, facial-recognition-equipped eyeglasses to improve individual surveillance, and a big-data policing system ironically named "Skynet."[71] A report by Human Rights Watch captures the chilling power of artificial intelligence and big data turned against a society:

> Perhaps the most innovative—and disturbing—of the repressive measures in Xinjiang is the government's use of high-tech mass surveillance systems. Xinjiang authorities conduct compulsory

---

[66] *See generally* Saritha Rai, *India Considers Sweeping GDPR-Style Curbs for Online Data*, BLOOMBERG (July 30, 2018), https://www.bloomberg.com/news/articles/2018-07-30/india-considers-sweeping-gdpr-style-curbs-for-online-data.

[67] *See, e.g.*, Vindu Goel, *India's Regulators Seek to Rein In Internet Giants*, N.Y. TIMES (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html (noting that Indian regulators want to establish European-style data protection for its citizens, while also adopting the Chinese approach of maintaining its right to obtain private information).

[68] *See generally* Patpicha Tanakasempipat, *Thai Proposal for All-Powerful Cyber Agency Alarms Businesses, Activists,* REUTERS (NOV. 16, 2018), https://www.reuters.com/article/us-thailand-cyber/thai-proposal-for-all-powerful-cyber-agency-alarms-businesses-activists-idUSKCN1NL0JP.

[69] *Id*.

[70] *Id*.

[71] Maya Kosoff, *China's Terrifying Surveillance State Looks A Lot Like America's Future*, VANITY FAIR (July 9, 2018), https://www.vanityfair.com/news/2018/07/china-surveillance-state-artificial-intelligence.

> mass collection of biometric data, such as voice samples and DNA, and use artificial intelligence and big data to identify, profile, and track everyone in Xinjiang. The authorities have envisioned these systems as a series of "filters," picking out people with certain behavior or characteristics that they believe indicate a threat to the Communist Party's rule in Xinjiang. These systems have also enabled authorities to implement fine-grained control, subjecting people to differentiated restrictions depending on their perceived levels of "trustworthiness."
>
> Authorities have sought to justify harsh treatment in the name of maintaining stability and security in Xinjiang, and to "strike at" those deemed terrorists and extremists in a "precise" and "in-depth" manner. Xinjiang officials claim the root of these problems is the "problematic ideas" of Turkic Muslims. These ideas include what authorities describe as extreme religious dogmas, but also any non-Han Chinese sense of identity, be it Islamic, Turkic, Uyghur, or Kazakh. Authorities insist that such beliefs and affinities must be "corrected" or "eradicated."[72]

If there are differences between the regulatory attempts over privacy, security, and trade practices from a decade ago and today, they include the ever-increasing sophistication of totalitarian nations, a new willingness of democratic countries to introduce intrusive regulatory regimes, and a diminution of multinational corporate media companies' ability to withstand regulatory pressure. Taken together, these changes are making the power of governments stronger than ever when it comes to regulating conduct on the internet and throughout the increasingly data-driven society.

IV. THE U.S. GETS INTO THE ACT

The reaction to the current cyber environment has motivated governments at every level of jurisdiction to increase regulation and enforcement. Currently, California's approach to cybersecurity regulation far outpaces other states, though others have recently begun to address these data privacy issues. At the federal level, the U.S. government has approached cyber concerns via enhancing export controls.

---

[72] Maya Wang, HUMAN RIGHTS WATCH, ERADICATING IDEOLOGICAL VIRUSES: CHINA'S CAMPAIGN OF REPRESSION AGAINST XINJIANG'S MUSLIMS (Sept. 9, 2018), https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs#.

a. A Californian Approach to Cyber Protection: The California Consumer Privacy Act of 2018

In the U.S., California continues to take the lead on cybersecurity legislation.[73] In 2018, California extended its lead by enacting two significant pieces of legislation that impact privacy and data security.

The first of these laws is the California Consumer Privacy Act of 2018 (CCPA),[74] which has been labeled "the broadest United States privacy law."[75] The second statute is the "Security of Connected Devices" law, designed to regulate and secure internet-connected devices ("IoT devices") and the Internet of Things.[76] Both laws will become effective on January 1, 2020.[77] California also enacted a Net Neutrality state law that directly conflicts with federal efforts to deregulate telecommunications.[78]

The CCPA has been labeled the American GDPR,[79] and while the analogy is reasonable, the two regimes differ significantly. Like the GDPR,

---

[73] *See, e.g.*, James F. Brelsford, *California First State to Require Online Privacy Policies,* JONES DAY COMMENTARIES (2004), https://www.jonesday.com/California-First-State-to-Require-Online-Privacy-Policies-01-06-2004/# (last visited Mar. 31, 2019) (stating "[i]n 2003, California enacted groundbreaking consumer rights legislation in the areas of database security, sharing of personal financial information, spam, and the use of personal information in direct marketing. Maintaining its pioneer status, California is the first state to require that all companies that collect personal information online from California residents must post online privacy policies that describe their practices in a conspicuous manner."); *See generally* Chuck DeVore, *California Seeks to Regulate the Internet in a Drive to Resurrect Net Neutrality*, FORBES (May 31, 2018, 10:24am), https://www.forbes.com/sites/chuckdevore/2018/05/31/california-seeks-to-regulate-the-internet-in-a-drive-to-resurrect-net-neutrality/#3b0de8f627c1; Randall Stempler, *California Takes the Lead in Regulating the Internet of Things*, POLSINELLI BLOGS (Oct. 2018), https://www.jdsupra.com/legalnews/california-takes-the-lead-in-regulating-56214/ (last visited Mar. 31, 2019).

[74] California Consumer Privacy Act of 2018, 2018 Cal. Stat. ch. 55 (A.B. 375) (codified as amended at CAL. CIV. CODE § 1798.100 (2018)).

[75] Stempler, *supra* note 73.

[76] CAL. CIV. CODE§ 1798.91.04 (West 2018).

[77] *Id.* §§ 1798.91.04, 1798.175.

[78] Cecilia Kang, *California Lawmakers Pass Nation's Toughest Net Neutrality Law*, N.Y. TIMES (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/technology/california-net-neutrality-bill.html.

[79] *See* Bret Cohen et al., *California Consumer Privacy Act: The Challenge Ahead – A Comparison of 10 Key Aspects of The GDPR and The CCPA*, HOGAN LOVELLS DATA PROTECTION BLOG (Oct. 3, 2018), https://www.hldataprotection.com/2018/10/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-a-comparison-of-10-key-aspects-of-the-gdpr-and-the-ccpa/ (comparing the CCPA with the EU's GDPR).

the CCPA provides Californians rights to control the collection, use, and dissemination of data through an amendment of California Civil Code 1798. As explained in the legislative finding for the statute, the goals of the CCPA are the following:

> (1) The right of Californians to know what personal information is being collected about them.
> (2) The right of Californians to know whether their personal information is sold or disclosed and to whom.
> (3) The right of Californians to say no to the sale of personal information.
> (4) The right of Californians to access their personal information.
> (5) The right of Californians to equal service and price, even if they exercise their privacy rights.[80]

Under these provisions, third parties must provide consumers with explicit notice and opportunity to opt out before the sale or resale of personal information.[81] This requirement, particularly the ability of the public to say no to the sale of their personal information, as the potential to significantly reduce the marketability of consumer information.

These CCPA goals are consistent with the consumer protection provisions of the GDPR. The two statutory schemes will undoubtedly expand the enforcement and scope of data management requirement and consumer protection.

Like the EU, California seeks to expand its influence outside the state. The CCPA covers any enterprise that collects consumers' personal information, determines the processing of that information, and "does business in the State of California," and either (A)"[h]as annual gross revenues in excess of twenty-five million dollars ($25,000,000)," (B) transacts "the personal information of 50,000 or more consumers, households, or devices, or (C) "[d]erives 50 percent or more of its annual revenues from selling consumers' personal information."[82]

---

[80] CAL. CIV. CODE § 1798.100 § 2(h) (1)–(5)

[81] CAL. CIV. CODE § 1798.115(d) (West 2018) ("A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to 1798.120.").

[82] *See generally* CAL. CIV. CODE § 1798.140(c)(1)(A)–(C) (West 2018).

While the CCPA's extraterritorial effect differs from that of the GDPR, both governments seek to extend a broad net outside their physical territory to protect their residents wherever they transact in cyberspace. California, however, has the additional concern that state laws do not interfere with interstate commerce.[83] Implicit in the Commerce Clause, the Dormant Commerce Clause "precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State."[84]

Because the CCPA requires that the consumer be a California resident and the entity at least conduct business in California,[85] there is less of a risk that the law applies to out-of-state transactions. Thus, the CCPA is likely to avoid triggering the Dormant Commerce Clause.

However, the CCPA may still violate the Dormant Commerce Clause if it "is clearly excessive in relation to the putative local benefits."[86] The CCPA imposes a condition upon a corporation of another state seeking to do business in California.[87] As such, the regulation may be subject to constitutional scrutiny.

The Dormant Commerce Clause concerns will continue with privacy and customer control legislation because of the actual or potential consequence of having a patchwork of state laws—and international obligations—that require customer databases to be broken up or coded based on the state's various regulatory regimes.[88]

---

[83] *See generally* Sam Francis Found. v. Christies, Inc., 784 F.3d 1320, 1323 (9th Cir. 2015) (noting that the dormant Commerce Clause provides a limitation on states' powers and bars states from unduly regulated interstate commerce, in the context of California's Resale Royalty Act).

[84] *Id*. (quoting Healy v. Beer Inst., 491 U.S. 324, 336 (1989) (ellipsis and internal quotation marks omitted)).

[85] *See* CAL. CIV. CODE § 1798.140(g) (West 2018) (defining "consumer" as a "natural person who is a California resident . . . .").

[86] S. D. v. Wayfair, Inc., 138 S. Ct. 2080, 2091 (2018).

[87] *See* Am. Library Assoc. v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) (stating that courts have held "that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.", citing Wabash, St. L. & P. Ry. Co. v. Ill., 118 U.S. 557, 7 S.Ct. 4 (1886) (holding railroad rates exempt from state regulation).

[88] *See* S. Pac. Co. v. State of Ariz. ex rel. Sullivan, 325 U.S. 761, 773 (1945) (addressing state regulation of train lengths). The Supreme Court in *S. Pac. Co.*, was addressing train

"The courts have long recognized that railroads, trucks, and highways are themselves 'instruments of commerce,' because they serve as conduits for the transport of products and services."[89] "The Internet is more than a means of communication; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos which can be downloaded from the provider's site to the Internet user's computer."[90]

The Dormant Commerce Clause issues are not automatically fatal to all Internet regulation, but where the regulation allows individual states to create substantial burdens for the same data in various locations, the regulation may be too much. "Concerns about the cross-border costs of state Internet regulation are heightened when the sale and transmission of digital goods as opposed to real-space goods are at issue."[91]

There is a practical burden in a requirement that forces a business to track the residency of each consumer in a database—in addition to the persons national citizenship for purposes of GDPR and the IP-address-based geolocations.[92] Given these conflicting demands, inconsistent standards,

---

lengths, but the nearly identical language can be understood by analogy to protect various entries into a database or consumer files in a business database. For example:

Compliance with a state statute limiting [train lengths or data sets requires these] to be broken up and reconstituted as they enter each state according as it may impose varying limitations upon [the varying consumer protection schemes]. The alternative is for the carrier to conform to the lowest [] limit restriction of any of the states through which its [trains or data] pass, whose laws thus control the carriers' operations both within and without the regulating state.

[89] Am. Library Ass'n v. Pataki, 969 F.Supp. 160, 173 (S.D.N.Y. 1997) (citing Kassel v. Consolidated Freightways Corp., 450 U.S. 662 (1945)).

[90] *Id.*

[91] Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L. J. 785, 824 (2001). *See generally,* ORIN S. KERR, COMPUTER CRIME LAW 697 (2013); Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L. J. 409, 420–21 (2015).

[92] *See* Glosson, *supra* note 91, at 422–23 ("With the advent of geolocation technology, however, the question becomes more complex. Now it is often possible, at least in theory, to distinguish communications sent to devices in New York from those sent to devices in any other state."). *But see* James E. Gaylord, *State Regulatory Jurisdiction and the Internet: Letting the Dormant Commerce Clause Lie*, 52 VAND. L. REV. 1095, 1121 (1999) (The broad rail analysis initially used in the telegraph cases eventually gave way to more state regulation. "[T]he Court concluded that the state where a telegraph contract was made had sufficient interest to regulate that contract, even though it might affect conduct in other states.").

and risks of liability, "firms would likely choose to comply with the most stringent state laws across the board, rather than incurring the expense . . . and tailoring their products accordingly."[93]

The push to use California law as the new national platform is precisely what California lawmakers hoped to achieve.[94] "[T]he Golden State . . . promised a wall of resistance to conservative policies coming out of Washington, D.C. And as President Donald Trump approaches his 100-day mark, Californians have beefed up vows to push back with legislation and lawsuits."[95] For the Internet, "California will attempt to go it alone in regulating internet access after . . . restor[ing] Obama-era regulations barring the telecommunications industry from favoring certain websites."[96]

If California's goal is to use its state's influence to change the national standards for consumer protection of privacy, then it is much more likely to run afoul of the Dormant Commerce Clause than if it were merely seeking to protect its residents from the same risks. The expansive nature of the legislation increases the likelihood of a successful constitutional challenge.

Beyond the jurisdictional differences between the GDPR and the CCPA, there are other differences as well. The CCPA, for example, introduces the undefined concept of "household" information to the term personal information.[97] "While not defined in the CCPA, a 'household' will likely cover, at minimum, data linked to a particular address, even if such data is not linked to any natural persons or device identifiers."[98]

---

[93] Glosson, *supra* note 91, at 422.

[94] Katy Steinmetz, *7 Ways California Is Fighting Back Against President Trump's Administration*, TIME (Apr. 6, 2017), http://time.com/4725971/california-resisting-trump-administration/.

[95] *Id*.

[96] Melody Gutierrez, *California OKs Net-Neutrality Rules: Trump Administration Promptly Sues*, S.F. CHRON. (Sep. 30, 2018, 7:54 PM), https://www.sfchronicle.com/business/article/California-restores-Obama-era-net-neutrality-13270511.php ("First, however, the state will have to prevail in a legal fight with the Trump administration's Justice Department, which sued to block California from installing its own rules minutes after [Governor] Brown signed the bill.").

[97] *See* CAL CIV. CODE § 1798.140(o) (defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

[98] Cohen et al., *supra* note 79.

Uniquely, the CCPA also carves "publicly available" information into information that can be used without consent.[99] However, the CCPA states that information is not considered "'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained"[100] (i.e., beyond the scope of original intent). This distinction may allow real estate agency sites, like Zillow, Trulia, or Realtor.com, to use real estate records without consumer consent but prohibit a healthcare company or goods reseller from data mining this information. Many of the terms in the CCPA are opaque and in need of interpretation.

Both the GDPR and CCPA have notice requirements, but the CCPA also requires that the business maintain lists of personal information that the business has sold or disclosed.[101] Both laws have some access rights, opt-out rights, anti-discrimination protections, and deletion rights.[102] However, the CCPA includes certain exemptions for data requests that may violate the First Amendment; for example, if the requests interfere with a right to "exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law."[103] Given the strength of EU privacy rights, it is unsurprising that GDPR does not provide a similar exemption.[104]

California has not limited itself to the CCPA. Another of the recently enacted statutes, the Security of Connected Devices (SCD) law,[105] has the following purpose:

> This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate

---

[99] See generally CAL. CIV. CODE § 1798.140(o)(2).

[100] *Id.* (noting additional exemptions on what is considered "publicly available" information).

[101] CAL. CIV. CODE § 1798.130(a)(5)(C).

[102] Cohen et al., *supra* note 79.

[103] David Kessler & Anna Rudawski, *CCPA Extends "Right to Deletion" to California Residents*, NORTON ROSE FULBRIGHT DATA PROTECTION REPORT (Sept. 27, 2018), https://www.dataprotectionreport.com/2018/09/ccpa-extends-right-to-deletion-to-california-residents/.

[104] *See generally id.*

[105] S.B. 327, ch. 886, 2017-18 S. Reg. Sess. (Cal. 2018) (statement of Sen. Hannah-Beth Jackson) (codified as amended at CAL. CIV. CODE § 1798.91.04).

> to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.[106]

The statute proposes requirements for protecting networked devices that are limited to those devices sold or offered for sale in California.[107] The statute is further limited by exempting devices that are governed by federal law, regulations, or guidance.[108] These limitations could reflect an attempt to address the Commerce Clause issues. Cybersecurity expert Robert Graham critiques the law, given its backward-looking nature that prioritizes adding currently undefined "reasonable and appropriate" security measures rather than emphasizing isolation technologies.[109] However, the law does emphasize the need for better security requirements for the introduction of IoT devices. It is possible the FCC will create regulations that supersede the California statute or that Congress will move forward on IoT legislation.[110]

b. Other States' Approach to Cyber Policy

California is not the only state adding new legislation to improve cybersecurity. For instance, Ohio passed Senate Bill 220, which became effective November 2, 2018, "to provide a legal safe harbor to covered entities that implement a specified cybersecurity program . . . ."[111] This law reflects another effort to encourage proactive cybersecurity behavior. In this case, the statute creates limited immunity from Ohio tort claims for those companies that adopt a written cybersecurity program and comply with that

---

[106] *Id.*

[107] *See* CAL. CIV. CODE § 1798.91.05(c) (defining "manufacturer" subject to the statute as a "person who manufactures, or contracts with another person to manufacture on the person's behalf, *connected devices that are sold or offered for sale in California*.") (emphasis added).

[108] CAL. CIV. CODE § 1798.91.06(d).

[109] Robert Graham, *California's Bad IoT Law*, ERRATA SECURITY BLOG (Sept. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W_gfvuhKiiO, ("This law is backwards looking rather than forward looking. Forward looking, by far the most important thing that will protect IoT in the future is 'isolation' mode on the WiFi access-point that prevents devices from talking to each other (or infecting each other).").

[110] *See generally* IoT Cybersecurity Improvement Act of 2017, S.1691, 115th Cong. (2017); IoT Consumer TIPS Act of 2017, S.2234, 115th Cong. (2017); SMART IoT Act, H.R.6032, 115th Cong. (2018).

[111] S.B. 220, 132nd Gen. Assemb., Reg. Sess. (Ohio 2018) (codified as amended at OHIO REV. CODE ANN. § 1354.01 (West 2019)).

program.[112] To be compliant under the new laws, companies must adopt an industry-recognized cybersecurity framework, such as one of several NIST-published frameworks, or comply with a federal statutory regime, if the company is an entity required to comply with such laws.[113] In addition, companies that accept credit card payments must comply with "both the current version of the 'payment card industry (PCI) data security standard' and conform[] to the current version of another applicable industry recognized cybersecurity framework."[114]

Other states have expanded deceptive trade practices laws to cover online activities. Oregon has expanded its state deceptive trade practices law to include a violation for being materially inconsistent with a company's website related to the use, disclosure, collection, maintenance, or destruction of personal information.[115] This expansion of the state deceptive practices law is similar to laws in Pennsylvania and Nebraska.[116]

States have also enacted statutes to promote biometric information privacy. Illinois first passed its biometric data privacy law in 2008,[117] with Texas enacting one in 2009.[118] More recently, and after limited state legislative action, Washington also passed a biometric privacy law in 2017.[119] Although the Illinois and Texas statutes have been on the books for over a decade, plaintiffs' attorneys have just recently recognized the potential application.[120] Plaintiffs initially had difficulty prevailing because of the lack

---

[112] *See* OHIO REV. CODE ANN. § 1354.04 (West 2019) (noting limitation of private right of action).

[113] *Id.* § 1354.03. In addition to a NIST framework, a compliant entity could use other frameworks such as FedRAMP, CIS Critical Security Controls or ISO 27000. The federal programs include HIPAA, GLBA, FISMA and HITECH.

[114] *Id.* § 1354.03(D).

[115] *See generally* David Kitchen & Alan L. Friel, *Oregon Expands Deceptive Trade Practices Act to Include Misrepresentations About PI Usage*, BAKERHOSTETLER DATA PRIVACY MONITOR (Jul. 26, 2017), https://www.dataprivacymonitor.com/enforcement/oregon-expands-deceptive-trade-practices-act-to-include-misrepresentations-about-pi-usage/.

[116] *Id*.

[117] 740 ILL. COMP. STAT. 14/1 (2008).

[118] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2018).

[119] H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2018).

[120] *See* Jeffrey L. Widman, *Measuring the Impact of the Illinois Biometric Information Privacy* Act, FOX ROTHSCHILD PRIVACY COMPLIANCE AND DATA SECURITY (June 21, 2018), https://dataprivacy.foxrothschild.com/2018/06/articles/data-protection-law-

of injury.[121] But in 2019, the Illinois Supreme Court reversed this trend, stating that "a person need not have sustained actual damage beyond violation of his or her rights under the [Biometric Information Privacy] Act in order to bring an action under it."[122] The willingness of the Illinois Supreme Court to recognize the potential harm in biometric privacy invasion highlights the growing concerns in the U.S. over privacy.[123]

These states' actions represent just a few of the significant changes to cyber privacy laws across the U.S.[124] California has added additional laws beyond those covered. Furthermore, many other states have enacted one or more Internet, privacy, or cybersecurity laws. These states include Arizona,[125] Connecticut,[126] Delaware,[127] Minnesota,[128] Missouri,[129] Nebraska,[130] Oregon,[131] Pennsylvania, [132] and many others.

---

compliance/the-illinois-biometric-information-privacy-act/ (noting the recent increase in class actions filed for alleged BIPA violations).

[121] *See e.g.*, Santana v. Take-Two Interactive Software, Inc., 717 F. App'x. 12, 16–18 (2d Cir. 2017) (affirming holding that plaintiffs failed to allege defendant-company's alleged Illinois BIPA violations raised a material risk of improper data access by third parties); *see also* Rosenbach v. Six Flags Ent. Corp., No. 2–17–0317, 2017 IL App (2d) 170317, *1 (Ill. App. Ct. Dec. 21, 2017) (affirming that a plaintiff "aggrieved" by a BIPA violation must allege that such a violation caused actual harm), *rev'd*, 2019 IL 123186, *5 (Ill. Jan. 25, 2019).

[122] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, *5 (reversing holding that actual damage is required to bring an action under BIPA).

[123] *See e.g.*, Catalin Cimpanu, *Wendy's Faces Lawsuit For Unlawfully Collecting Employee Fingerprints,* ZDNET: ZERO DAY (Sep. 23, 2018, 8:10 AM), https://www.zdnet.com/article/wendys-faces-lawsuit-for-unlawfully-collecting-employee-fingerprints/ (discussing a 2018 class-action BIPA case filed in Illinois state court).

[124] *See generally*, *State Laws Related to Internet Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Feb. 8, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (listing current state laws related to internet privacy).

[125] ARIZ. REV. STAT. ANN. § 41-151.22 (2018) (e-Reader privacy).

[126] CONN. GEN. STAT. § 42-471 (2018) (online social security number protection).

[127] DEL. CODE ANN. tit. 6, §§ 1205C, 1206C (2018) (notification of privacy policy and e-Reader privacy, respectively).

[128] MINN. STAT. §§ 325M.01-.09 (2018) (protection of search behavior).

[129] Mo. REV. STAT. § 182.815, 182.817 (2018) (e-Reader privacy).

[130] NEB. REV. STAT. § 87-302(14) (2018) (privacy policy).

[131] OR. REV. STAT. § 646.607 (2018) (privacy policy).

[132] 18 PA. STAT. AND CONS. STAT. ANN. § 4107(a)(10) (West 2018) (privacy policy).

The enactment of state-level legislation highlights the growing national concern over data misuse and distrust of the corporate institutions collecting and sharing personal information. The same trends that are driving global politics are equally at play in setting local policies.

c. Expansion of Federal Export Controls to Address Cyber Concerns

At the federal level, one recent piece of legislation is the Export Controls Act of 2018 (ECA).[133] The ECA expands the categories of products subject to export controls,[134] a move consistent with current national protectionist trends. Although the statute does not specify particular technologies subject to the new controls, the new regulated products may include those related to "cybersecurity, artificial intelligence, machine learning, autonomous vehicles, 3D printing, augmented virtual reality, gene editing, financial technology, semiconductors, robotics, nanotechnology and biotechnology."[135] Specifically, the ECA requires that the Department of Commerce establish controls on emerging and foundational technologies, requiring additional export licenses, and taking into account the potential end-users of the technology and the uses to which the technology will be put.[136]

The vague outline of the export controls is likely related to the concerns raised by the Department of Defense that "the U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting."[137] However, the ECA's expansion of export

---

[133] Pub. L. No. 115-232, § 1751 et seq., 132 Stat. 2209 (2018) (part of the National Defense Authorization Act).

[134] *Id.* at § 1758.

[135] Burt Braverman & Brian Wong, *Congress Enacts the Export Controls Act of 2018, Extending Controls to Emerging and Foundational Technologies*, DAVIS WRIGHT TREMAINE LLP BLOG (Sept. 26, 2018), https://www.dwt.com/Congress-Enacts-the-Export-Controls-Act-of-2018-Extending-Controls-to-Emerging-and-Foundational-Technologies-09-26-2018/ (citing Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation,* DEFENSE INNOVATION UNIT EXPERIMENTAL (DIUX) (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.)

[136] Export Controls Act, Pub. L. No. 115-232, § 1758, 132 Stat. 2209 (2018); *see generally* Braverman, *supra* note 135.

[137] Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown*

controls does reflect a recognition that "China is executing a multi-decade plan to transfer technology to increase the size and value-add of its economy, currently the world's 2nd largest. By 2050, China may be 150% the size of the U.S. and decrease U.S. relevance globally."[138]

d. U.S. Judicial Demand for Privacy Protection

In addition to the reassertion of privacy norms by nations and U.S. states, the U.S. Supreme Court has significantly expanded privacy protections under its Fourth Amendment jurisprudence.[139] Although the Court has struggled in the past decade to develop a coherent approach to privacy,[140] it has recently recognized the massive role of technology in citizens' private lives.[141] For example, in *Carpenter v. U.S.*, the Court held that prosecutors' sequester of cell phone GPS data without a warrant constituted an illegal search in violation of the Fourth Amendment.[142] Writing for the majority, Chief Justice Roberts rejected the lower standard of privacy in section 2703(d) of the Stored Communications Act, which enabled law enforcement to access private cell phone data by simply showing that cell-site location information (CSLI) may be pertinent to an investigation, and held that Carpenter's Fourth Amendment rights had been violated.[143] Specifically, he noted that:

Jewels of U.S. Innovation, DEFENSE INNOVATION UNIT EXPERIMENTAL (DIUX) (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

[138] *Id*. at 3.

[139] *See* United States v. Jones, 565 U.S. 400, 400 (2012) (holding that the government attaching a GPS device to the vehicle to monitor the vehicle's movements constitutes a Fourth Amendment search).

[140] *See id.* at 417–18 (Sotomayor, J., concurring) (discussing the modern issues of what is a "reasonable expectation in privacy").

[141] *See id.* at 419 (Alito, J., concurring) (approaching the issue by considering "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."); *see* Riley v. California, 573 U.S. 373, 395 (2014) (affirming suppression of cell phone evidence and noting that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."); *see* Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015) (stating "a State . . . conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements," but remanding on separate question of reasonableness for tracking policies).

[142] Carpenter v. United States, 138 S. Ct. 2206, 2217–21 (2018).

[143] *See Carpenter*, 138 S. Ct. at 2221.

> Whether the Government employs its own surveillance technology as in *Jones*[144] or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[145]

The Court was clear: the lower standard of CSLI data privacy under the Stored Communications Act was "a 'gigantic' departure from the probable cause rule"[146]and therefore, "an order issued under section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant."[147]

The *Carpenter* decision was intimated by *Jones*, but is much starker in tone.[148] The Government's ability to engage in pervasive surveillance requires that the Fourth Amendment be invoked to require search warrants. Relevance is not an acceptable standard:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not . . . call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.[149]

However, following the *Carpenter* decision, not all lower courts have reversed criminal cases that rely on CSLI searches under section

---

[144] *Jones*, 565 U.S. 400 (2012).

[145] *Carpenter*, 138 S. Ct. at 2217.

[146] *Id*. at 2221.

[147] *Id*.

[148] *See Jones*, 565 U.S. at 411–12 (using a limited physical trespass analysis to find Fourth Amendment violation, without addressing broader concerns raised in the concurrence for "cases that do not involve physical contact, such as those that involve the transmission of electronic signals.").

[149] *Carpenter,* 138. S.Ct. at 2220.

2703(d) of the Stored Communications Act.[150] For example, one court applying *Carpenter* found that the previous CSLI searches fell within the good-faith exception to the warrant requirement, because the officers acted in good faith that the order was within constitutional bounds under its circuit precedent.[151]

e. Why the State Cares: The Public Wants its Privacy Back

The consistent pattern of national governments, state governments, and even the Supreme Court, highlights an emphasis on resurrecting privacy. In the U.S., this change in the zeitgeist is likely attributable to the cascade of data protection failures at high-profile companies such as Facebook[152] and Uber.[153] But in terms of sheer volume, the top data protection failure for 2018 likely goes to Aadhaar, the Indian authority that manages the personal identity card of every person in India.[154]

In early 2018, login credentials on Aadhaar were sold to Tribune News Service reporters for 500 rupees, enabling access to the information of any of the 1.1 billion Indian citizens in the database.[155] "[Y]ou could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification

---

[150] *See e.g.*, United States v. Scott, No. 4:17-CR-50, 2018 WL 5087237, at *2 (S.D. Ga. Oct. 18, 2018) (applying a good faith exception to CSLI data acquired under a section 2730(d) request, because the request occurred 11 months before the *Carpenter* case and when the prosecutors still believed the acquisition was constitutional).

[151] *See id.*at *2 (applying the good-faith exception as cited in United States v. Leon, 468 U.S. 897, 919–21 (1984)).

[152] *See e.g.*, Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html ("[T]hree software flaws in Facebook's systems allowed hackers to break into user accounts," exposing 50 million users.).

[153] *See* Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html (discussing a 2016 hack and subsequent cover up by Uber, where hackers stole data from over 57 million user accounts).

[154] *See* David Bisson*, The 10 Biggest Data Breaches of 2018. . . So Far, July 2018*, ALERT LOGIC BLOG (July 16, 2018), https://blog.barkly.com/biggest-data-breaches-2018-so-far (discussing Aadhaar hack which impacted 1.1 billion India citizens).

[155] Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, INDIA TRIBUNE NEWS SERVICE (Jan. 4, 2018), https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

Authority of India), including name, address, postal code (PIN), photo, phone number and email."[156]

U.S.-based Facebook also failed to secure its single sign-in feature, which resulted in a massive data breach across multiple user platforms that affected 50 million people.[157] The single sign-in feature vulnerability also meant that Facebook users were potentially vulnerable on any other sites where they had used their Facebook accounts to login, exponentially expanding the potential scale of the breach.[158] In March 2018, Facebook was also forced to admit that it collected data on people's phone calls and texts, though it denied that it was data mining the contents of these interactions.[159] Facebook also claimed that the data collection was only done with the user's consent to improve the user's experience on the platform.[160]

Facebook also faces a lawsuit by Pikinis app developer Six4Three, which alleges "the social network's chief executive 'weaponized' the ability to access data from any user's network of friends—the feature at the heart of the Cambridge Analytica scandal."[161] These reports come on the heels of Facebook's failure to manage the misuse of customer data by Cambridge Analytica.[162] Although the actual data protection failures occurred in 2016, the full extent was not discovered until 2018.[163] The aftermath, therefore, has been a 2018 phenomenon.

---

[156] *Id.*

[157] Isaac, *Facebook Security Breach Exposes Accounts of 50 Million Users*, *supra* note 152.

[158] *Id.*

[159] Andrew Griffin, *Facebook Admits Collecting Phone Call and Text From People's Phones, But Claims It Had Consent*, INDEP. (Mar. 26, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-cambridge-analytica-data-my-download-phone-calls-text-messages-contacts-history-a8274211.html.

[160] *Id.*

[161] Carole Cadwalladr & Emma Graham-Harrison, *Zuckerberg Set Up Fraudulent Scheme To 'Weaponise' Data, Court Case Alleges*, GUARDIAN (May 24, 2018), https://www.theguardian.com/technology/2018/may/24/mark-zuckerberg-set-up-fraudulent-scheme-weaponise-data-facebook-court-case-alleges; *see also* Six4Three LLC v. Facebook Inc., No. 17-CV-359, 2017 WL 657004, at *1 (N.D. Cal. Feb. 17, 2017) (overcoming Facebook effort to remove case to federal court).

[162] *See* Paul Lewis & Paul Hilder, *Leaked: Cambridge Analytica's Blueprint For Trump Victory*, GUARDIAN (Mar. 23, 2018, 8:53 AM), https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

[163] *Id.*

The Guardian obtained a 27-page presentation produced by Cambridge Analytica in the aftermath of the Trump victory to show employees its effectiveness.[164] "Intensive survey research, data modelling and performance-optimizing algorithms were used to target 10,000 different ads to different audiences in the months leading up to the election. The ads were viewed billions of times . . . ."[165] This was the content created on behalf of the Trump campaign, not the information made by the Russians or other third parties.[166]

These and many other society-damaging activities by Facebook earned it the sobriquet "menace" to society and "obstacle[] to innovation" from philanthropist George Soros at the World Economic Summit.[167] In response, Facebook hired the right-leaning Definers Public Affairs organization to investigate and smear Soros.[168] Facebook's leadership also lied about the hiring of Definers and strategically released an admission during late November 2018 to bury its disclosure.[169]

The manipulation of Google, Facebook, Twitter, and Snapchat through legal advertising strategies and exploitation of Facebook's lax partnership agreements have been linked to Trump's victory in 2016.[170] In Britain, the Information Commissioner's Office (ICO) found two violations of the 1998 UK Data Protection Act, which could result in a fine of up to

---

[164] *Id*.

[165] *Id*.

[166] *But see* Donie O'Sullivan et al., *Cambridge Analytica's Facebook Data Accessed from Russia, MP Says*, CNN (July 17, 2018), https://money.cnn.com/2018/07/17/technology/cambridge-analytica-data-facebook-russia/index.html (noting a possible relationship between Russia and Cambridge Analytica).

[167] George Soros, Philanthropist, Remarks delivered at the World Economic Forum (Jan. 25, 2018).

[168] Laura Mandaro, *Facebook Admits It Asked Opposition Firm Definers to Investigate George Soros*, FORBES (Nov. 21, 2018, https://www.forbes.com/sites/forbes/2018/11/21/facebook-admits-it-asked-definers-to-look-into-george-soros/#33fb327f37c8; s*ee also* Sheera Frenkel et al., *Delay, Deny, Deflect: How Facebook Leaders Leaned Out in Crisis*, N.Y. TIMES (Nov. 15, 201), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html (discussing Facebook's relationship with Definers Public Affairs company).

[169] Nellie Bowles & Zach Wichter, *On Thanksgiving Eve, Facebook Acknowledges Details of Times Investigation*, N.Y. TIMES (Nov. 23, 2018), https://www.nytimes.com/2018/11/22/business/on-thanksgiving-eve-facebook-acknowledges-details-of-times-investigation.html.

[170] Lewis, *supra* note 162.

£500,000.[171] Despite the many crimes and failures of Facebook, it is certainly not alone in failing to protect data from outside threats and management failures and has fueled the populist antagonism by its misconduct. In consequence, the publicness of Facebook's data privacy failures has likely motivated the current public push towards more data security.[172]

One of the largest data breaches of 2018 was tied to Marriott, which stemmed from its acquisition of the Starwood hotel group.[173] The size of the potential breach included 383 million people.[174] In addition, Starwood, which was the source of the cyber network vulnerability, failed to encrypt the passport numbers for at least 5.25 million hotel customers, who had their passport numbers stolen in plain text.[175] An additional 20.3 million passport numbers were stolen, but those numbers were protected by encryption.[176]

The thefts have been attributed to the Chinese Ministry of State Security.[177] China plans to commit over $150 billion towards quantum computing.[178] Absent lattice-based encryption or other quantum encryption

---

[171] Warwick Ashford, *Facebook Could Face ICO Fine of Up to £500,000*, COMPUTERWEEKLY.COM (July 11, 2018, 9:30 AM), https://www.computerweekly.com/news/252444559/Facebook-could-face-ICO-fine-of-up-to-500000.

[172] *See* Layton, *supra* note 28, at 236, 242 (discussing the role of GDPR for its efforts to achieve European geopolitical goals and response to Facebook abuse of market power).

[173] *See* Ellen Nakashima & Craig Timberg*, U.S. Investigators Point to China in Marriott Hack Affecting 500 Million Guests*, WASH. POST (Dec. 11, 2018), https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/ ("Marriott acquired Starwood in 2016 and kept the reservation databases separate from its own until recently. The reservation system of Marriott hotels themselves was not affected by the breach.").

[174] Peter Holley, *Marriott: Hackers Accessed More Than 5 Million Passport Numbers During November's Massive Data Breach*, WASH. POST (Jan. 4, 2019), https://www.washingtonpost.com/technology/2019/01/04/marriott-hackers-accessed-more-than-million-passport-numbers-during-novembers-massive-data-breach/ ("Marriott also said that the breach affected an estimated 383 million 'unique guests,' down from the original estimate of 500 million given when the company said in November that its Starwood guest reservations database had been penetrated by hackers.").

[175] *Id*.

[176] *Id.*

[177] Michael Balsamo, *China Suspected in Huge Marriott Data Breach, Official Says*, ASSOCIATED PRESS (Dec. 12, 2018), https://www.apnews.com/4032b90c40824fbb892206702c5d30ad.

[178] Arthur Herman, *China's Brave New World of AI*, FORBES (Aug. 30, 2018, 9:53 AM), https://www.forbes.com/sites/arthurherman/2018/08/30/chinas-brave-new-world-of-ai/#32b786f028e9.

techniques, it is inevitable that the encrypted information stolen and stored will be unlocked by the increasingly operational quantum computers.[179]

The healthcare industry has also experienced significant data breaches in 2018, which has likely contributed to growing public sentiment toward data privacy. Between January and August, there were 229 data breaches impacting 6.1 million accounts.[180] In addition, the U.S. Centers for Medicare and Medicaid Services reported that Healthcare.gov was breached less than two weeks before open enrollment for the Affordable Care Act, with 75,000 records accessed.[181] The health care risks are arguably more serious because of the personal nature of the information available.

There have been many other cyber-attacks beyond the healthcare context. Panera Bread, for example, stored customer data in plaintext on a publicly available website.[182] The Panera Bread breach is believed to have impacted as many as 37 million customers, though the company is reporting only a fraction of that.[183] Third-party app Timehop, which leverages data from social media sites, was hacked, exposing information of 21 million users.[184] GovPayNet exposed the receipts of 14 million users of the government payment platform.[185] Cathay Pacific Airways' data breach exposing 9.4 mission records.[186] Finally, to end 2018, Tribune Publishing suffered a cyber-attack that affected its printing centers for all current and former Tribune Publishing newspapers, including stopping the distribution of Los

---

[179] *Quantum Computers Will Break the Encryption That Protects the Internet*, ECONOMIST (Oct. 20, 2018), https://www.economist.com/science-and-technology/2018/10/20/quantum-computers-will-break-the-encryption-that-protects-the-internet.

[180] Marianne Kolbasuk McGee, *Health Data Breach Victim Tally for 2018 Soars*, HEALTHCARE INFO SECURITY (Aug. 21, 2018), https://www.healthcareinfosecurity.com/health-data-breach-victim-tally-for-2018-soars-a-11407.

[181] Susan Morse, *CMS Responds to Data Breach Affecting 75,000 in Federal ACA Portal*, HEALTHCARE FIN. (Oct. 22, 2018), https://www.healthcarefinancenews.com/news/cms-responds-data-breach-affecting-75000-federal-aca-portal.

[182] *Top 10 Application Security Data Breaches of 2018*, HIGH-TECH BRIDGE (Nov. 20, 2018), https://www.htbridge.com/blog/top-ten-application-security-databreaches-2018.html.

[183] *Id*. (citing security analyst Brian Krebs).

[184] *Id.* For example of a post-GDPR breach notification, *see* Press Release, TIMEHOP, Timehop Security Incident (July 4, 2018) (providing in-depth overview of hack).

[185] *Top 10 Application Security Data Breaches of 2018*, *supra* note 182.

[186] *Id*.

Angeles Times' Saturday's edition.[187] This is a fraction of the list of successful cyber-incursions and ransomware attacks in recent history.

The consequences of systemic data breaches are taking their toll. A World Economic Forum (WEF) survey, which included global data from over 12,000 executives, found that cybersecurity risk had moved from being a top concern in only North America in 2016, to the top concern for three of the eight regions in 2018.[188] The different global regions had different top concerns.[189] "[C]yber-attacks were considered the number one risk by executives in Europe and advanced economies, while failure of national governance was the top concern for their Latin American counterparts."[190] The study's findings point to a need for government action.[191] More specifically, "[c]yber-attacks [were] seen as the number one risk for doing business in markets that account for 50% of global GDP . . . ."[192] "This strongly suggests that governments and businesses need to strengthen cyber security and resilience in order to maintain confidence in a highly connected digital economy."[193]

Business leaders' concern in economically developed countries reflects the increasing challenge of responding to cyber-attacks, the increased cost of security failures, and the risks associated with operating a business in today's cyber world. Downtime, ransomware, customer attrition, regulatory fines, and lawsuits are combining to add to the cost of each attack while the rate of attacks is likely to only increase.[194] In addition, malicious or

---

[187] Emily Alpert Reyes et al., *Foreign Cyberattack Hits Newspapers: Here Is What We Know*, L.A. TIMES (Dec. 29, 2018), https://www.latimes.com/local/lanow/la-me-cyberattack-times-newspaper-malware-20181229-story.html.

[188] Chloe Taylor, *Cyber-Attacks, Weak Government, and Energy Shocks Pose Biggest Risks to Firms*, *WEF Finds*, CNBC (Nov. 12, 2018), https://www.cnbc.com/2018/11/12/cyber-attacks-and-weak-government-among-biggest-risks-to-firms-wef.html ("WEF head of global risks and geopolitical agenda Aengus Collins said that the report had helped the organisation uncover some eye-catching trends. 'Cyber-attacks are increasing in prominence, but it is striking how many business leaders point to unemployment and national governance as the most pressing risks for doing business . . . .'").

[189] *Id.*

[190] *Id*.

[191] *Id.* (quoting Lori Bailey, Global Head of Cyber Risk, Zurich Insurance Group).

[192] *Id.*

[193] *Id.*

[194] *See* IBM SECURITY, 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 6 (July 2018). https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf (The four cost centers of a data breach are "detection and escalation;"

criminal attacks now account for 48% of the data breaches, making the need to respond to these outward attacks an even larger priority.[195]

V. CYBERSECURITY INSTABILITY IS MERELY A SYMPTOM: WHERE THE WORLD IS HEADED

The increased concern among the economically developed nations over cybersecurity risk and the tensions between the U.S. conglomerates and European and Asian regulators will likely drive the public policy for the coming years. The overlapping agenda among Asian and European regulators and U.S. states will blunt any global tension regarding disagreements over worldwide privacy policies.[196] California's new privacy laws, for example, "echoes many of [the GDPR] rights, and it is likely that future U.S. privacy legislation—whether at the state or federal level—will also incorporate components of these affirmative information rights."[197] The interest in expanding customer privacy will likely not be seen as a conflict between the U.S. and the EU precisely because states are struggling to enforce GDPR inspired laws within the U.S.[198]

a. Impact of Cyber Espionage on Policy

At the same time, there remains great distrust toward Russia, and likely other nondemocratic regimes, to the extent to which they are harboring, promoting, or operating cyberattacks against the West.[199] For example,

---

"notification costs;" "post data breach response" – including fines, discounts, and legal expenditures; and "lost business cost." Ransomware payments were not included in study.)

[195] *Id*. at 19 (Human error was responsible for 27% of the breaches while system glitches were responsible for 25% of the failures.).

[196] *See e.g.*, George P. Slefo, *Marketers and Tech Companies Confront California's Version of GDPR*, ADAGE (June 29, 2018), https://adage.com/article/digital/california-passed-version-gdpr/314079 ("Consumers' personal information is clearly endangered and consumers are fed up with impacts that could last a lifetime . . . . Thus far, 48 states in all have enacted privacy laws requiring notification of security breaches involving personal information. Echoing global initiatives, especially the E.U.'s GDPR, the trend to more closely govern personal data will continue.'" (quoting Chris Olson, CEO of the Media Trust)).

[197] Joseph Jerome, *California Privacy Law Shows Data Protection is on the March,* ANTITRUST MAG., Fall 2018, at 96.

[198] *See id*. (noting significant similarities regarding compliance and practical requirements between the GDPR and CCPA).

[199] *See e.g.*, Nicu Popescu, *Russian Cyber Sins and Storms*, EUROPEAN COUNCIL ON FOREIGN RELATIONS (Oct. 10, 2018), https://www.ecfr.eu/article/commentary_russian_

in April 2017, the Dutch government expelled "four Russian hackers with diplomatic passports attempting to snoop on the Organisation for the Prohibition of Chemical Weapons."[200] Two questions remain: how will these foreign cyber adversaries evolve, and how will their choices impact the public?

> That Russia is very active in cyber-espionage should be a source of concern, but certainly not indignation. The American, Chinese, French, British, Iranian or North Korean governments are among the most active cyber-spies in the world. And Russian cyber-espionage is not a recent phenomenon. … It is quite possible that China has even more access to sensitive political, security, technical or business information from the entire world, and is quietly passing what is relevant to its companies, manufacturers, or the military.[201]

This suggests that cyber-espionage is simply part of the new normal, tucked neatly into noise created by criminal cybercrime and accepted as the state of digital warfare. The consequences are changing the world, and mere privacy regulation is likely insufficient.[202]

As evidence of this new normal, the U.S. Department of Justice filed an indictment against a division of the Chinese Ministry of State Security's Tianjin State Security Bureau, known as Advanced Persistent Threat 10 ("APT10").[203] The APT10 hacking group was active in the U.S. since 2006 and continued in various forms unabated until the time of the indictment.[204]

---

cyber_sins_and_storms (discussing the wave of indignation towards Russian-supported cyber activities).

[200] *Id*.

[201] *Id*.

[202] *See* Jared Keller, *Hacking is the New Norma*l, PACIFIC STANDARD (June 8, 2015), https://psmag.com/news/hacking-is-the-new-normal (discussing the pervasive nature of cyberattacks by nation states and noting that "[e]veryday Americans face the risk of cyberattack more than ever before.").

[203] *See generally* Sealed Indictment at 1-2, United States v. Hua, 18 Cr. 891 (S.D.N.Y. Dec. 17, 2018) (noting defendant-hackers are part of "hacking group operating in China known . . . as Advanced Persistent Threat 10 (the 'APT10 Group') . . . .") [hereinafter APT10 Indictment]; *see also* Press Release, U.S. Dept. Justice, Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion [hereinafter APT10 Press Release].

[204] APT10 Press Release, *supra* note 203.

These allegations are representative of the activities described by the FBI and Defense Criminal Investigation Service:

> 5.Over the course of the Technology Theft Campaign, the defendants and their co-conspirators successfully obtained unauthorized access to at least approximately 90 computers belonging to, among others, commercial and defense technology companies and U.S. Government agencies located in at least 12 states, and stole hundreds of gigabytes of sensitive data and information from their computer systems, including from at least the following victims:
>
> a. seven companies involved in aviation, space and/or satellite technology;
> b. three companies involved in communications technology;
> c. three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments;
> d. a company involved in maritime technology;
> e. a company involved in oil and gas drilling, production, and processing;
> f. The National Aeronautics and Space Administration ("NASA") Goddard Space Center; and
> g. The NASA Jet Propulsion Laboratory.…
>
> 10. Finally, the APTl0 Group also compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.[205]

The indictment highlights the pervasive efforts undertaken by the Tianjin State Security Bureau, and notes that "the APTl0 Group's hacking operations evolved over time, demonstrating advances in overcoming network defenses, victim selection, and tradecraft."[206]

b. Impact of Globalization and Economic Displacement on Cybersecurity

Against the backdrop of this cyber cold war, a Department of Defense (DoD) report raises non-military alarms regarding the existential threat posed to the West by the Chinese goals for global hegemony.[207]

---

[205] APT10 Indictment, *supra* note 203, at 9–10, 14.

[206] *Id.* at 2.

[207] *See generally* Brown, *supra* note 137.

Among the risks highlighted by the report are the economic threat, specifically that in the next 30 years, China's economy may be 150% the size of the U.S., which will decrease the U.S.'s power globally.[208] In addition, the DoD highlights both the legal and illegal strategies of China, such as "industrial espionage," wherein China employs "hundreds of thousands of Chinese army professionals" to conduct its campaign of cybertheft,[209] and that "25% of U.S. STEM graduate students are Chinese foreign nationals."[210] Whether or not the report provides an accurate reflection of the true risk the Chinese strategy poses to the West, it outlines the U.S. government's concern on its own technology relevancy.

The underlying relationship between the East and West has continued to erode under 21st-century economic pressures, state disintermediation, and the tensions of the Middle East.[211] It is not enough to recognize that the government control over the movement of labor and people has eroded in the age of globalization.[212] Fears of economic displacement relating to immigration have raised further concerns that "could have grave consequences" for the world's democracies.[213]

---

[208] *Id*. at 3.

[209] *Id.*

[210] *Id*.

[211] *See, e.g.*, Yury Barmin, *Syria and the Beginning of a New Cold War*, AL JAZEERA (Apr. 23, 2018), https://www.aljazeera.com/indepth/opinion/syria-beginning-cold-war-180422075430047.html ("Events of the past few months, indeed, have shown that the conflict in Syria has gradually assumed the character of a Cold War-style struggle. Just like during the Cold War of the 20th century, today, positive diplomatic engagement between Russia and the US has been reduced to communication and coordination to avoid direct military confrontation."); *see also* Julian Borger & Lily Kuo, US-China Tensions Soar as 'New Cold War' Heats Up, GUARDIAN (Oct. 16, 2018), https://www.theguardian.com /world/2018/oct/16/us-china-new-cold-war-tensions ("Chinese officials have accused Washington of starting a new cold war, but the jostling between the two powers has already shown its potential to turn hot through accident or miscalculation, if action is not taken to defuse tensions.").

[212] *See* Garon, *Revolutions and Expatriates: Social Networking, Ubiquitous Media and the Disintermediation of the State*, *supra* note 58, at 302–04.

[213] William A. Galston, *The Rise of European Populism and the Collapse of the Center-Left*, BROOKINGS (Mar. 8, 2018), https://www.brookings.edu/blog/order-from-chaos/2018 /03/08/the-rise-of-european-populism-and-the-collapse-of-the-center-left/ ("Immigration raises cultural and security concerns as well as fears of economic displacement, and it weakens the legitimacy of transnational institutions that are seen as preventing sovereign peoples from using national political means to protect themselves against the threatening developments."); *see also* Kelsey P. Norman & Lisel Hintz, T*he Real Refugee Crisis is in*

The relationship between the cyber changes and the impacts of globalization are beyond the scope of this Article, but it is highly suggestive that social media, the Arab Spring, and state-sponsored cyber espionage are interwoven into the political and economic landscape shaping these changes.[214]

c. The Growth of the Internet of Things, Cultural Challenges, and Policy

Next add the growth of the Internet of Things (IoT) into the mix. "The Internet of Things is predicted to revolutionize the way in which we live our lives, with many industry experts tipping it to have the biggest technological impact since cloud computing, as more data than ever before can be collected, stored and analysed."[215] It is predicted to allow hospitals to better monitor patients, allow municipalities to monitor traffic, pollution, and much more.[216] Industry giant GE estimates improvements in industry productivity will generate $10 trillion to $15 trillion in GDP worldwide over the next fifteen years.[217] Essentially, "IoT is making businesses rethink their models, products, the way they offer products and their pricing."[218]

---

the Middle East, Not Europe, PROJECT ON MIDDLE EAST POLITICAL SCIENCE (2017), https://pomeps.org/2017/03/29/the-real-refugee-crisis-is-in-the-middle-east-not-europe/ ("A supra-national entity of 500 million, the E.U. is up in arms at the 1 million Syrian refugees who entered its borders last year.") (last visited Apr. 6, 2019).

[214] *See* Garon, *Revolutions and Expatriates: Social Networking, Ubiquitous Media and the Disintermediation of the State*, *supra* note 58, at 297 ("At its extreme, this interconnectedness may illustrate the declining role of the nation-state in an information economy. As both goods and information have moved toward a networked, global economy, the ability of a country to control production of goods and management of content has ebbed.").

[215] Mike Moore, *What is the IoT? Everything You Need to Know*, TECHRADAR PRO (Nov. 15, 2018), https://www.techradar.com/news/what-is-the-iot-everything-you-need-to-know.

[216] *Id*.

[217] Swati Kashyap, *10 Real World Applications of Internet of Things (IoT) – Explained in Videos*, ANALYTICS VIDHYA (Aug. 26, 2016), https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/.

[218] James Buckley, *How Banks Can Create A Successful IoT Strategy*, TECHRADAR PRO (Nov. 8, 2018), https://www.techradar.com/news/how-banks-can-create-a-successful-iot-strategy.

For many of these businesses, there is also an automated IoT enabled payment system connected to the relationship.[219] Add to this another technological darling—blockchain[220]—and the potential for a consumer or citizen experience that is fundamentally different than the technologies of today.[221] This transition to IoT blockchain-based payment systems may be on the horizon, but not in the upcoming year.[222] In the meantime, scalability, processing power, interoperability, and other challenges may make the enthusiasm behind these technologies overshadow their reality.[223] But the hype leads competitors to feel left behind, which in turn fuels a global sense that the most resource-rich, most powerful, and most cutting-edge entities will create a future on their own terms.

> Imagine you are a French lawmaker. For decades, you have protected your nation's cultural output with the diligence of a gardener tending a fragile patch against invasive killer weeds.
>
> You have imposed quotas on the French film industry, required radio stations to play more French music than anyone seems to want to listen to, and you have worked methodically to exempt your actions from international free-trade rules.
>
> And now, out of nowhere, come a handful of American technology companies to wash away all your cultural defenses. Suddenly just about everything that a French citizen buys, reads, watches or listens to flows in some way or another through these behemoths.
>
> There is Facebook co-opting your news media. Amazon is dominating book sales, while YouTube and Netflix are taking over television and movies. And the smartphone, arguably the most

---

[219] *Id*. ("The hand-shake between the consumer side and the supplier side in any transaction between things requires a financial exchange. This puts banks and payments at the center of every IoT ecosystem.").

[220] *See generally* Christian Legare, *Blockchain & IoT Convergence: Is It Happening?,* EE TIMES (Feb. 16, 2018), https://www.eetimes.com/author.asp?section_id=36&doc_id=1332967.

[221] *See* Buckley, *supra* note 218 (discussing that banking is at the center of the future IoT ecosystem).

[222] Legare, *supra* note 220 ("The blending of blockchain with the billions of IoT devices is not for the immediate future. Blockchain processing tasks are computationally difficult and time-consuming, and IoT devices are still relatively underpowered, lacking the processing power to directly participate in a blockchain.").

[223] *See id*. (discussing the shortcomings of a blockchain model).

> important platform for entertainment in this era, is controlled almost entirely by Apple and Google.[224]

The scenario helps explain GDPR, but it also does much more. Imagine instead that you are Vladimir Putin, Xi Jinping, or Kim Jong-un, an undisputed absolute ruler of your regime. These cultural challenges are vexing.[225] The threat of technological irrelevance is much, much worse—it is truly horrifying.[226] For revisionist countries, the threat of the digital divide is propelling increasingly aggressive and reckless responses.[227]

At the 2018 Bloomberg New Economy Forum in Singapore, former U.S. Treasury secretary Hank Paulson warned of an "Economic Iron Curtain," which would divide the world into estranged economic spheres if the U.S. and China failed to resolve their strategic differences.[228] Paulson

---

[224] Farhad Manjoo, *Why the World is Drawing Battle Lines Against American Tech Giants*, N.Y. TIMES (June 1, 2016), https://www.nytimes.com/2016/06/02/technology/why-the-world-is-drawing-battle-lines-against-american-tech-giants.html.

[225] *See* U.S. DEPT. DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA: SHARPENING THE AMERICAN MILITARY'S COMPETITIVE EDGE 2 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf ("The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.").

[226] *But see* Yuval Noah Harari, *Why Technology Favors Tyranny*, ATLANTIC MAGAZINE (Oct. 2018), https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/ (discussing technology's threat to all governments and the fear felt by common people unfamiliar with new technology and its application to them).

[227] *See, e.g.*, Matthew Bey, *The Coming Tech War with China*, STRATFOR (Feb. 6, 2018, https://worldview.stratfor.com/article/coming-tech-war-china ("Five years ago, by contrast, [China] was widely perceived as an imitator in technology, not an innovator. As hard as it may be for Washington to admit, China is catching up in the tech race."); Steven Pifer, *The Growing Russian Military Threat in Europe: Assessing and Addressing the Challenge: The Case of Ukraine*, BROOKINGS (May 17, 2017), https://www.brookings.edu/testimonies/the-growing-russian-military-threat-in-europe/ ("Russian President Vladimir Putin and the Kremlin leadership have . . . concluded that the European security order that developed in the aftermath of the Cold War disadvantages Russian interests. They have sought to undermine that order and define Russia in opposition to the United States and the West.").

[228] Christian Edwards, *Former U.S. Treasury Secretary Hank Paulson Warns of an 'Economic Iron Curtain' if the U.S. and China Can't Find a Way to Get Along*, BUSINESS INSIDER (Nov. 7, 2018), https://www.businessinsider.com/former-treasury-secretary-hank-paulson-warns-us-china-trade-war-2018-11.

flagged the current global tensions, noting that the world is "arriving at a moment of change, challenge, and potentially even crisis."[229]

i. Government Use of Monitoring Technologies

The new "smart" policing technologies are already among us. In the U.S., for example, the ACLU has published a report listing "costly and invasive surveillance technologies that might be recording you, your family, and your neighbors right now."[230] Some of these technologies have ubiquitous social uses, including Electronic Toll Readers (E-Z Pass Plate Readers),[231] Closed-Circuit Television (CCTV) Cameras,[232] government-owned hacking hardware and software,[233] and Police Body Cameras.[234] Other technologies are primarily limited to their surveillance purpose:

- Biometric Surveillance Technology: "Biometric surveillance technology includes facial, voice, iris, and gait-recognition software and databases. Used in combination with other surveillance technologies, like CCTV cameras, this tool can completely undermine the ability of person to travel in public or gather with friends anonymously."[235]
- Stingrays: "Also known as cell-site simulators or international mobile subscriber identity (IMSI) catchers, the device mimics a cell phone communications tower, causing your cell phone to communicate with it. This communications link gives the Stingray the ability to track your location and intercept data from your phone, including voice and typed communications."[236]
- Automatic License Plate Readers (ALPRs): "Mobile or fixed-location cameras that are used to take photographs of license plates, digitize them, and then store, process, and search

---

[229] *Id*.

[230] *See generally* ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101 (2018), https://www.aclu.org/report/community-control-over-police-surveillance-technology-101.

[231] *Id*. at 4.

[232] *Id*.

[233] *Id*. at 7.

[234] *Id*. at 8–9.

[235] *Id*. at 5.

[236] *Id*. at 3.

captured data in real time or over the course of months or even years."[237]

- ShotSpotter-Gunshot Detection Systems: "[M]icrophones that are designed to detect the sound of a gunshot. By placing them throughout an area, the microphones are able to triangulate a gunshot and provide police with a limited geographic location from which a gunshot emanated."[238]
- Surveillance-Enabled Light Bulbs: Camera and microphone equipped, networked LED light bulbs are sold with built in surveillance capabilities that can turn any room into an invisibly monitored space.[239]
- Social Media Monitoring: "This software can be used to covertly monitor, collect, and analyze individuals' social media data from platforms like Twitter, Facebook, and Instagram. It can identify social media posts and users based on specific keywords; geographically track people as they communicate; chart people's relationships, networks, and associations; monitor protests; identify the leaders of political and social movements; and measure a person's influence."[240]

These are not all the technologies in use even in the U.S.[241] Other countries use similar technologies and more, exploiting smart national identification cards to monitor the movement of the public with even greater precision.[242] These technologies are often targeted at minorities and

---

[237] *Id*. ("Some private companies provide ALPRs to the police free of charge in return for access to the data they collect and the ability to collect fees from private citizens later, such as a vehicle owner they identify as owing outstanding court fees.").

[238] *Id*. at 5.

[239] *Id*. at 6.

[240] *Id*. at 7.

[241] *See e.g.*, Adi Kamar et. al, *NSA Turns Cookies (And More) Into Surveillance Beacons,* ELECTRONIC FRONTIER FOUNDATION (Dec. 11, 2013), https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons (discussing various new technologies used by the NSA).

[242] *See e.g.*, Eva Dou, *Chinese Surveillance Expands to Muslims Making Mecca Pilgrimage*, W.S.J. (July 31, 2018), https://www.wsj.com/articles/chinese-surveillance-expands-to-muslims-making-mecca-pilgrimage-1533045703 (discussing China's use of state-issued tracking devices used for "ensur[ing] the wearer's safety" to monitor Chinese Muslims on their pilgrimage to Mecca); Loreben Tuquero, *Nothing To Be Afraid Of? Other Countries Use Their National IDs in Countless Ways*, RAPPLER (Aug. 6, 2018), https://www.rappler.com/newsbreak/iq/204657-national-id-functions-worldwide (noting various

dissidents.[243] Within the U.S., there also are significant concerns about disparate use of the technology and disparate impact of the efficiency they bring.[244]

The new technologies enable the police, intelligence community and military to respond to alleged threats.[245] The cost of expensive tools creates a need to justify the cost and prove the worth of the technology, fueling an expansion of their use.[246] This, in turn, creates market opportunities for the creators of increasingly sophisticated technologies, including more autonomous products and services.[247]

If the world once again finds itself chilling in a state of cold war, then the development of autonomous military and commercial devices pose a real and destabilizing threat to the cyber world order. "It is now undeniable that the *homeland is no longer a sanctuary*. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion."[248]

---

countries' national identity cards and the uses beyond government functions, like banking and healthcare).

[243] *See* Dou, *supra* note 242 (discussing Chinese surveillance on the minority Chinese Muslim group).

[244] *See* Tamara Evdokimova, *Turning the Tide on Police Surveillance*, NEW AM. (Sept. 20, 2018), https://www.newamerica.org/weekly/edition-218/turning-tide-police-surveillance/ (highlighting various harmful consequences that stem from the inevitable government misuse of surveillance technologies).

[245] *See e.g.*, *id.* (noting the police can use surveillance technologies, like automatic license plate readers (ALRPs), to respond more quickly and more effectively to an Amber Alert).

[246] Valarie Findlay, *Quantifying, Justifying the Costs of Body-Worn Cameras,* NAT'L POLICE FOUND. (2016), https://www.policefoundation.org/quantifying-justifying-cost-of-body-worn-cameras/ (last visited Apr. 7, 2019) (referring to the cost-benefit analysis of body-worn camera programs as an important "shell game" for the future of policing).

[247] *See* Billy Perrigo, *A Global Arms Race for Killer Robots is Transforming the Battlefield*, TIME (Apr. 9, 2018), http://time.com/5230567/killer-robots/, (noting that five years since UN talks to ban autonomous weapons, high-tech militaries, including the U.S., Russia, the U.K., Israel, South Korea and China, are using drones and weapons with increased autonomy).

[248] U.S. DEP'T DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA: SHARPENING THE AMERICAN MILITARY'S COMPETITIVE EDGE, *supra* note 225 at 3 (emphasis included).

ii. Military Use of Autonomous Weapon Technologies

Thus far, it appears that concerns over fully autonomous weapons remain theoretical for the time being.[249] But self-directed machines and devices are being developed that will inevitably put the human actor further and further into the margins of the engagement decisions.[250]

> By 2016, China had tested autonomous technologies in each domain: land, air and sea. South Korea announced in December it was planning to develop a drone swarm that could descend upon the North in the event of war. Israel already has a fully autonomous loitering munition called the Harop, which can dive-bomb radar signals without human direction and has reportedly already been used with lethal results on the battlefield. The world's most powerful nations are already at the starting blocks of a secretive and potentially deadly arms race, while regulators lag behind.[251]

Against this perceived threat, the U.S. is responding with new technologies and tactics. Self-directed autonomous weapons could change the face of warfare for those nations with the capacity to build and deploy these tools.[252] As the U.S. Department of Defense stated in a 2014 report, "unmanned systems (air, maritime, and ground) continue to hold much promise for the warfighting tasks ahead."[253] According to a recent congressional report, "AI is not a wholly revolutionary idea to be applied to the military domain, and it is merely the next logical step in the digitization and

---

[249] Lara Seligman, *No, the Pentagon Is Not Working on Killer Robots — Yet*, FOREIGN POLICY (Feb. 13, 2019), https://foreignpolicy.com/2019/02/13/no-the-pentagon-is-not-working-on-killer-robots-yet/ (quoting Lt. Gen. Jack Shanahan, head of the Pentagon's Joint Artificial Intelligence Center) ("We are nowhere close to the full autonomy question that most people seem to leap to a conclusion on when they think about DoD and AI").

[250] *See* Bonnie Docherty, *We're Running Out of Time to Stop Killer Robot Weapons*, GUARDIAN (Apr. 11, 2018), https://www.theguardian.com/commentisfree/2018/apr/11/killer-robot-weapons-autonomous-ai-warfare-un ("Precursors have already been developed or deployed as autonomy has become increasingly common on the battlefield. Hi-tech military powers, including China, Israel, Russia, South Korea, the UK and the US, have invested heavily in the development of autonomous weapons."); *see generally* Perrigo, *supra* note 247.

[251] Perrigo, *supra* note 247.

[252] *See generally* Ingvild Bode & Hendrik Huelss, *Autonomous Weapons Systems and Changing Norms in International Relations*, 44 REV. INT'L STUDIES, 393 (2018).

[253] U.S. DEPT. DEFENSE, UNMANNED SYSTEMS INTEGRATED ROADMAP FY2013–2038, vii (Jan. 2014), https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf.

mechanization of the modern battlefield."[254] Against the fog of war, the amount of information now overwhelms the military's capacity to analyze and respond.[255] So AI provides a potential solution. Implicit in the choice is that to lift the fog of war, the military has to turn to the black box of AI.

Left out of most the discussion on military automation is the EU.[256] Although its citizens remain on the borders of the countries likely to be engaged in kinetic engagements and economic upheavals, only Britain appears to be actively pursuing the development of this technology.[257]

iii. Current Cybersecurity Regulations Do Not Address the Larger Cyber Picture

Against this context, current EU and U.S. regulations do not address these concerns. With their intended focus on consumer data privacy with private entities, the GDPR and new changes to U.S. law do not address the pressures fueling international cyberattacks, escalating cyber-espionage, military automation, and other trends such as the growth of autonomous

---

[254] CONG. RESEARCH SERV., R45392, U.S. GROUND FORCES ROBOTICS AND AUTONOMOUS SYSTEMS (RAS) AND ARTIFICIAL INTELLIGENCE (AI): CONSIDERATIONS FOR CONGRESS 1 (2018) (citing Adam Wunische, *AI Weapons Are Here to Stay*, NAT'L INTEREST (Aug. 5, 2018), https://nationalinterest.org/feature/ai-weapons-are-here-stay-27862)).

[255] *See* Dakota S. Rudesill, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the Laws of War*, 32 YALE J. INT'L L. 517, 536 (2007) ("[I]nformation overload is a problem in a way it never was before. . . . The torrent of data before commanders can crowd out the refined actionable intelligence that is the basis for not just reasonable decisions but right decisions.").

[256] *See e.g.*, Marc Champion, *Europe Wants a Robot Army to Challenge the U.S. and China on AI*, BLOOMBERG (Apr. 25, 2018), https://www.bloomberg.com/news/articles/2018-04-25/europe-wants-a-robot-army-to-challenge-the-u-s-and-china-on-ai (Europe "has no vast internet platforms on the scale of Google Inc. or China's Tencent Holdings Ltd. to hoover up the data that underlie many current technological advances in AI. Worse, those American and Chinese tech giants have deep pockets, allowing them not only to fund expensive research, but also to scoop up successful European startups."); *see also* Bruno Macaes, *Europe's AI delusion, Brussels is Failing to Grasp Threats and Opportunities of Artificial Intelligence*, POLITICO (Mar. 19, 2018), https://www.politico.eu/article/opinion-europes-ai-delusion/ (noting that the European Union's current AI strategy draft reflects the failure to recognize the technology's significance).

[257] *See* Jamie Doward, *Britain Funds Research Into Drones That Decide Who They Kill, Says Report*, GUARDIAN (Nov. 10, 2018), https://www.theguardian.com/world/2018/nov/10/autonomous-drones-that-decide-who-they-kill-britain-funds-research (noting the UK Ministry of Defense's alleged interest in building autonomous lethal drones, in the context that the UK has refused to support UN proposals to ban them).

technologies, IoT devices, and the ever-increasing reliance on AI technologies embedded in consumer and commercial technologies. In order to dissipate fears of cyber warfare—and reduce the impact of cyber espionage on economies—more regulation, with a focus beyond consumer privacy, is imperative.

VI. CONCLUSION

The road to hell is paved with good intentions; specifically, policymakers focus on privacy concerns, rather than broader vulnerabilities in cyberspace.

After decades struggling to tame cyberspace, 2018 became the year that the EU put its muscular GDPR privacy regime into effect, grabbing extraterritorial authority over the FAAMG multinational corporations that dominate global economics and communications. U.S. states such as California have followed suit with a range of regulations attempting to reduce the impact these companies have on the lives of the public.

Despite this, other nation states have maintained their ability to exploit new cyber technologies, causing damage to businesses, economies, governments, and citizens. Time will tell whether these consumer privacy-oriented laws actually change behaviors in online environments for the benefit of the public or merely add a layer of protectionism for Europe and its local industries.

None of these policies focus on the growing role of AI, IoT devices, and autonomous machines, or on the potential weaponization of these devices. In each sphere, however, the reaction has been the same. The role of the state has reemerged to fight its disintermediation triggered by these data-infused technologies.

The Empires are striking back. Unfortunately, they aren't addressing the gravest threats.

PAYOLA 3.0? THE RISE OF INTERNET "PLAYOLA"

Elizabeth Levin*

The terrestrial radio payola (or "pay-to-play") scandal resulted in regulations, lawsuits, and millions of dollars in settlements. In light of the move away from terrestrial radio and toward Internet radio and streaming services, the payola era may seem irrelevant to modern-day practices. This view, however, is mistaken. Payola has reappeared in a new form: Spotify.

Spotify, the world's most well-known music-streaming platform, has stated publicly that it does not accept payment for placement on its most popular playlists. But rumors of this practice have begun to surface, as have explicit agreements to pay for placement on popular playlists created by individuals—placement on which significantly increases an artist's chances on appearing on Spotify's own major playlists. Appearance on a Spotify-created playlist is the most direct path to higher streaming revenue, so payment for placement may significantly affect artists' potential for success. Regulators who observe this practice on Spotify may take lessons from the payola scandal of the past and respond through regulation limiting the practice. However, regulation may not be the best answer for Internet payola, specifically in light of arguments against anti-payola regulation more broadly and its applicability or likely effectiveness given the unique nature of the Internet.

*Yale Law School, J.D. Candidate 2020. I am deeply grateful to Jacqueline Charlesworth and Lisa Alter for their feedback and for teaching the course that inspired the topic of this paper, as well as to the editors of the *Journal of Law and Technology at Texas* for their meticulous editing. All views and errors expressed in this piece are my own.

TABLE OF CONTENTS

I. INTRODUCTION

It appears that an old problem has arisen in new form: payola, the practice of an artist paying for airtime without the radio station disclosing this payment, may have appeared in online streaming services. While Spotify has publicly stated that it is against accepting payment in exchange for placement on playlists, rumors have surfaced that record labels can and have bought spots on Spotify playlists.[1] Further, some user-created playlists, placement on which can impact whether a song is added to an in-house playlist, have begun offering placement for payment.[2] If this practice of accepting payment for playlist placement—nicknamed "playola"—is a form of payola, regulation against it may be justified for the same reasons as for terrestrial radio payola, particularly given the concern that payola practices lead to a decline in music quality. On the other hand, several factors counsel against such regulation, including arguments against anti-payola regulation in terrestrial radio, the distinguishing characteristics of the Internet, and uncertainty over whether the FCC would have the authority to administer anti-playola regulation in light of its position on Internet regulation more broadly.

II. THE RISE OF INTERNET MUSIC SERVICES

a. Types of Internet Music Services

Internet music services have become primary players in the music-listening industry. Internet music providers take two primary forms: music-streaming platforms, like Spotify and Apple Music, and webcasting services, like Pandora and iHeartRadio. The market for Internet music services is fairly concentrated: a study by MusicWatch found that Spotify and Apple Music are the dominant players, with north of 20 million subscribers each; Pandora, at over 6 million subscribers, comes next; the remaining 5 million

---

[1] Louis Aguiar & Joel Waldfogel, *Platforms, Promotion, and Product Discovery: Evidence from Spotify Playlists* (JRC Digital Economy Working Paper 2018-04), JOINT RESEARCH CTR., EUROPEAN COMM'N 7, https://www.tse-fr.eu/sites/default/files/TSE/documents/ChaireJJL/Digital-Economics-Conference/Conference/aguiar_luis.pdf.

[2] Glen Peoples, *How 'Playola' is Infiltrating Streaming Services: Pay for Play is Definitely Happening*, BILLBOARD (Aug. 19, 2015), https://www.billboard.com/articles/business/6670475/playola-promotion-streaming-services.

subscribers (10% of the total subscriber base) are divided between Google, YouTube, Amazon Music, and iHeartRadio.[3]

Music-streaming platforms are interactive, allowing users to listen to songs within that platform's collection on demand. Most also provide users with curated playlists meant to appeal to each user's individual tastes, as well as access to themed playlists created for a broader audience.[4] Webcasting services are non-interactive, creating Internet radio broadcasts through a mix of algorithmic and human curation.[5] While webcasting services like Pandora can operate under a statutory license in accordance with 17 U.S.C. § 144,[6] streaming services like Spotify have to strike deals with labels and publishers to license their music for legal use.[7]

Internet radio and streaming services have been consistently growing in popularity since they hit the music-listening market.[8] Even as the music industry as a whole has faced declining revenues, digital streaming and digital sales have continued to grow.[9] The number of Internet music listeners paying for monthly subscriptions for music-streaming services nearly doubled from 2016 to 2018, hitting an estimated 51 million.[10] While this still stands in stark contrast to the number of users streaming music for free, whether on the free tier of Spotify, on YouTube, or by sharing

---

[3] Cherie Hu, *Paid Music Streaming Subscribers Surpass 50 Million in US, But There's a Twist: Exclusive*, BILLBOARD (Sept. 11, 2018), https://www.billboard.com/articles/business/8474560/paid-music-streaming-subscribers-surpass-50-million-us-exclusive.

[4] *What is Spotify and How Does it Work?*, TECHBOOMERS (Nov. 8, 2016, 12:14 PM), https://techboomers.com/what-is-spotify.

[5] Glenton Davis, *When Copyright is Not Enough: Deconstructing Why, as the Modern Music Industry Takes, Musicians Continue to Make*, 16 CHI.-KENT J. INTELL. PROP. 373, 380 (2017).

[6] *Id*. at 380 n. 46.

[7] Zack O'Malley Greenburg, *Revenge of the Record Labels: How the Majors Renewed Their Grip on Music*, FORBES (Apr. 15, 2015), https://www.forbes.com/sites/zackomalleygreenburg/2015/04/15/revenge-of-the-record-labels-how-the-majors-renewed-their-grip-on-music/#2b8b2c42fba7.

[8] Davis, *supra* note 5; *2017 Year-End Music Report*, NIELSEN 2 (2017), https://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2018-reports/2017-year-end-music-report-us.pdf ("The surge in streaming continued throughout 2017, topping all forms of music consumption.").

[9] Nikelle Murphy, *Why Streaming Is the Future of the Music Industry, Not Its End*, CHEATSHEET (Aug. 26, 2015), https://www.cheatsheet.com/entertainment/music/why-streaming-is-the-future-of-the-music-industry-not-its-end.html/.

[10] Hu, *supra* note 3.

subscriptions,[11] developments in online music platforms' technological capabilities have encouraged users to switch over to paid subscriptions, despite having these free alternatives.[12] With the growing user base, revenues have risen as well.[13]

b. Spotify and the Streaming Economy

Digital music streaming has essentially become an independent economy. The proportion of U.S-recorded music revenues from streaming has steadily increased.[14] Rather than offering digital music downloads, streaming services provide users with various subscription options.[15] Generally, some amount of content is available for free, and users can pay a monthly price to access things like the ability to play any song on demand, certain playlists curated to their tastes, and more.[16] Although most Spotify users elect not to pay for a premium subscription, most of Spotify's revenue comes from this service.[17] Other than access to music, the main benefit that Spotify provides to its listeners is personalization—curating

---

[11] *Id.*

[12] Davis, *supra* note 5, at 374.

[13] Spotify has been reporting modest growth for its streaming business, but is struggling in public markets as investors have been skeptical about its ability to sustain growth long-term and become profitable. *See* Sarah Perez, *Spotify Plans to Buy Up to $1 Billion in Stock*, TECHCRUNCH (Nov. 5, 2018), https://techcrunch.com/2018/11/05/spotify-plans-to-buy-back-up-to-1-billion-in-stock/; *see also, Spotify Expects its 2018 Revenue to Grow 20% to 30%, Slower than Last Year's Pace*, CNBC (Mar. 26, 2018), https://www.cnbc.com/2018/03/26/spotify-expects-its-2018-revenue-to-grow-20-percent-to-30-percent-slower-than-last-years-pace.html (noting the decline in Spotify's revenue growth from 2017 to 2018).

[14] U.S. COPYRIGHT OFFICE, *Copyright and the Music Marketplace* 71 (Feb. 2015) [hereinafter Music Licensing Study], https://www.copyright.gov/policy/musiclicensingstudy/copyright-and-the-music-marketplace.pdf; *see also* Dani Deahl, *The Verge 2018 Tech Report Card: Streaming Music* (Dec. 31, 2018), https://www.theverge.com/2018/12/31/18156503/2018-tech-recap-streaming-music-spotify-apple-soundcloud-tidal (stating that the proportion of revenue in the music industry from streaming services has increased from 62 percent in 2017, to 75 percent in 2018).

[15] Hu, *supra* note 3.

[16] *Id.*

[17] Kerry Flynn, *Spotify Plans to Add Interest-Based Targeting to Its Self-Serve Platform*, DIGIDAY (Feb. 1, 2019), https://digiday.com/marketing/spotify-plans-add-interest-based-targeting-self-serve-platform/ (describing how Spotify's 2018 third-quarter earnings report reflected that only "10.5 percent of [its] revenue is from ads").

recommendations meant to help listeners discover music they like.[18] The two primary forms of personalization are personalized music suggestions, and more general playlists from which a user can choose.[19] An example of a music suggestion is Spotify's Discover Weekly playlist.[20] The general playlists, like Spotify's Today's Top Hits and New Music Friday, provide particular types of music in an accessible form.[21]

Spotify's "in-house" playlists are either curated by Spotify employees or created algorithmically.[22] Some of its most popular playlists are created by employees, who frequently focus on songs and artists that are already widely known.[23] Generally, Spotify "tests" songs by including them on playlists with smaller followings before adding them to the major global lists.[24] Appearing on a Spotify in-house playlist has serious implications for revenue; it results both in more revenue through Spotify's pay-per-play payment system and more listeners and subscribers for the artist.[25] As such, Spotify can determine which songs and artists are discovered in the first place.[26] Although there are an estimated 2 billion playlists on Spotify,[27] the company's in-house playlists "have over three quarters of the followers of the top 1,000 playlists," and its "algorithmic lists have another 9.3 percent."[28]

Although being placed on a playlist does not necessarily guarantee that a song will be played, it has an empirical effect. A study by authors for the European Commission analyzed what happens to a song's streams when

---

[18] Aguiar & Waldfogel, *supra* note 1, at 2.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* at 5.

[24] *See* David Pierce, *The Secret Hit-Making Power of the Spotify Playlist*, WIRED (May 3, 2017, 7:30 PM), https://www.wired.com/2017/05/secret-hit-making-power-spotify-playlist/.

[25] Aguiar & Waldfogel, *supra* note 1, at 3–4; *see also* Steven Bertoni, *How Spotify Made Lorde a Pop Superstar*, FORBES (Nov. 26, 2013, 4:46 AM), https://www.forbes.com/sites/stevenbertoni/2013/11/26/how-spotify-made-lorde-a-pop-superstar/.

[26] Aguiar & Waldfogel, *supra* note 1, at 3.

[27] *See* Craig Smith, *72 Amazing Spotify Stats and Facts (December 2018)*, DMR (Dec. 17, 2018), https://expandedramblings.com/index.php/spotify-statistics/.

[28] Aguiar & Waldfogel, *supra* note 1, at 3–4.

it appears on Spotify's most popular playlists.[29] To illustrate the effect of inclusion in one of these in-house playlists, when country singer Kane Brown's song "What Ifs" appeared on "Today's Top Hits," its daily stream count rose from about 200,000 times a day to nearly 500,000,[30] and his followers rose from 11.6 million to 29.2 million.[31] Once it was removed from the playlist, his number of followers dropped from 30.8 million to just 10.8 million, and declined for months thereafter.[32] The authors of the study concluded that getting on Today's Top Hits is worth almost 20 million additional streams, which translates to between $116,000 and $163,000 in revenue from Spotify alone.[33]

For most artists who do not make it to a Spotify-curated playlist, the primary criticism of Spotify—and of music-streaming services more generally—is that its underpays artists.[34] Critics argue that music-streaming revenue cannot outweigh the shift away from purchasing physical units and downloads, even considering an overall increase in performance royalties.[35] Even for the most widely played songs, the musician would likely earn more through the sale of a digital download or sale of merchandise than what the artist would get from the online streams.[36] The decline in payment to artists

---

[29] *See* Neil Shah, *Spotify Uproar Points to the Power of the Playlist*, WALL ST. J. (Jun. 6, 2018, 01:43 PM), https://www.wsj.com/articles/spotify-disputes-point-to-the-power-of-the-playlist-1528307004 (this included Today's Top Hits, which had over 20 million followers, RapCaviar, with 9.7 million followers, and New Music Friday, with 2.7 million followers).

[30] *Id.*

[31] Aguiar & Waldfogel, *supra* note 1, at 10.

[32] *Id.* at 13.

[33] *Id.* at 27.

[34] *See* Davis, *supra* note 5, at 374 ("[A] spokesman for Spotify confirmed that the company pays 'between $0.006 and $0.0084' in royalties to an artist each time a user streams a work by that artist. . . . [T]o the independent artist, this wage . . . is not livable."); Music Licensing Study, *supra* note 14, at 73–74; Victor Luckerson, *Is Spotify's Model Wiping Out Music's Middle Class?*, RINGER (Jan. 16, 2019, 5:30 AM), https://www.theringer.com/tech/2019/1/16/18184314/spotify-music-streaming-service-royalty-payout-model ("The fact that Spotify and other streaming services offer paltry payouts to artists is widely known . . . .").

[35] Davis, *supra* note 5, at 380–81; Music Licensing Study *supra* note 14, at 74.

[36] *See* Jessica Michelle Ciminero, *Technology, the Internet and the Evolution of Webcasters – Friends or Foes of Musicians and Their IP*, 5 BERKELEY J. ENT. & SPORTS L. 16, 30 (2016) ("[A]nd even for the most widely played songs the musician would likely earn more through the sale of a digital download."); *see also* Maya Kosoff, *Pharell Made Only $2,700 In Songwriter Royalties From 43 Million Plays of 'Happy' On Pandora*, BUS.

can likely be attributed to the pay-per-play model, as the amount actually spent by consumers has generally stayed flat, but with a different mix of digital downloads, streaming services, and physical copies.[37] Streaming companies are resisting royalty rate hikes, concerned with the damage that over-paying royalties could cause to the business.[38] Viewed as a percentage of revenue, "royalty obligations vary from about five percent of revenue (for traditional radio) to about seventy percent of revenue (for on-demand streaming)" due to rate-setting in copyright law.[39] Although Spotify's paid-subscription consumer base has grown over the years, as of 2017 Spotify still had an operating loss of $421.3 million.[40] Digital music services also contend that the blame for underpayment of artists may lie with intermediaries such as record labels, music publishers, and performance rights organizations, rather than the services themselves.[41]

Another major concern with streaming services is the potential for fraud within the pay-per-play model.[42] Streaming services uniquely allow individual consumers "to shape the revenue stream of a creator purely by

---

INSIDER (Dec. 23, 2014, 10:12 AM), https://www.businessinsider.com/pharrell-made-only-2700-in-songwriter-royalties-from-43-million-plays-of-happy-on-pandora-2014-12; David Lowery, *My Song Got Played On Pandora 1 Million Times and All I Got Was $16.89, Less Than What I Make From a Single T-Shirt Sale!*, TRICHORDIST (June 24, 2013), http://thetrichordist. com/2013/06/24; Doug Gross, *Songwriters: Spotify Doesn't Pay Off . . . Unless You're a Taylor Swift*, CNN (Nov. 13, 2014), http://www.cnn.com/2014/11/12 /tech/web/spotify-pay-musicians (noting that the songwriters of the Bon Jovi hit "Livin' on a Prayer" split $110 in royalties from Pandora for 6.5 million plays of that song).

[37] Peter Kafka, *The Music Business's Song Is on Repeat: Streaming Is Up, Sales Are Flat*, RECODE (Sep. 21, 2015, 2:00 PM), https://www.recode.net/2015/9/21/11618774/the-music-businesss-song-is-on-repeat-streaming-is-up-sales-are-flat.

[38] Mark Hogan, *A Guide to the Royalties Battle Between Streaming Services and Songwriters*, PITCHFORK (Mar. 12, 2019), https://pitchfork.com/thepitch/a-guide-to-the-royalties-battle-between-streaming-services-and-songwriters/.

[39] Peter DiCola, *Copyright Equality: Free Speech, Efficiency, and Regulatory Parity in Distribution*, 93 B.U. L. REV. 1837, 1839 (2013); *see* Glenn Peoples, *Pandora Revenue Up 40 Percent, Listening Growth Softens,* BILLBOARD (Oct. 23, 2014), https://www.billboard.com/articles/6296384/pandora-revenue-up-40-percent-listening-growth-softens.

[40] *See* Ed Christman, *Spotify's Losses More Than Double to $581M, Revenues Rise to $3B*, BILLBOARD (Jun. 15, 2017), https://www.billboard.com/articles/business/7833686/spotify-2016-losses-financial-results-revenue/ ("Spotify actually hides how much they pay out to content owners.").

[41] Music Licensing Study, *supra* note 14, at 77.

[42] *See* Joseph Dimont, Note, *Royalty Inequity: Why Music Streaming Services Should Switch to a Per-Subscriber Model*, 69 HASTINGS L.J. 675, 700 (2018) (noting the ability "for some to rig the system using click-fraud techniques . . . .").

consuming more of their work without any additional expense";[43] in other words, creations are now rewarded by mass appeal.[44] Because the number of plays is what matters, the system can be rigged through click-fraud and "fan activism," where hackers or actual listeners can increase the number of plays they give a song or artists for the explicit purpose of increasing their revenues.[45] With music-streaming services increasingly being seen as "the new radio," their impact on revenue is important.[46] If the only way for an artist to earn a sustainable living on Spotify is to appear on a Spotify-curated playlist,[47] then the potential for fraud or unfair practices becomes even more significant.

III. PAYOLA ON TERRESTRIAL RADIO

The term "payola" was originally used by *Variety* magazine in 1938.[48] Payola is the practice of accepting or receiving money or other valuable consideration "for the inclusion of material in a broadcast *without* disclosing that fact to the audience."[49] Payola "represents a 'pay-to-play' formula in which recording industry representatives, in basic quid pro quo

---

[43] *Id.*

[44] Luckerson, *supra* note 34.

[45] Dimont, *supra* note 42, at 688–89; *see also* Jonathan Griffin, *The Mystery Tracks Being 'Forced' on Spotify Users*, BBC (Jan. 25, 2019), https://www.bbc.com/news/blogs-trending-46898211 (describing possible hack of Spotify, resulting in fake bands appearing in users' playlists); Chris Welch, *Spotify Removes Silent Album that Earned Indie Band $20,000*, VERGE (May 7, 2014, 10:25 AM), https://www.theverge.com/2014/5/7/5690590/spotify-removes-silent-album-that-earned-indie-band-20000 (describing how a Michigan-based band earned $20,000 in Spotify royalties through a completely silent album, which they encouraged fans to stream continuously at night while they slept). Recently, and concerningly, forms of fraud that extend beyond fraudulent plays for profit have begun to crop up as well. *See* Amy X. Wang, *Why Fake Beyoncé Albums on Spotify and Apple Music Highlights Streaming's Wider Licensing Troubles*, MUSIC BUSINESSS WORLDWIDE (Jan. 10, 2019), https://www.musicbusinessworldwide.com/why-fake-beyonce-music-on-spotify-and-apple-music-highlights-streamings-wider-licensing-troubles/ (describing unauthorized leaks of Beyoncé and SZA demos).

[46] *See* Shah, *supra* note 29.

[47] *See* Luckerson, *supra* note 34 ("In the current streaming economy, the only way to survive is to be huge.").

[48] Douglas Abell, *Pay-for-Play: An Old Tactic in a New Environment*, 2 VAND. J. ENT. L. & PRAC. 52, 53 (2000) (citing Kerry Segrave, PAYOLA IN THE MUSIC INDUSTRY: A HISTORY, 1880–1991, at 1 (1994)).

[49] Charles W. Logan, Jr., *Getting Beyond Scarcity: A New Paradigm for Assessing the Constitutionality of Broadcast Regulation*, 85 CAL. L. REV. 1687, 1696 n. 47 (1997).

fashion," pay for airtime of songs by an artist whom they represent.[50] Radio stations have four primary motivations for engaging in pay-for-play practices: first, the scarcity of airtime (due to the limited nature of the radio spectrum) increases its value; second, breaking new hits is risky but necessary for success in the radio industry; third, individuals from record labels often have existing relationships with radio stations that they can leverage for the benefit of new artists; lastly, even controlling for tracks that are likely to be unpopular, radio stations always have more tracks than time slots available.[51] However, the on-air *disclosure* of pay-to-play has a cost, as it interrupts programs with announcements and may give the impression that the stations are not independent in their programming choices.[52]

The terrestrial radio "payola" scandal first hit in the 1950s.[53] Attempts to ban payola before 1945 were meant to restrict competition.[54] The 1950s scandal, in contrast, emerged as a response to the growing popularity of rock 'n' roll, which accelerated in popularity in part because of payola paid by small record labels to DJs.[55] In the late 1950s, payola became subject to FTC, FCC, and congressional investigations.[56] This resulted in Congress amending the Federal Communications Act of 1934—specifically, sections 317 and 507—to require disclosure of purchased airtime, subject to penalties under section 508.[57] Section 317 requires broadcasters to disclose any consideration received for airing certain material (such as songs)

---

[50] Clay Calvert, *Payola, Pundits, and Press: Weighing the Pros and Cons of FCC Regulation*, 13 COMMLAW CONSPECTUS 245, 246 (2005).

[51] Patryk Galuszka, *Undisclosed Payments to Promote Records on the Radio: An Economic Analysis of Anti-Payola Legislation*, 11 VA. SPORTS & ENT. L.J. 38, 47–48 (2011).

[52] *See id.* at 48.

[53] Ronald Coase, *Payola in Radio and Television Broadcasting*, 22 J.L. & ECON. 269, 287 (1979). Some have estimated that payola practices in the music industry has existed since as early as the 1890s. *See id.* at 272; *see also* Galuszka, *supra* note 51, at 49. The 1950s scandal, however, was the first time that the practice was publicly brought to light and made subject to regulation as a result.

[54] *See* Coase, *supra* note 42, at 316.

[55] *See id.* at 312.

[56] *Id.* at 287. Major record companies pushed for the investigation, arguing to Congress that rock 'n' roll was immoral music spreading through immoral business practices. Galuszka, *supra* note 50, at 51.

[57] J. Gregory Sidak & David E. Kronemyer, *The "New Payola" and the American Record Industry: Transactions Costs and Precautionary Ignorance in Contracts for Illicit Services*, 10 HARV. J. L. & PUB POL'Y 521, 522 (1987); Robin Cartwright, *What's the Story on the Radio Payola Scandal of the 1950s?*, STRAIGHT DOPE (Aug. 31, 2004), http://www.terryewell.com/m355/Docs/Payola_Radio.pdf.

when it is broadcasted.[58] Section 507 requires disclosure of any promise of consideration before the broadcast of that material.[59]

Following the congressional payola investigations and 1960 amendments, labels hoping to continue engaging in payola but evade punishment turned to a new solution: independent record promoters, or "indies."[60] The so-called "independent promoters loophole" stemmed from an FCC administrative ruling in 1979 specifying that "social exchanges between friends are not 'payola.'"[61] As a result of this ruling, prosecuting payola violations––particularly those effected through interactions between independent promoters and radio stations—became more difficult.[62] Throughout the 1980s, labels could pay a third party or independent record promoter, who would then go "promote" their songs to radio stations.[63] The independent promoters were able to get the songs that their clients (the record companies) wanted on the radio, by offering radio stations "promotion budgets,"[64] which included "cocaine, prostitutes, and hundreds of thousands of dollars."[65]

Independent promoters acted as brokers for hit singles, providing radio stations with information about the "quality and nature of the recording, its likely demographic appeal, its advertising support, sales performance and, ultimately, the likelihood of its public acceptance as a 'hit

---

[58] Communications Act of 1934 § 317, 47 U.S.C. § 317 (2017); 47 C.F.R. § 73.1212 (2018).

[59] Communications Act of 1934 § 507, 47 U.S.C. § 508 (2017).

[60] Lauren J. Katunich, Comment, *Time to Quit Paying the Payola Piper: Why Music Industry Abuse Demands a Complete System Overhaul*, 22 LOY. L.A. ENT. L. REV. 643, 656 (2002).

[61] In re Applications of Kaye Smith Enter., 71 F.C.C.2d 1402, 1408 (1979).

[62] Galuszka, *supra* note 51, at 52 ("[I]t would be difficult to prove that gifts given to a radio station employee from an independent promoter were something more than a 'social exchange between friends.'").

[63] *See* Rachel M. Stilwell, Note, *Which Public - Whose Interest - How the FCC's Deregulation of Radio Station Ownership Has Harmed the Public Interest, and How We Can Escape from the Swamp*, 26 LOY. L.A. ENT. L. REV. 369, 419–28 (2006).

[64] *See* Galuszka, *supra* note 51, at 64 ("'[P]romotional budgets' were meant to help increase radio stations' audiences . . . . The promoter would charge a record label a small weekly fee and would be paid bonus fees depending on how successful the label's records were . . . ."); Katunich, *supra* note 60, at 658 ("The promotional budget supplied by the indie, supposedly used by the radio station to buy T-shirts, billboard ads, and station vans, is in reality spent by the station in any manner that it sees fit.").

[65] Abell, *supra* note 48, at 53.

record.'"[66] Since the independent intermediaries were the ones paying the stations, it was thought that their inducements did not fall under the "payola" rules and did not need to be reported. In other words, it was thought that "[b]ecause radio stations are one step removed from record-label money, these payments are not technically payola."[67] These promotional payments were not tied directly to the purchase of airtime for any particular song.[68] Instead, the payments resulted in the song being added to the station's "playlist," essentially putting it into the station's rotation but leaving it up to the station's programmers to decide how often it was played.[69] These features made the use of independent promoters a way, at least in the view of record labels, of circumventing payola regulations.[70] On February 24, 1986, the *NBC Nightly News* reported, in a story titled "The New Payola," on investigations on the "re-emergence of payola at rock music radio stations" through the use of independent promoters.[71] These investigations, however, only temporarily derailed the use of payola.[72]

The practice of "independent promoter payola" was rarely addressed until New York Attorney General Eliot Spitzer initiated an investigation into the promotion of music to radio stations in 2005.[73] In its summary of the results of the investigation, the New York Attorney General's office described Sony BMG's practice of obtaining airtime for its songs "through both direct deals between high-level Sony and radio executives, and indirect payments made via independent promoters."[74] In a 2005 settlement, Sony BMG agreed to "pay $10 million and stop giving payments and awarding

---

[66] Sidak & Kronemyer, *supra* note 57, at 529 (quoting Complaint in Isgro v. Recording Indus. Ass'n of Am. at 6-7, No. 86-2740 (C.D. Cal. filed Apr. 30, 1986)).

[67] Katunich, *supra* note 60, at 656.

[68] *Id.* at 658.

[69] *Id.*

[70] Devin Kosar, Note, *Payola—Can Pay-to-Play Be Practically Enforced*, 23 ST. JOHN'S J. LEGAL COMMENT. 211, 223 (2008).

[71] Sidak & Kronemyer, *supra* note 57, at 556–57.

[72] *See* Galuszka, supra note 51, at 64 ("After the 1986 ban on independent promotion, the major record labels resumed using promoters' services."); *see also* Sidak & Kronemyer, *supra* note 57, at 559–60 ("By early 1987, the 'new payola' scandal had faded, Senator Gore's investigation reportedly having uncovered no evidence of wrongdoing.").

[73] Kristen Lee Repyneck, Note, *The Ghost of Alan Freed: An Analysis of the Merit and Purpose of Anti-Payola Laws in Today's Music Industry*, 51 VILL. L. REV. 695, 717–18 (2006); *see* Katunich, *supra* note 60, at 651–52 (2002).

[74] Repyneck, *supra* note 73, at 718.

expensive gifts" to radio programmers in exchange for airplay.[75] Spitzer's investigation resulted in fines of more than $36 million against Universal Music, Warner, EMI, and Sony BMG.[76] The FCC then conducted a nationwide payola investigation.[77] The investigation culminated in a consent decree and a $12.5 million settlement with the four record companies.[78] The FCC's fine was seen by some as merely a "slap on the wrist,"[79] and even after these settlements, payola continued in new forms.[80] Instead of direct payments, record labels moved to providing "incentives such as free concerts, paid vacations, bulk advertising purchases and more."[81]

The rise of payola was consequential: "For record labels, radio is the most powerful promotional tool to sell albums."[82] In the music climate of the 1950s, record-industry moguls realized that teenagers (the primary economic force in the music market at the time) "had cash, loved rock 'n' roll, listened to the radio, and were easily stampeded into buying hit records by popular deejays."[83] The practice of payola rose in popularity simply because of its efficiency: while major labels ignored rock 'n' roll, smaller labels were able to pay radio stations for a chance to get their artists' music on the air.[84] Eventually, the major labels caught on; record executives believed that independent promoters who had financial arrangements with radio stations

---

[75] Marc Fisher, *Paying for Airplay: The Beat Goes On*, WASH. POST (Aug. 7, 2005), https://www.washingtonpost.com/archive/lifestyle/style/2005/08/07/paying-for-airplay-the-beat-goes-on/eec6fc24-9cb8-4b73-bbd6-2fbbfaa989b8/?utm_term=.d6cea1d3a86e; Press Release, Attorney General of the State of New York, Sony BMG NY Settlement: In the Matter of Sony BMG Music Entertainment (July 22, 2005), https://ag.ny.gov/press-release/sony-settles-payola-investigation.

[76] Kosar, *supra* note 70, at 236; *see also* Michael Gormley, *Warner Music Settles in Probe into 'Payola'*, MAIL & GUARDIAN (Nov. 23, 2005), https://mg.co.za/article/2005-11-23-warner-music-settles-in-probe-into-payola.

[77] Kosar, *supra* note 70, at 213. Kosar notes that this investigation failed to be "legitimate and thorough," especially in light of the evidence provided to the FCC by Attorney General Spitzer. *Id*. at 213 n.9. The FCC's consent decree levied less than half the fines that New York State had issued to the same record labels. *Id.*

[78] Kosar, *supra* note 70, at 213.

[79] *Id.*

[80] *See* Krystal Conway, Comment, *The Long Road to Desuetude for Payola Laws: Recognizing the Inevitable Commodification of Tastemaking*, 16 SETON HALL J. SPORTS & ENT. L. 343, 369–70 (2006).

[81] *Id*. at 372.

[82] Abell, *supra* note 48, at 53.

[83] *See* Cartwright, *supra* note 57.

[84] *See* Galuszka, *supra* note 51, at 50.

had the power to influence a song's success, by either getting them on or keeping them off the air.[85] As a result of this practice, labels that lacked the resources to pay such fees were unable to generate hit records; small record labels without such resources could barely get their records played.[86]

IV. SPOTIFY AND THE RISE OF "PLAYOLA"

Spotify's official stance is that it does not allow the exchange of cash or other payment for a space on its playlists.[87] However, it is rumored that major labels are able to purchase placement on Spotify's in-house playlists.[88] Additionally, a process has developed that is analogous to the "independent promoters loophole" of years past. While Spotify does not directly engage in payola, the way its playlists are created depends on an algorithm that takes into account the existing popularity of a song, including its placement on other playlists, particularly ones with large listener and subscriber bases.[89] This has resulted in the commodification of certain user-generated playlists; if a user-generated playlist has enough popularity, certain artists are willing to pay for a spot on that playlist. Being added to a popular playlist will not only result in an increased listener base through the followers of that playlists, but will also increase the artist's chances of being located on a Spotify-generated playlist. Because of this impact, a market for playlist placement has developed.

While Spotify has publicly stated that it does not engage in payola, the market for playlist inclusion has given rise to new forms of payola unique to the music-streaming market, nicknamed "playola."[90] Streaming services have adopted "playola" in two primary forms. The first stems from the three major record labels' (Universal Music Group, Sony Music, and Warner Music Group) control of spots on many of the largest Spotify playlists.[91] This is concerning in light of the relationship between Spotify and the major labels. For these labels, the rise of streaming services like

---

[85] Stilwell, *supra* note 63, at 421.

[86] *Id.*

[87] Robert Cookson, *Spotify Bans 'Payola' on Playlists*, FIN. TIMES (Aug. 20, 2015), https://www.ft.com/content/af1728ca-4740-11e5-af2f-4d6e0e5eda22.

[88] Peoples, *supra* note 2.

[89] *See* Aguiar & Waldfogel, *supra* note 1, at 5; *Spotify Artists FAQ,* SPOTIFY (last visited Mar. 30, 2019), https://artists.spotify.com/faq/promotion ("The more streams and followers you have, the higher up you'll appear in searches.").

[90] *See* Peoples, *supra* note 2.

[91] *Id.*

Spotify destroyed a portion of old revenue sources—namely, the sale of physical recorded music—but opened new ones, particularly through the large licensing scheme that online-streaming services require.[92] In exchange for stakes in online music services, record labels have been giving music startups access to the artists and their songs; the artists derive minimal royalties, while the record labels hold the ownership.[93] Notably, the three major labels own nearly 20% of Spotify.[94] These three labels' ownership in digital music startups overall is estimated at about $3 billion.[95]

In spite of Spotify's public statements denouncing the sale of playlists or of inclusion on playlists, these transactions appear to be taking place behind the scenes, as one major label marketing executive has stated that "popular playlists can and have been bought."[96] This practice has given rise to fear that streaming playlists will become like the radio playlists of the payola era, accepting compensation to influence content rather than operating free of financial incentive.[97] Further, the three major labels have their own playlists, controlling between 0.9 and 3.1% of the top 1,000 playlists' cumulative followers.[98] The success of these playlists makes it even more likely that Spotify will choose one of the labels' songs to add to a Spotify playlist, and makes behind-the-scenes payment for playlist placement easier to pass off as legitimate decision-making based on established popularity.

The second form of "playola" involves promotional-streaming companies that promise Spotify plays by securing song placements in highly followed playlists that influencers unaffiliated with Spotify curate.[99] Spotify does not explicitly allow "pay-for-play" behavior,[100] and has expressed a commitment to independent artists, such as through its creation of a

---

92 Davis, *supra* note 5, at 394.

93 O'Malley Greenburg, *supra* note 7.

94 Davis, *supra* note 5, at 394 n.144. Specifically, Sony BMG owns 5.8%, Universal owns 4.8%, Warner Music owns 3.8%, and EMI has 1.9%. Aguiar & Waldfogel, *supra* note 1, at 3.

95 O'Malley Greenburg, *supra* note 7.

96 Peoples, *supra* note 2.

97 *Id*.

98 Aguiar & Waldfogel, *supra* note 1, at 8.

99 Jessica French, *This Is How You Get Added to Spotify's Curated Playlists*, MEDIUM (Mar. 8, 2018), https://medium.com/@jessicafrech/this-is-how-you-get-added-to-spotifys-curated-playlists-7f01f2f6b891.

100 Cookson, *supra* note 87.

"Spotify for Artists" tool, allowing new artists to submit songs for consideration to be included in Spotify-created playlists.[101] On Spotify's FAQ, it specifically states that artists cannot pay to get on one of the 4,500 in-house playlists, though they can now upload unreleased tracks for consideration.[102] However, for most artists listed on Spotify, whether they appear on a Spotify-created playlist depends on their number of followers: "the more followers you have, the more playlists you'll be on."[103] This creates an incentive to appear on a highly subscribed playlist if possible, including by paying for placement. Spotify does not limit independent influencers' ability to sell placement on their playlists.

The top three promotional-streaming companies are owned by major labels. Generally, "major label artists get direct access to these services" owned by their labels, while indie artists have to "pay an average of $2,500 per song to be pitched and placed into influencer playlists."[104] From the perspective of curators, pitching services are a way to monetize their playlist-making hobby.[105] One source described indie musician Ari Herstand's experiences with these services. After receiving three offers for Spotify visibility—$500 for 50,000 to 100,000 plays; a four-month plugging campaign for $5,000; or 50,000 streams for $150—Ari went with the third, and his songs were quickly added to a user-generated playlist on Spotify with around 50,000 followers.[106] The playlist plugging service he used, "Streamify, had likely used click farms to generate plays," leading to Herstand's album being removed from the platform.[107]

Because the number of views and plays a song or artist gets increases its likelihood of being featured on a Spotify-curated playlist, this practice has serious implications. Fraudulent transactions are difficult for

---

[101] SPOTIFY, *supra* note 89.

[102] *Id.*; Aric Jenkins, *The Murky Business of Spotify 'Playlist Pitching'*, FORTUNE (Aug. 10, 2018), http://fortune.com/2018/08/10/spotify-playlist-pitching-curators/.

[103] SPOTIFY, *supra* note 89.

[104] French, *supra* note 99 ("Digmark is owned by Universal. Filtr is owned by Sony. Topsify is owned by Warner.").

[105] Jenkins, *supra* note 102.

[106] Daniel Sanchez, *How I Got 10,000 Spotify Plays For a Totally Fake Song*, DIGITALMUSICNEWS (Dec. 5, 2017), https://www.digitalmusicnews.com/2017/12/05/spotify-fake-plays/.

[107] *Id.*

Spotify to detect.[108] As such, it would be challenging for Spotify to enforce a policy against payment for placement on user-created playlists, including popular playlists that enhance a song's chances of being featured in an in-house Spotify playlist. This "playola" functions through a third party, much like the "independent promoter" payola of terrestrial radio. Even if Spotify is not seeking this result, its playlists incorporate the effects of these payments. The increased likelihood of appearing on an in-house playlist, in turn, leads to an increased likelihood of receiving significant revenues and an increased listener base.

If a market for playlist placement develops, the "pay-to-be-played paradigm" of success in the online music industry may develop in streaming services, requiring artists to purchase spots on known playlists to have a chance of being placed on Spotify's playlists.[109] The amount of advertising payments that would need to achieve success through Spotify is unclear; it has been noted that to earn minimum wage, an artist would need to have 1,117,021 plays per month.[110] If this number of plays can be achieved only through placement on popular playlists, payment may be many artists' best option. The problem with this paradigm is that many musicians, particularly new and independent ones, cannot afford to make this investment at an early stage in their career.

V. SHOULD THERE BE REGULATION OF INTERNET "PLAYOLA"?

If "playola" practices develop, either through under-the-table transactions in exchange for direct placement on in-house playlists, or through the market for user-generated playlist placement that influences the songs featured on the in-house playlists, the question becomes whether it should be regulated. "Anti-playola" regulation can best be analyzed by assessing the arguments for and against payola regulation in terrestrial radio, and applying these arguments in the context of Internet streaming services.

---

[108] *See* Tim Ingham, *The Great Big Spotify Scam: Did a Bulgarian Playlister Swindle Their Way to a Fortune on Streaming Service?*, MUSIC BUS. WORLDWIDE (Feb. 20, 2018), https://www.musicbusinessworldwide.com/great-big-spotify-scam-bulgarian-playlister-swindle-way-fortune-streaming-service/ (describing how a Bulgarian operation received as much as $1 million in royalties out of Spotify after uploading several third-party playlists of songs and creating fake Spotify accounts to boost their play counts).

[109] *See* Davis, *supra* note 5, at 403.

[110] INFORMATION IS BEAUTIFUL, *How Much do Music Artists Earn Online – 2015 Remix* (Apr. 2015), https://informationisbeautiful.net/visualizations/how-much-do-music-artists-earn-online-2015-remix/.

a. The Debate on Payola Regulation in Terrestrial Radio

The first source of debate on whether payola regulation is worthwhile comes from commentators dealing with the long history of payola in terrestrial radio. The debate over regulation of payola can be divided into three categories: economic efficiency, aesthetics, and morality.[111]

Economic-efficiency arguments concern whether regulation makes sense from a law-and-economics point of view. Pro-regulation commentators argue that allowing payola will result in a market where only well-off players have an opportunity to succeed, or even participate. They posit that there is no efficient market for payola due to the influence of major record labels. On the other end, various law-and-economics scholars have argued that the market will efficiently price songs to reflect the costs of the music market. They also argue that allowing pay-to-play would open opportunities to smaller labels and independents, either through a set price for airtime or increased prices meant to compensate radio stations for the increased risk of airing a lesser-known artist.

The aesthetic argument posits that if payola is permitted, music will be chosen based on money paid rather than its quality. As such, the overall quality of music on radio will decline; "bad" music will be played despite its lower quality as long as the artist is willing to pay. The main response is that radio stations will not air music that their listeners will not enjoy, even if they are offered money for doing so. Because radio stations can only profit if they have a loyal base of listeners, playing "bad" music will cause harm that outweighs the compensation they may receive for playing those songs. Critics of payola regulation have also tried to reframe the debate. They argue that music quality should be measured based on whether it is "homogeneous" or "diverse," and that there is no reason to believe that payola will result in homogenous programming.[112]

The morality argument stems from the view that the harm of payola is not the pricing mechanism, but its deceptive quality. The prohibited action is not pay-to-play, but pay-to-play without disclosure. Therefore, some commentators argue that regardless of whether the price paid would stem from an efficient market for airtime, the practice of payola should be banned

---

[111] *See* Galuszka, *supra* note 51, at 68.

[112] *See, e.g.*, *id.* at 69 ("Instead of discussing whether payola leads to the promotion of 'bad music,' the analysis should rather focus on whether anti-payola legislation adds to the emergence of homogenized radio.").

because it deceives listeners. The response, however, is that this deception will not be relevant where there is an efficiently priced market that encourages diverse programming. Critics of regulation also point out that other sectors of the entertainment industry engage in practices akin to undisclosed payola, and customers do not suffer for it.

i. Economic Efficiency

Government regulation of radio has traditionally been justified by scarcity: "its facilities are limited; they are not available to all who may wish to use them; the radio spectrum simply is not large enough to accommodate everybody."[113] Regulators' decision to control limited airtime stemmed from their desire to prevent concentration of political power that could potentially be dangerous, as the combination of spectrum scarcity and the ability to broadcast was seen as having political significance.[114] As such, both the legislature and the Supreme Court envisioned the FCC playing an intrusive role in traditional broadcasting, "choosing [who received control of airtime] from among the many who apply."[115] Based on the scarcity rationale, the FCC put a large number of regulations on traditional broadcasters, meant to satisfy a number of public policy goals.[116] Under this argument, because of the scarcity of the market, allowing payola practices would result in a concentration of airtime in the hands of those with the greatest wealth. As such, failure to regulate payola would result in the very concentration of power that the FCC was entrusted to avoid.

The primary economic argument against anti-payola regulation is simply that legalizing a market for airplay is the most efficient solution.[117] Critics posit that regulatory efforts stem from a failure to recognize the elements of the music market. In short, they say that radio is a market for music, and "should be left to regulate itself."[118] This argument is based on an

---

[113] Nat'l Broadcasting Co., Inc. v. United States, 319 U.S. 190, 216 (1943).

[114] *See* David A. Moss & Michael R. Fein, *Radio Regulation Revisited: Coase, the FCC, and the Public Interest*, 15 J. POL'Y HIST. 389, 390, 396 (2003).

[115] *Nat'l Broadcasting Co.*, 319 U.S. at 216; *see* John W. Berresford, *The Scarcity Rationale for Regulating Traditional Broadcasting: An Idea Whose Time Has Passed*, FED. COMM. COMM'N, MEDIA BUREAU STAFF 1 (Mar. 2005), https://docs.fcc.gov/public/attachments/DOC-257534A1.pdf.

[116] Berresford, *supra* note 115, at 3.

[117] *See* Galuszka, *supra* note 51, at 54–55, 58.

[118] Repyneck, *supra* note 73, at 725.

early paper by Professor Ronald Coase on the economics of payola.[119] Professor Coase argued three fundamental propositions of terrestrial radio payola.[120] The most relevant is his first proposition: a radio station that plays a song in effect advertises a specific product, and there is no reason to believe that a record company that dispenses payola will spend its advertising resources on "bad" music rather than "good" music.[121] A potential response to the economic-efficiency argument is that it would be difficult to precisely price the airing of a song, since it is difficult to measure the relationship between the broadcasting of each track and the size of the audience for that track.[122] However, in a competitive market for airtime, it would be in the interest of radio stations to learn as much as possible about the popularity of each track in order to develop an adequate price mechanism.[123]

Another economic argument (not put forward by Coase) is that direct pay-for-play would actually allow independent record labels to compete with major labels that control the promotional market, since paying a finite amount for airtime is easier than the web of informal connections that determine airtime otherwise.[124] Even if payola were outlawed, program directors are still more likely to prefer airing music released by major record labels because it is easier to justify, or because it is less risky, since major labels have already put in some amount of due diligence in determining which artists they represent.[125] A legal market for airplay might give smaller labels and independent artists the opportunity to pay radio stations a price that incorporates a premium for the increased risk—the higher chance that the audience will not like the song—that the station will take.[126]

---

[119] Sidak & Kronemyer, *supra* note 57, at 521.

[120] *Id*.

[121] *Id.* Coase's other propositions were that a similar pricing system was commonplace with respect to the inclusion of songs in live performances, and that movements to prohibit payola have been used since at least the 1890s as weapons by record and music publishing firms to reduce their own advertising costs and restrict advertising by new entrants. Sidak & Kronemyer, supra note 57, at 521.

[122] Galuszka, *supra* note 51, at 53–54.

[123] *Id.* at 54.

[124] *See* Repyneck, *supra* note 73, at 731.

[125] *See* Galuszka, *supra* note 51, at 70.

[126] *Id*.

ii. Aesthetics

Critics of payola contend that the practice results in "mediocre radio, declining listenership, and falling advertising revenues" because music is determined "by the parties with the deepest pockets" rather than being selected for its artistic merit.[127] They argue that there is less room for "creative freedom" on the air, forcing the DJ to make decisions based on economic considerations, thereby commodifying artistic expression.[128] As such, payola shifts the focus from exposing the public to capable musicians to generating maximal revenue from labels' playlists.[129] Further, the limited nature of radio broadcast time means that the potential for promotion of undesirable music is felt even more acutely. If those with money take up the airtime, those with the inability to afford airtime may never be rewarded for their good music.[130] Another fear is that unregulated pay-for-play transactions will reduce radio to "one long series of infomercials."[131]

The argument that payola will hurt the quality of music played on the radio can be addressed by Coase's first proposition: radio stations will make programming decisions based on song quality rather than pay-for-play because higher-quality songs are the most economically lucrative.[132] Regulatory efforts ignore the fact that payola renders the market for hit singles more efficient.[133] When a record label promotes an unpopular song, it will lose money, because "you can't buy a hit."[134] So long as a station can detect that this decreased quality is due to the incorporation of payola practices, it will remedy this by ceasing the use of payola, and the practice will fade away naturally. If payola increases radio quality, the practice will not disappear, but everyone—from the stations to the listeners—will be better off.[135]

---

[127] Abell, *supra* note 48, at 55.

[128] *See* Conway, *supra* note 80, at 345–46.

[129] Zeb G. Schorr, *The Future of Online Music: Balancing the Interests of Labels, Artists, and the Public*, 3 VA. SPORTS & ENT. L.J. 67, 88 (2003).

[130] *See* Repyneck, *supra* note 73, at 725.

[131] Repyneck, *supra* note 73, at 728.

[132] *Id.* at 729.

[133] Sidak & Kronemyer, *supra* note 57, at 566.

[134] Jacob Slichter, *The Price of Fame*, N.Y. TIMES (Jul. 29, 2005), https://www.nytimes.com/2005/07/29/opinion/the-price-of-fame.html.

[135] Galuszka, *supra* note 51, at 73.

The aesthetic issue can also be reframed to focus not on "good" versus "bad" music, but rather on "homogenized" versus "diverse" music. We might care more about the diversity-homogenization dichotomy, because diverse radio satisfies the desires of a wider group of listeners.[136] The problem of insufficient-program diversity arises in terrestrial radio due to the limited frequency spectrum. Critics of payola argue that those who might finance radio through payola or other advertisement are likely more interested in reaching a broader audience than satisfying diverse tastes. However, payola may actually encourage programming diversity by reducing the barriers to entry for small record labels and independent artists.[137]

iii. Morality

The focus of the morality argument against payola is its deceptive quality; the Communications Act outlaws not the actual process of pay-to-play, but doing so without disclosure.[138] The problem with payola is that it "blurs the line between publicity and advertising by concealing sponsorship for a price."[139] Undisclosed sponsorship "deceives the listening audience into thinking songs are selected for airplay based on merit rather than payment."[140] Implicit in this argument is the aesthetic argument detailed above, since listeners will believe that they are listening to music chosen for its quality, when in fact it was chosen based on a payment. The morality/deception argument further suggests that even if payola does not hurt the quality of music, it should not be permitted because of its deceptive nature.

A morality-based argument against anti-payola regulation is that disclosed pay-for-play "makes radio more honest."[141] This argument is based on the premise that, even with anti-payola regulation, some form of payment for airtime will still develop; rather than direct payments, record labels just put their resources into "trips, free records, and other promotional gimmicks."[142] This argument falls in line with the actual history of payola, in which limitations on direct payment resulted in payment through illicit

---

[136] *Id.* at 69.

[137] *See supra* Section IV.

[138] Communications Act of 1934 § 317, 47 U.S.C. § 317 (2017); 47 C.F.R. § 73.1212 (2018).

[139] Ellen P. Goodman, *Stealth Marketing and Editorial Integrity*, 85 TEX. L. REV. 83, 90 (2006).

[140] Kosar, *supra* note 70, at 215.

[141] Abell, *supra* note 48, at 56.

[142] *Id*.

means.[143] Furthermore, payments for airtime could create a "self-regulating system," encouraging the development of new music while addressing the "economic realities" of the music industry, whether or not they are disclosed.[144] Critics of regulation also point out that pay-for-play practices analogous to payola are common in other realms of the entertainment industry.[145] If undisclosed payments for placement in other entertainment industries are not unlawfully deceptive, it is less clear why they should be categorized as such in music.

b. Application to Internet Music Streaming Services

i. Economic Efficiency

Traditionally, the primary rationale for regulating terrestrial radio has been that airspace is limited, so practices that risk reducing competition or increasing homogenization should be regulated.[146] Internet streaming services, however, do not have the problem of frequency spectrum limits; theoretically, there can be as many Internet radio stations as there are listeners.[147] Thus, even if limited airspace would sufficiently curb the market for terrestrial radio, justifying increased regulation, the Internet's openness may make that argument inapplicable and move the Internet music market far closer to Coase's efficient market. If "playola" practices decrease the quality of music on certain playlists, listeners are not confined to those playlists by virtue of limited selection, they can easily unsubscribe and find an alternative. Based on Coase's first proposition, since playlist creators want their playlists to have listeners, if "playola" practices take hold, it will be because they lead to featuring music listeners want to listen to.

Further, while it is difficult and costly to obtain a license and start a terrestrial radio station, a playlist can be created by the click of a button. The market for Internet music services allows for competition among all comers, from established players to new entrants. In fact, nothing can prevent record labels from creating their own Internet radio stations or playlists.[148] However, if this practice actually results in lower-quality music,

---

[143] *See supra* Section III.

[144] Abell, *supra* note 48, at 56.

[145] *See* Conway, *supra* note 80, at 346.

[146] *Nat'l Broadcasting Co.*, 319 U.S. at 216.

[147] Galuszka, *supra* note 51, at 70.

[148] *See id.* at 74–75.

listeners will respond by unsubscribing from those playlists, and biased playlists will be unable to succeed.

ii. Aesthetics

An efficient market for playlist placement also implicates the aesthetic argument: if allowing "playola" results in lower-quality music, users will stop listening to those playlists that incorporate it, and the practice will likely fizzle out. Since competition among Internet streaming services is much stronger than among terrestrial radio stations, if a playlist or Internet radio station incorporates "playola" practices and its quality suffers as a result, it will simply lose subscribers and listeners.[149] If "playola" results in similar-quality or even better music, then everyone benefits.[150] In all likelihood, users will subscribe only to those playlists that feature music they actually like, without considering whether "playola" practices occurred; the playlists with the best-quality music will be the ones that succeed.

As for the homogenization of music, Internet music services can be as diverse as necessary to reach the entire music-listening market; there is no limit on the number of listeners they can serve. The potential negative impact of "playola" is that if only major labels representing generic artists have the means to pay for playlist placement, niche artists may not appear on those playlists. However, the potential influence of "playola" on the diversity of programming is similar to its influence on the quality of programming—because there is no limit to the number of playlists, there will always be some playlists that do not accept "playola" and cater to those with diverse music tastes. The lack of limited airspace means that major labels' influence is limited; even if they pay for their artists to be featured, user-created playlists can ensure that independent or smaller artists are also within reach for the interested listener.

iii. Morality

With no implication of scarce resources, there may not be a justification for prohibiting even radio stations that use the "deceptive" practice of undisclosed pay-for-play.[151] If users care enough to research whether certain playlists accept "playola" or are owned by record labels and find these practices unsavory, they will simply limit themselves to playlists that do not

---

[149] *Id.* at 73.

[150] *Id*. at 73.

[151] *Id.* at 72–73.

engage in these practices. The robustness of the Internet allows for alternatives to be made with relative ease. Users of streaming services who strive to be "ethical consumers" can elect to do so with a bit of extra work. The vast majority of users, however, who simply want access to songs they like, will choose their preferred playlists without regard to the practices behind the scenes, so a station's success will depend on the quality of what they feature.

iv. Other Differences

An important distinction between terrestrial radio and Internet streaming services lies in the regulatory landscape. When terrestrial stations air music, they must pay songwriters royalties.[152] However, they are not required pay performance royalties to record labels and artists.[153] Internet music streaming services, on the other hand, must pay performance royalties.[154] Thus far, these rates have given terrestrial radio stations a competitive advantage.[155] Anti-payola legislation may thus be seen as a "trade-off"; terrestrial radio stations are not allowed to accept payola, diminishing their profits, but they do not have to pay performance royalties.[156] Online music services are not exempt from performance royalties, arguably because airplay on the Internet does not stimulate demand for records.[157] If this is true, Internet music services should be allowed to engage in "playola," either because the theoretical basis for anti-payola regulation does not apply to them, or to reduce the competitive disadvantage they face.[158]

---

[152] *Id.* at 73.

[153] *Id.* at 73.

[154] *See* Digital Performance Right in Sound Recordings Act, Pub. L. No. 104-39, 109 Stat. 336 (1995); The Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[155] Galuszka, supra note 51, at 74.

[156] *See* Doug Perlson, *Payola: Could an Old Idea Save Online Radio and the Music Industry?*, BUS. INSIDER (Sept. 8, 2008, 9:35 AM), https://www.businessinsider.com/2008/9/could-payola-save-online-radio ("The law did throw a legal bone to broadcasters. While it made payola illegal for terrestrial broadcasters, it gave the networks an exemption on paying performance royalties to artists. Under this theory, the artists get free promotion for their work and the networks receive their 'payola' in their free use of the artists' material.").

[157] Galuszka, *supra* note 51, at 74.

[158] Perlson, *supra* note 156; *see also* Galuszka, *supra* note 51, at 74.

VI. AUTHORITY TO REGULATE INTERNET MUSIC SERVICES

Even if one concludes that Internet streaming "playola" should be regulated, the question remains whether the FCC would have the authority to do so under the Communications Act or whether a change in the law would be necessary. Further, one can ask whether such regulation would be normatively justified.

a. Legal & Statutory Bases

The national and international nature of the Internet requires that, if it is to be regulated, it should be regulated at the federal level.[159] The question, however, is whether the FCC as it currently stands has authority to regulate Internet music services. On a purely textual basis, "When Sections 317 and 508 of the Communications Act of 1934 were amended in 1960, the legislators could not have foreseen the advent of the Internet."[160] Based on the period in which the amendments were added, one could argue that "any radio stations" must have specifically referred to terrestrial radio.[161] Some have argue that the meaning of "radio station" can evolve to reflect current technology; because Internet radio stations describe themselves as "radio stations," they should be treated in the same way as traditional stations, regardless of the difference in their technology.[162] However, doing so would likely require amending the statutes to refer to radio "by use of any method of transmission."[163] While the argument that the meaning of "radio stations" should evolve might apply to Internet radio services like Pandora, it is less clear in its application to streaming services such as Spotify, which provide a service that is distinct from that of traditional radio.

While the FCC traditionally considered the regulation of Internet content to be beyond the scope of its regulatory power,[164] the Supreme Court has construed the Communications Act as indicating that the FCC was given "regulatory power over all forms of electrical

---

159 *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997).

160 Galuszka, *supra* note 51, at 71.

161 *Id*.

162 *See* Jennifer I. Swirsky, *Payola: Should Internet Radio Stations Be Able to Accept Pay for Play while Over-the-Air Stations Are Statutorily Precluded?* 6 (2009) (unpublished manuscript) https://works.bepress.com/jennifer_swirsky/1/download/.

163 *Id.* at 5–6.

164 A. Nati Davidi, *Patrolling The Red Light District Of The Information Superhighway*, 49 ADMIN. L. REV. 429, 446 (1997).

communication."[165] This suggests that, if the FCC finds that regulation of Internet music streaming services is justified, it would have the authority to enact them. Additionally, the Supreme Court's rationales for the FCC's authority to regulate broadcast radio may apply to regulation of Internet streaming services. In *FCC v. Pacifica Foundation*, the Court held that radio fell into the same category, for the purposes of indecency regulation, as cable television,[166] The Court gave two justifications for its holding: first, that broadcast media had established a "uniquely pervasive presence" in the lives of Americans,[167] and second, "[t]he ease with which children may obtain access to broadcast material broadcasting."[168]

Similar concerns would apply identically to Internet music services—the Internet is pervasive, located in most if not all homes, and usually accessible to children. While one might respond that accessibility of the Internet to children can be limited through parental control, the same argument could apply to broadcast media. One could argue that the pervasiveness of Internet music services suggests that they should be treated the same way as broadcast programming with respect to FCC authority; if the FCC's regulatory authority is justified where a medium is pervasive, Internet music services seem to be a fit.[169]

However, although the "pervasiveness" justification was adopted by the Court, it was not the FCC's original justification for regulating payola practices; that reason was the scarcity of radio and potential for concentration of political power.[170] Since a fundamental distinction between Internet streaming services and terrestrial radio is that there is no scarcity of frequencies, even if the FCC has regulatory authority over the Internet, exercising this authority over "playola" may not be justified.[171]

Another source of potential justification for "playola" regulation is the FCC's own statements regarding its purpose with respect to the Internet. In September 2005, the FCC released an Internet Policy Statement

---

[165] United States v. Southwestern Cable Co., 392 U.S. 157, 168 (1968).

[166] F.C.C. v. Pacifica Foundation, 438 U.S. 726, 750–51 (1978).

[167] *Id.* at 748.

[168] *Id.* at 750.

[169] Matthew Bloom, *Pervasive New Media: Indecency Regulation and the End of the Distinction between Broadcast Technology and Subscription-Based Media*, 9 YALE J.L. & TECH. 122, 126 (2006).

[170] *See* Moss & Fein, *supra* note 114, at 390.

[171] *Id.* at 412.

indicating an intent to "preserve and promote the open and interconnected nature of the public Internet."[172] Under the Internet Policy Statement, the FCC established its authority to act if it found that "Internet service providers were violating principles of openness and interconnectedness."[173] In 2010, the FCC imposed three new rules on Internet broadband providers: a transparency requirement, an anti-blocking provision, and an anti-discrimination requirement.[174] In response to a challenge to this order by Verizon, the D.C. Circuit in *Verizon v. FCC* struck down the anti-blocking and anti-discrimination requirements as outside the FCC's statutory authority.[175] It upheld, however, the FCC's authority to regulate broadband providers in order to achieve its goals of maintaining an open Internet and deploying Internet service to all Americans as described in the Internet Policy Statement, as long as these regulations were within the FCC's statutory authority.[176]

Whether regulation of Internet "playola" would foster or hinder the FCC's goal of encouraging openness and interconnectedness is up for debate. If accepting payment for playlist placement without disclosure to listeners creates limitations to entry in the music market, openness would be hindered. On the other hand, because of the nature of Internet streaming services, there is no limitation on the number of playlists that exist. Thus, even if some playlists are accepting "playola," one could argue that this practice has little effect on the variety of music available. Still, since the Supreme Court did not strike down the FCC's transparency requirement in *Verizon*,[177] it is possible that it would uphold a requirement of disclosure where payola practices are used, under the premise of encouraging openness through enhanced transparency.

b. Normative Arguments

Some commentators have argued that the current royalty structure set by Congress has been seen as a distortion of consumer choice, favoring

---

[172] FED. COMMC'NS COMM'N, INTERNET POLICY STATEMENT, 20 FCC Rcd. 14988 ¶ 4 (2005).

[173] Emma N. Cano, *Saving the Internet: Why Regulating Broadband Providers Can Keep the Internet Open*, 2016 BYU L. REV. 711, 715 (2016) (citing 20 FCC Rcd. 14904 ¶ 96 (2005)).

[174] 25 FCC Rcd. 17937 ¶¶ 54, 63, 68 (2009); Cano, *supra* note 173, at 716.

[175] Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014); Cano, *supra* note 173, at 717.

[176] Cano, *supra* note 173, at 718.

[177] *Verizon*, 740 F.3d at 659.

terrestrial radio over new, competing technologies.[178] This may counsel against additional regulation of streaming services; their success thus far has been an uphill battle against a regulatory structure that favors terrestrial radio, and additional regulation may be too much for them to bear.[179] If Internet music services are swamped by regulation, the effects of their failure will not only be the success of the terrestrial radio industry; the harm will be in the limitation of consumer choice and the slowing of innovation.[180] Further, if one takes the "trade-off" view of the performance-royalties structure, regulating against "playola" could tip the scales even further in favor of terrestrial radio, as Internet music streaming services would not be able to engage in a practice that is justified by the market for playlist placement.

The question of FCC regulation of the Internet also depends on what the "public interest" to be served by the FCC is.[181] In the telecommunications arena, for example, some have argued that the FCC would be better served to focus its policies on the benefits of the Internet rather than the incentives of incumbent actors in the industry.[182] Here, this might justify limiting additional regulation of Internet music services, particularly in light of the existing differences in terrestrial radio and music-streaming services' royalty structures. Over-regulation of Internet music services may result in the stifling of innovation and a limitation on consumer choice, both of which act against the FCC's goal in the 2005 Internet Policy Statement.[183]

Finally, from a law-and-economics perspective, because some argue that prohibiting payola is economically inefficient,[184] critics of regulation have argued that additional regulation of payola may distort the Internet music market's pricing mechanism, which has incorporated the fact that Internet music services have to pay performance royalties, while terrestrial

---

[178] *See* DiCola, *supra* note 39, at 1841.

[179] *See, e.g.*, Michael A. Carrier, *Copyright and Innovation: The Untold Story*, 2012 WIS. L. REV. 891, 916-17 (2012) (describing the music industry as a "wasteland" due to its lack of venture-capital activity); DiCola, *supra* note 39, at 1841 ("Popular webcasting services like Pandora and on-demand streaming services like Spotify operate under enormous uncertainty about their future royalty obligations.").

[180] *See* DiCola, *supra* note 39, at 1841.

[181] Susan P. Crawford, *The Radio and the Internet*, 23 BERKELEY TECH. L.J. 933, 938 (2008).

[182] *Id.* at 959–60.

[183] *See* 20 FCC Rcd. 14988 ¶ 4 (2005).

[184] *See supra* Section IV.

radio stations do not.[185] While the distortion of the market through heavy regulation may be impossible to avoid on terrestrial radio due to the scarcity of airwaves, commentators argue that the same "mistake" should not be made for streaming services.[186] This might suggest that, even with the authority to do so, regulation of Internet "playola" is something that the FCC ought not do.

VII. CONCLUSION

As the market for music streaming services has grown, several practices have developed that may be seen as analogous to the practice of illegal payola in terrestrial radio. These "playola" practices—the direct payment by record labels to streaming services for placement on in-house playlists, and payment for placement on user-created playlists that may lead to being placed on in-house playlists—can be criticized for reasons similar to the traditional criticisms of terrestrial radio payola. Specifically, one could argue that accepting payment for placement may lead to "worse" music; promoting music based on payment rather than based on artistic merit in combination with a failure to disclose placement for payment is a form of immoral deception. However, because Internet streaming services do not face the issue of scarcity, brought on by spectrum limits in terrestrial radio, the market for playlists may be more efficient, giving rise to the potential benefits of payola while controlling for its costs. Even if one concludes that "playola" practices should be regulated based on the traditional rationale for payola regulation, the FCC's approach to Internet regulation likely counsels against such regulations, particularly in light of the established disparity in regulation of terrestrial radio and streaming services.

---

[185] Galuszka, *supra* note 51, at 72.

[186] *Id.* at 73.

SMART HOME TECHNOLOGY: ABUSERS ADAPT TO TECHNOLOGY QUICKER THAN LAWS DO

Kate Lanagan*

Domestic abusers have long used various resources available to them to terrorize their victims. Smart home technology is one of the newest resources that abusers manipulate to control and scare victims. Home is where a person is supposed to feel safest, but the manipulation of smart home technology by domestic abusers obliterates this sense of security and autonomy. Courts are failing to respond to abusive uses of new technology as quickly as abusers are exploiting them. To catch up, states should impose regulations that prevent known domestic abusers from exploiting smart home technology; explicitly include smart home technology in legal definitions of abuse, stalking, and harassment; and offer public educational programs about the misuse of technology.

TABLE OF CONTENTS

* B.A. in Biological Sciences and English, University of Missouri, 2017. J.D. Candidate, University of Missouri School of Law, 2020. Special thanks to Professor Mary Beck for her guidance throughout this process.

I. INTRODUCTION

Smart home technology includes "[i]nternet-connected locks, speakers, thermostats, lights and cameras."[1] Smart home technology is already popular, and projections show it will become even more popular in upcoming years.[2] As of 2018, 32% of American households have installed some form of smart home technology.[3] By 2022, this number is projected to increase to 53.1%.[4] This increase in the number of people using smart home technology is accompanied by a concomitant increase in the number of people who abuse it. Moreover, this technology is economically accessible to the average abuser—indoor smart home cameras that can be connected to smartphones can be purchased on Amazon for as little as $30.[5]

Historically, abusers have employed new methods of domestic violence as technology develops and provides new forms of control.[6] The Domestic Violence Resource Centre Victoria, one of the premier institutions studying the use of smart home technology by abusers, found that 98% of practitioners who serve domestic violence clients said their clients "had experienced technology-facilitated stalking and abuse."[7] Smart home

---

[1] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[2] *Smart Home Penetration Rate*, STATISTA (Nov. 2018), https://www.statista.com/outlook/279/109/smart-home/united-states.

[3] *Id.*

[4] *Id.*

[5] *Aobelieve Outdoor Wall Mount with Weatherproof Case for Wyze Cam Wireless Camera, Security Mounting Bracket Holder with Protective Waterproof Housing Cover for Wyze v1/v2 Camera, White*, AMAZON, https://www.amazon.com/Wyze-Indoor-Wireless-Camera-Vision/dp/B076H3SRXG?qid=1539049363&refinements=p_36%3A1253504011&s=Camera+%26+Photo&sr=1-1&ref=sr_1_1 (last visited Feb. 11, 2019 5:34 PM) (selling wireless cameras for $25.98 per camera).

[6] Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, *ReCharge: Women's Technology Safety, Legal Resources, Research & Training*, SMARTSAFE (2015), http://www.smartsafe.org.au/sites/default/files/ReCharge-Womens-Technology-Safety-Report-2015.pdf; *see also,* Wendy Patrick, *Remote Controlled: Domestic Abuse Through Technology*, PSYCHOLOGY TODAY (Jul. 22, 2018), https://www.psychologytoday.com/us/blog/why-bad-looks-good/201807/remote-controlled-domestic-abuse-through-technology ("[I]nventions have provided new avenues to harass, scare, or intimidate victims in a domestic violence context.") (citations omitted).

[7] Women's Legal Service NSW, Domestic Violence Resource Centre Victoria and WESNET, *ReCharge: Women's Technology Safety, Legal Resources, Research &*

technology now allows abusers to easily control and terrorize victims in the place in which they should feel most secure—their home. Through smartphone apps, they can use smart home technology to harass victims by remotely engaging locks, randomly blaring music, controlling lights and thermostats, and watching victims through cameras or webcams.[8] Abusers also extract extensive and intimate information from smart home devices.[9] Such information is so easily accessible that even non-abused consumers express anxiety about their technology and its control over them.[10] An average of 70% of consumers worry about hackers invading their home systems and 58% worry that manufacturers retain access to their personal data.[11] Abusers' deliberate manipulation of smart home technology terrifies victims, violates their sense of security, and makes them question their sanity.[12]

This Article will examine the evolving connection between domestic violence and technology and address the complexities courts face in responding to technology-based abuse. Additionally, this Article will discuss the quandary state legislators face in trying to craft laws that can keep pace with ever-changing technology to both protect victims and punish abusers. This Article proposes specific initiatives to address the abusive uses of smart home technology including: (1) state regulations on this technology to prevent known domestic abusers from exploiting it; (2) legislation explicitly including exploitation of smart home technology in legal definitions of abuse, stalking, and harassment; and (3) educational programs implemented by states to educate the judiciary and the public about this topic.

II. BACKGROUND

Courts slowly adapt to evolving forms of technology, in part as a response to legislators' failure to draft specific statutes that accurately

---

Training, SMARTSAFE (2015), http://www.smartsafe.org.au/sites/default/files/ReCharge-Womens-Technology-Safety-Report-2015.pdf

[8] *Id.*

[9] Ronda Kaysen, *Is My Not-So-Smart House Watching Me?*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/realestate/is-my-not-so-smart-house-watching-me.html?module=inline.

[10] *Id.*

[11] *Id.*

[12] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

express the many ways abusers exploit technology.[13] Courts have historically struggled to keep up with all of the ways that technology is being used or misused.[14]

Abusers' misuse of technology is prevalent.[15] A 2014 survey from the National Network to End Domestic Violence found that 97% of victims are being "harassed, monitored, and threatened by offenders misusing technology."[16] Three of the most frequently used technologies for abuse are texting (96%), social media (86%), and email (78%).[17] Survivors often have difficulty removing their abuser's access to them through these mediums because of society's dependence on technology.[18] Moreover, law enforcement often has problems identifying an abuser who uses technology because it is difficult to prove the identity of a virtual abuser.[19] Based on these statistics, abusers will have more modes of abuse as availability of newer technology expands and will potentially have more ways to disguise their abusive actions.

The Supreme Court began recognizing privacy in 1886 in *Boyd v. United States*, where it examined governmental invasion of one's home.[20] The Court stated, "[I]t is not the breaking of doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . which underlies and constitutes the essence of [this] judgment."[21] Over a century later, SCOTUS expanded its invasion of security theme to 21st century technology in *Kyllo v. United States*.[22] The Court stated in *Kyllo* that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have

---

[13] Melissa F. Brown, *Safety and Security in a Digital Age*, S.C. LAW., July 2010, at 38, 44.

[14] *Id.*

[15] *See* Kaofeng Lee, *A Glimpse from The Field: How Abusers Are Misusing Technology*, Technology Safety (Feb. 17, 2015), https://www.techsafety.org/blog/2015/2/17/a-glimpse-from-the-field-how-abusers-are-misusing-technology (follow "Click here for a copy of the report" hyperlink for access to the National Network to End Domestic Violence, *Safety Net Technology Safety Survey 2014*, 1 (2014) [hereinafter *Technology Safety Survey*]).

[16] *Technology Safety Survey, supra* note 15 at 1.

[17] *Technology Safety Survey, supra* note 15 at 2.

[18] *Technology Safety Survey, supra* note 15 at 2.

[19] *Technology Safety Survey, supra* note 15 at 2.

[20] Boyd v. United States, 116 U.S. 616 (1886).

[21] *Id.* at 630.

[22] Kyllo v. United States, 533 U.S. 27 (2001).

been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[23] That holding dealt with warrants, but abusive use of smart home technology necessitates a further expansion of the standard of invasion of security. The autonomy and safety of a person's private life is of utmost importance.

The original legislative intent behind the Fourth and Fifth Amendments was to protect people from *physical* home invasions.[24] There is an argument that these amendments should also be extended to prevent the government from abusing technology to virtually invade a person's home.[25] It stands to reason that a private person (a domestic abuser) should not be able to legally invade a victim's home, especially if the government's invasion is prohibited as well.

While unauthorized government invasion of privacy is unconstitutional, laws limit the reach of the state.[26] A domestic partner's invasion of privacy is especially problematic because the victim has likely granted access to the abuser who is unlikely to limit his reach or respond to any limits. When victims call shelters and hotlines for help, they report feeling like they are going crazy because smart home abuse is so personal and done anonymously from a distance.[27] In a recently sensationalized case, an abuser's emotional manipulation over text messages were found to be coercive enough to cause a young man to take his own life.[28]

Telephone harassment and GPS stalking are now recognized forms of domestic abuse, but it is taking legislators and courts a long time to

---

[23] *Id.* at 40.

[24] Jessica Cocco, *Smart Home Technology for the Elderly and the Need for Regulation*, 6 PITT. J. ENVTL PUB. HEALTH L. 85, 100 (2011) (referencing *Boyd*, 116 U.S. 616).

[25] *Id*.

[26] *See, e.g.,* The National Domestic Violence Hotline, *Stalking Safety Planning,* https://www.thehotline.org/2019/01/25/stalking-safety-planning/ (last visited Feb. 25, 2019) ("The legal definition of stalking does vary from state to state.").

[27] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES, (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[28] Com. v. Carter, 52 N.E.3d 1054, 1063-64 (Mass. 2016) (finding the defendant guilty of involuntary manslaughter, considering "the ***defendant's virtual presence*** at the time of the suicide, the previous constant pressure the defendant had put on the victim, and his already delicate mental state.") (emphasis added).

acknowledge this.[29] In 2007, the Seventh Circuit held in *United States v. Garcia* that installing a GPS device on a car that is located on a public street does not constitute a search and that such monitoring does not violate the Fourth Amendment.[30] Along these same lines, the Supreme Court held in *United States v. Knotts* that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[31] Later, New York's highest court distinguished *Knotts* in *People v. Weaver* by asserting that improved technology requires more restrictions and held that the installation of a GPS and monitoring of a car's location did qualify as a search under the Fourth Amendment and was thereby unconstitutional.[32] The *Weaver* court stated, "It bears remembering that criminals can, and will, use the most modern and efficient tools available to them, and will not get warrants before doing so."[33] The dissent in *Weaver* was concerned that imposing constitutional restrictions would limit law enforcement's ability to adapt to advancements in technology as quickly as criminals would be able to.[34] Constitutional restraints vis a vis law enforcement aside, this concern should still be at the forefront of domestic violence courts' agendas because abusers adapt to technology quicker than laws do.[35]

The Violence Against Women Act of 2005 (VAWA 2005) criminalized stalking by way of surveillance, including GPS tracking.[36] It also extended abusers' accountability for substantial emotional harm to victims, which was a major improvement to federal stalking law.[37] Part of VAWA 2005's stated purpose is "to develop safe uses of technology . . . to protect against abuses of technology (such as electronic or GPS stalking), or provid[e] training for law enforcement on high tech electronic crimes of

---

[29] Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR, (Sept. 15, 2014), https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

[30] United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

[31] United States v. Knotts, 460 U.S. 276, 281 (1983).

[32] People v. Weaver, 909 N.E.2d 1195, 1204 (N.Y. 2009).

[33] *Id.*

[34] *Id.*

[35] *See id.*

[36] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109–162, § 41102(4), 119 Stat 2960, (2006) (codified as amended 34 U.S.C. § 12442(4)).

[37] *Id*.

domestic violence, dating violence, sexual assault, and stalking."[38] VAWA 2005 also increased minimum penalties for abusers who violated already existing orders of protection.[39] However, many abusers still go undeterred because of loopholes in laws dealing with stalking by way of surveillance.[40] For example, the criminal definition of stalking does not include marital spying as a criminal offense.[41] Abusers can also easily illegally gain control over a phone's GPS system to track the whereabouts of their victims.[42] In December of 2018, VAWA expired.[43] The reauthorization process has been slow due to the government shutdown[44] and partisan fights over potential changes to existing law.[45] As of April 4, 2019, the House of Representatives voted to reauthorize VAWA, but the Senate is working on a new version.[46]

Courts can evolve to adapt to new technologies. For example, courts recognized the use of spyware software, which collects personal information, records keystrokes, and monitors a user's browsing history and habits, as a form of abuse.[47] Similar to smart home technology, spyware software is accessible and inexpensive.[48] It is also relatively undetectable on computers unless users purchase and install special anti-spyware detection software.[49] When abusers take advantage of spyware to abuse, they violate the Unlawful Access to Stored Communications Act (UASCA),[50] which

---

[38] *Id.*

[39] *Id.*

[40] Melissa F. Brown, *Safety and Security in a Digital Age*, S.C. LAW., July 2010, at 38, 44.

[41] *Id.* at 47.

[42] *Id*.

[43] Ericka Cruz, *Congress Debates Reauthorization of Expired Violence Against Women Act*, IMMIGRATION IMPACT (Mar. 20, 2019), http://immigrationimpact.com/2019/03/20/congress-reauthorize-violence-women-act/ ("Due to the government shutdown, VAWA expired on December 21, 2018. It was briefly revived through a short-term spending bill in late January 2019 but lapsed again in mid-February. Last week, Congress resumed efforts to reinstate the legislation by passing out of the House Judiciary Committee H.R. 1585, a bipartisan bill to reauthorize VAWA and adjust some aspects of the existing law.").

[44] *Id.*

[45] Ashley Killough, *House passes reauthorization of Violence Against Women Act*, CNN, (Apr. 4, 2019 2:59 PM EST), https://www.cnn.com/2019/04/04/politics/house-passes-violence-against-women-act-reauthorization/index.html.

[46] *Id.*

[47] Melissa F. Brown, *Safety and Security in a Digital Age*, S.C. LAW, July 2010, at 38, 45.

[48] *Id.*

[49] *Id.*

[50] *Id.*; 18 U.S.C.A. § 2701 (West).

prohibits a person from "intentionally access[ing] without authorization a facility through which an electric communication service is provided . . . and thereby obtain[ing] . . . access to a wire or electronic communication."[51] The UASCA, originally enacted in 1986, was created to protect security in the age of evolving electronic communication.[52] As a reference point, the UASCA was passed three years prior to the invention of the "world wide web" and seven years before its public release.[53] The UASCA exhibits how legislators have crafted or adapted laws to evolve with similar technological advances in order to protect privacy.[54]

Abusers also utilize social media to control or intimidate victims. In *Shaw v. Young*, a Louisiana court held that threatening or harassing social media posts, emails, and text messages suffice for the issuance of a permanent protective order.[55] Massachusetts stated in *Commonwealth v. Walters*, "There is no question that new technology has created increasing opportunities for stalkers to monitor, harass, and instill fear in their victims, including through use of Web sites."[56] VAWA 2005 was amended to include provisions to prevent cyberbullying and cyberstalking.[57] Courts can recognize and adapt to technological advances; however, this adaptation seems to be slow and reluctant.

Courts have hesitated at protecting victims in public spaces, where abusers have more of a right to be.[58] Workplace violence is an example of this.[59] When domestic violence is relegated to the "private sphere,"

---

[51] 18 U.S.C.A. § 2701 (West).

[52] *Id*.

[53] David Grossman, *On This Day 25 Years Ago, the Web Became Public Domain,* POPULAR MECHANICS (Apr. 30, 2018), https://www.popularmechanics.com/culture/web/a20104417/www-public-domain/ (stating the "world wide web" was invented in 1989 and made public in 1993).

[54] *See* 18 U.S.C.A. § 2701

[55] Shaw v. Young, 2015-0974 (La. App. 4 Cir. 8/17/16), 199 So. 3d 1180, 1187.

[56] Commonwealth v. Walters, 37 N.E.3d 980, 995–96 (Mass. 2015).

[57] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109–162, § 41102(4), 119 Stat 2960, (2006) (codified as amended 34 U.S.C. § 12442(4)).

[58] Britney M. Miller, *From Private to Public: The Impact of Domestic Violence in the Workplace*, MOSS & BARNETT (May 24, 2016), http://www.lawmoss.com/publications/from-private-to-public-the-impact-of-domestic-violence-in-the-workplace-2/.

[59] *Id*.

instances of public domestic violence go unpunished.[60] Courts, historically, have "been hesitant to enter" the private realm.[61] The dilemma regarding the dangers of surveillance technology has been compared to the dangers of owning a knife: "You can always cut vegetables but you can also kill your neighbor."[62] Many people use smart home technology legally, but, once manipulated, the oppression and harm suffered by victims is petrifying.[63] Smart home technology poses a unique threat: the abuser is not in the home, but the abuse happening *is* in the home. This makes it more complicated to tie the abuser to the abuse, as smart home technology can be manipulated with the click of a button from thousands of miles away. A person's home is the crux of their private life, and courts need to protect victims there.

III. ANALYSIS

Today, technology pervades society and technology-facilitated abuse is difficult to control and stop.[64] People are increasingly using smart home technology, and its use exposes inhabitants to increased instances of abuse.[65] Courts and legislators need to catch up to advancements in technology to better protect victims of abuse. States should impose certain regulations prohibiting known domestic abusers from manipulating smart home technology. Legislators need to explicitly include smart home technology in legal definitions of abuse, stalking, and harassment for both civil and criminal law. With such definitions, judges can make civil protection orders or convict abusers for manipulating smart home technology. States should also offer educational programs to assist the judiciary and the public in recognizing this form of abuse. Education programs should specifically be implemented in shelters so that victims of abuse can learn to recognize the signs.

---

[60] *Id*.

[61] Claire Kelleher-Smith, Surveillance as Control: Legally Recognized Harms of Intimate Partner Spying, (2011) *in* DOMESTIC VIOLENCE LAW, 792-93 (Nancy K.D. Lemon, 5th ed., 2018).

[62] *Id.* at 793.

[63] *Id*.

[64] Mary Graw Leary, *The Supreme Digital Divide*, 48 TEX. TECH L. REV. 65, 76 (2015).

[65] *Id*.

Surveillance is key to controlling a victim, which is an abuser's main goal.[66] Federal and state laws have long recognized general surveillance as a form of domestic violence.[67] Historically, abusers control and monitor victims by stalking, arranging for someone else to follow them, or locking them into a house or room.[68] Now, abusers can purchase spyware or in-home surveillance and maintain control from anywhere in the world with the touch of an app.[69] As Massachusetts recognized in *Commonwealth v. Walters*, technology has indisputably increased a stalker's ability "to monitor, harass, and instill fear in their victims."[70]

Abusers exploit technology in many ways, including using smartphones and social media apps for human trafficking.[71] Technology offers an easily accessible and efficient way to control victims with minimal risk of detection—by the victim or by the authorities.[72] Victims are uniquely vulnerable to technology because it can be used to access every part of a person's life, including their text messages, current location, financial activities, and other aspects of a victim's life that provides an abuser with almost unlimited ability to monitor and control their victim.[73] Smart home technology gives abusers the ability to pervade the most intimate and private of places: one's home.[74] Home is where a person is supposed to feel safest, and the misuse of technology to destroy that safety obliterates any sense of security and peace.[75] The Supreme Court stated in *Union Pac. R.R.*

---

[66] Claire Kelleher-Smith, Surveillance as Control: Legally Recognized Harms of Intimate Partner Spying, (2011) *in* DOMESTIC VIOLENCE LAW, 790 (Nancy K.D. Lemon, 5th ed., 2018).

[67] *Id*.

[68] Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR ALL THINGS TECH, (Sept. 15, 2014) https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

[69] *Id*.

[70] Commonwealth v. Walters, 37 N.E.3d 980, 995–96 (Mass. 2015).

[71] Mark Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, USC ANNENBERG CENTER ON COMMUNICATION LEADERSHIP & POLICY (Nov. 2012), https://technologyandtrafficking.usc.edu/files/2012/11/USC-Annenberg-Technology-and-Human-Trafficking-2012.pdf.

[72] *See* Claire Kelleher-Smith, Surveillance as Control: Legally Recognized Harms of Intimate Partner Spying, (2011) *in* DOMESTIC VIOLENCE LAW, 792 (Nancy K.D. Lemon, 5th ed., 2018).

[73] *Id.*

[74] *Id*.

[75] *Id*.

v. Botsford, "[N]o right is held more sacred, or is more carefully guarded . . . than the right of every individual to the possession and control of his own person, free from restraint or interference of others, unless by clear and unquestionable authority."[76] Domestic violence courts and legislators should keep privacy of victims at the forefront of their agendas.

a. Legislators Should Explicitly Include Smart Home Technology in Legal Definitions.

Courts need to become aware of the abuses of smart home technology in order to better protect victims. Smart home manipulation should be explicitly included in criminal definitions and civil protection order definitions of abuse and stalking. This would be a bright-line rule, so courts would apply the law uniformly. Judges would have no discretion as to whether manipulation of smart home technology should constitute as abuse or stalking, as it would be explicitly included in legal definitions.

b. Regulation of Smart Home Technology or Mandatory Educational Programs Could Help Protect Victims of Abuse.

State regulatory protections could be extended over smart home technology to protect victims. Security implementations provided by vendors alone are poor and do not protect victims.[77] For example, the Privacy Rights Clearing House analyzed 43 health-related phone apps and found that only half of the privacy policies reflected the app's actual behavior.[78] They also found that only 15% of user data was being encrypted before being sent from the mobile device to the developer's website, and none of it was encrypted while being stored locally on the device.[79] To motivate companies to make their products more secure and less susceptible to hacks, states can require manufacturers to be more transparent.[80] California enacted a law requiring a company's privacy policies to be released to the general public instead of only to customers.[81] If other states implement similar regulations, it may motivate companies to make their products and

---

[76] Union Pac. R.R. v. Botsford, 141 U.S. 250, 251 (1891).

[77] Amadou Diallo, *Do Smart Devices Need Regulation? FTC Examines Internet of Things*, FORBES, (Nov. 23, 2013), https://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/#18291d878015.

[78] *Id.*

[79] *Id.*

[80] *Id*.

[81] *Id*.

policies more secure.[82] State requirement of public disclosures shows companies that privacy advocates and the Federal Trade Commission care about security and are monitoring them.[83]

Regulation could also include mandatory disclosures.[84] Manufacturers could use mandatory disclosures to warn purchasers of potential abuse. Additionally, smartphone applications that are used to control smart home technologies could carry basic minimum requirements and warnings. Smart home technology should not be available to those previously charged with domestic violence. The risk of abuser's manipulating this technology is too great.

States should offer data literacy and educational programs to further protect victims.[85] Public institutions, including libraries, schools, and shelters, could offer programs about advancements in technology and their effects on privacy. States should also offer seminars on technology as a form of continuing education for judges, lawyers, and law enforcement officers. Increasing awareness of this issue in the legal profession can allow practitioners and the judiciary to stay up-to-date with modern technology, ask the right questions, and recognize this serious form of abuse. Education within shelters could also help victims protect themselves. Many victims may not think to change passwords after fleeing abuse. Educational programs could remind them of this and help them understand the dangers that come with different forms of technology.

"Danger Assessments" are evidence-based tools to predict the likelihood a victim may suffer from serious harm or homicide.[86] These instruments are used to help determine a victim's level of danger based on a series of questions.[87] They presently inquire into partner surveillance and

---

[82] *Id*.

[83] *Id*.

[84] Thomas A. Lambert, *How to Regulate: A Guide for Policymakers*, 197 (2017).

[85] Elise Herron, *Watch: Intel's In-House Gender Studies Scholar Melissa Gregg Says Women Should Be Designing Smart Home Technology*, (June 25, 2018), https://www.wweek.com/news/2018/06/25/watch-intels-in-house-gender-studies-scholar-melissa-gregg-says-women-should-be-designing-smart-home-technology/.

[86] *See* John Hopkins School of Nursing, *Danger Assessment* https://learn.+nursing.jhu.edu/instruments-interventions/Danger%20Assessment/index.html (last visited Mar. 22, 2019 11:33 pm) ("The Danger Assessment helps to determine the level of danger an abused woman has of being killed by her intimate partner.").

[87] *Id*.

stalking.[88] The manipulation of smart home technology should count as a specific form of stalking on Danger Assessments, and researchers should examine the association of such smart home stalking to serious assault and homicide. After establishing an evidence-based research association, abuses of technology should be explicitly inquired about on Danger Assessments.

Jurisdictions could add additional questions about how partners use technology or if their homes have smart home technology. Abuse victims and domestic violence advocates may not initially think of smart home technology or at-home security cameras as instruments that could be aiding the abuser. Explicitly including technology on these Danger Assessments would help advocates and victims become aware of this prevalent issue, which they may not have previously considered.

c. Smart Home Technology Can Also be a Tool Against Abusers.

As problematic as smart home technology is in current legal schema, it is important to note that smart home technology may also be a resource to ensure justice for victims.[89] Police can pull records from smart home technology devices to build cases against abusers.[90] If the victim has access to the smart home technology, such as a doorbell camera or in-home camera, the victim can assess whether their abuser is in the home.[91] Importantly, a victim's ability to view recorded attacks may give victims insight into the extremity of the abuse,[92] which is often downplayed by abusers and victims alike. As the law evolves with technology, it is important for law enforcement and prosecutors to realize the potential of using smart home technology as a weapon against abusers.

---

[88] Claire Kelleher-Smith, Surveillance as Control: Legally Recognized Harms of Intimate Partner Spying, (2011) *in* DOMESTIC VIOLENCE LAW, 790-91 (Nancy K.D. Lemon, 5th ed., 2018).

[89] Hadeel Al-Alosi, *Technology is both a weapon and a shield for those experiencing domestic violence*, THE CONVERSATION (June 17, 2018), https://theconversation.com/technology-is-both-a-weapon-and-a-shield-for-those-experiencing-domestic-violence-97776.

[90] *Id.*

[91] *Id.*

[92] *Id.*

IV. CONCLUSION

Smart home technology gives abusers access to essentially all dimensions of a victim's life.[93] The abuse is unique in that it is a complete attack on an individual's autonomy and personhood.[94] An abuser's manipulation of the lights, thermostat, doorbell, and television could cause the victim to feel like she is trapped in her own home even if nobody is around.[95] This complete control over the victim's living space threatens a victim's senses of security, individualism, and autonomy. Courts must adapt to new changes in technology, and states must offer educational programs in order to protect victims of abuse.

Courts and legislators are failing to keep up with the advancement of technology.[96] As technology evolves, creative domestic abusers develop more terrifying ways to harass and control victims from a distance in less detectable formats. Legislators, victims, courts, law enforcement, and domestic violence service providers are unfamiliar with the reach of smart home technology manipulation. Smart home technology needs to be explicitly included in legal definitions of abuse, stalking, and harassment. Smart home technology is unique in that it allows abusers to have access over the most intimate and private part of one's life: one's home. Because smart home technology is so invasive and so accessible, courts need to rapidly catch up in order to protect victims.

To correct the power imbalance between abusers and victims, the government should impose certain regulations on smart home technology, such as requiring vendors to be more transparent about their security protections.[97] In order to protect technology users and victims of abuse, public institutions such as libraries, schools, and shelters should offer data literacy

---

[93] *See* Claire Kelleher-Smith, Surveillance as Control: Legally Recognized Harms of Intimate Partner Spying, (2011) *in* DOMESTIC VIOLENCE LAW, 789-90 (Nancy K.D. Lemon, 5th ed., 2018). ("Nearly all abusive intimate relationships involve surveillance.").

[94] *Id*. at 790.

[95] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[96] Delanie Woodlock, *The Abuse of Technology in Domestic Violence and Stalking*, 23 VIOLENCE AGAINST WOMEN 584–602 (2016).

[97] Amadou Diallo, *Do Smart Devices Need Regulation? FTC Examines Internet of Things*, FORBES (Nov. 23, 2013), https://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/#18291d878015.

and educational programs.[98] State bar associations should provide regular education on the abusive and illegal uses of technology to legal practitioners. Courts should explore the idea of educating the judiciary on technology and its abuses. A victim's privacy needs to be at the forefront of legislators' and courts' agenda.

[98] Herron, *supra* note 85.

THE BORDER-SEARCH EXCEPTION: WHAT LEVEL OF SUSPICION IS REASONABLE IN THE DIGITAL ERA?

Jessica G. Martz*

The privacy we can expect in our personal effects as we pass through a port of entry, cross the border, and return from a vacation outside of the United States is evolving slower than the technology we are increasingly reliant on in our daily lives. Three federal circuits are split on the standard that applies before a search of a digital device (such as a cell phone, external hard drive, or laptop) can be performed by law enforcement at the border. History tells us that individual privacy rights at the U.S. borders are different than those described in the Fourth Amendment, but what will happen to the border-search exception in an era of rapidly-advancing technology? Will the United States move closer to an Orwellian surveillance state or will the Court choose privacy over security? This paper's goal is to answer the likely outcome if the U.S. Supreme Court ever weighs-in on this question. Based on recent rulings at the Supreme Court regarding smartphones and cell site location data, it is likely that the Supreme Court will weigh in favor of individual privacy.

* L.L.M. Graduate, Spring 2019, Antonin Scalia Law School, George Mason University. Jessica Martz is also a judge advocate and an active duty Lieutenant Colonel in the United States Marine Corps. ***The views presented are those of the author and do not necessarily represent the views of Department of Defense or its Components***.

TABLE OF CONTENTS

I. INTRODUCTION

Nearly one percent of all travelers coming into the United States have their digital devices searched by Customs and Border Protection officers if they are referred for a secondary inspection.[1] Officers may look at devices during a secondary inspection to ensure that illegal contraband is kept out of the United States.[2] In fact, persons who attempted to bring child pornography or materials tied to terrorism, among other illegal items, have been barred from entry.[3] These searches serve an important function of keeping people and contraband out of the country. The justification for these searches is as old as the Fourth Amendment itself. The challenge courts face today is that issues involving national security and individual privacy seem to outpace the policies and law that seek to keep them in balance. For example, the Office of the Inspector General for the Department of Homeland Security reported violations of protocol when officers searched digital devices during the year 2018.[4] Sometimes, the officers failed to take the device offline in violation of the requirement to take devices off the cloud before performing searches.[5] Public concern about privacy in digital devices continues to grow as the amount of private details about a person's life that a phone or a laptop contains also increases. In the absence of legislation from Congress, the courts continue to wrestle with violations like those described by the Inspector General.

Judge Gregg Costa's concurring opinion in a Fifth Circuit case involving a border search illustrates the tension between privacy in personal digital devices and national security at the nation's border:

> The contours of the border-search doctrine in this new area—what level of suspicion, if any, is required and whether a warrant is ever required—may well turn on whether the interest at the border in general crime fighting and national security, which phone

---

[1] Colleen Long, *Customs Officers Searching More Travelers' Devices*, AP NEWS, (Dec. 10, 2018), https://apnews.com/54497b1d5f5541efb96dc25d11ee66a3.

[2] *Id.*

[3] *Id*.

[4] *Id*.

[5] *Id*.

> searches can further, is as weighty as the traditional justification of seizing contraband . . . .[6]

Until the Supreme Court or Congress weighs in on the matter, the best the courts can do is attempt to follow the law as it stands, which can result in varying approaches. For example, the Fourth and the Eleventh Circuits have applied the Supreme Court's decision in *Riley v. California* to electronic devices searched pursuant to the border-search exception to the Fourth Amendment and, in doing so, reached different conclusions regarding the level of suspicion required by authorities before conducting the search.[7] The federal district courts that have addressed the issue of searches of digital devices at the border mostly find that the government's interest is greater than an individual's privacy concerns. However, the fork in the road for the courts, particularly for the Fourth and the Eleventh Circuits, is the scope of the search that is permitted and the level of suspicion that is required to conduct the search. This paper seeks to explore the circuit split regarding border searches in the context of the latest rulings from the Supreme Court and to determine the appropriate standard that applies to searches and seizures of electronic devices at the border.

Riley v. California did not specifically address searches of devices at the border, but the Supreme Court said that a warrant is required before officers can search a cell phone pursuant to a search incident to an arrest.[8] The Court's treatment of a modern-day cell phone in *Riley* essentially placed it on a pedestal above all other items that a person could have on them, such as a wallet or a briefcase. This is no surprise to practitioners and courts that, in recent years, have seen the argument from defendants in criminal cases that digital devices, such as cell phones, computers, external hard drives, and laptops, are unlike other types of personal property and therefore, require greater privacy protection when it comes to searches and seizures of these items.[9]

---

[6] United States v. Molina-Isidoro, 884 F.3d 287, 297 (5th Cir. 2018) (Costa, J., concurring).

[7] *See, e.g.*, United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

[8] *See generally* Riley v. California, 573 U.S. 373 (2014).

[9] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY AND INFORMATION SECURITY 367 (Rachel E. Barkow et al. eds., 6th ed. 2018).

If Justice Brandeis, one of the early proponents of the right to privacy, were still alive, he might agree. Justice Brandeis said that the Fourth Amendment is the most important of all the rights granted by the Constitution because it gives individuals the "right to be let alone."[10] Individual privacy and protection from intrusions into the individual's home is inviolable in the United States. It is one of the many reasons that resulted in a revolution against the British crown.[11] Those who lived during colonial times dreaded the British "general warrant" used to search anywhere and anyone without any justification because the British law did not recognize an individual right of privacy.[12] British officials raided the homes of colonial Americans and arrested them. Incidentally, several states barred general warrants within their constitutions after the conclusion of the Revolutionary War. The Framers had these experiences in mind when they drafted the Fourth Amendment. The Fourth Amendment of the Constitution, arguably one of the main features of United States law that stands apart from the laws of other nations, states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The Fourth Amendment protects individuals from general warrants and unreasonable searches and seizures.[14] If the search or seizure is reasonable, but likely to be more intrusive, the government must seek a warrant that is based on probable cause and contains particularity regarding the

---

[10] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing that the right of privacy is fundamental to the exercise of "the right to life"); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution . . . . conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men.").

[11] See *Riley*, 573 U.S. at 403 (discussing colonial history driving development of the Fourth Amendment).

[12] *Id.* These general warrants were also referred to as "writs of assistance." *See Writ of Assistance*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/writ-of-assistance (last updated Feb. 28, 2020).

[13] U.S. CONST. amend. IV.

[14] *See id*.; SOLOVE, *supra* note 9, at 161.

things or persons to be searched or seized.[15] Warrantless searches of a person and their effects are often unreasonable unless they fall within one of the exceptions recognized by the law.[16] The exceptions to the general rule are directly tied to officer safety and preservation of evidence in criminal investigations, accident prevention, public health, and public safety.[17] Case law over the last few decades interpreted the Fourth Amendment to protect people, not just places, and often hinged on whether a reasonable expectation of privacy existed in the thing or person to be searched.[18] More recently, the Supreme Court and lower courts addressed cases where the right of the individual "to be let alone," as Justice Brandeis said, and law enforcement's role in keeping the citizens of the United States safe is made more challenging because of the role of emerging technology.[19]

Despite the protections guaranteed by the Fourth Amendment within the interior of the United States, history and Supreme Court precedent tell a different story when it comes to individual privacy rights at the international border. This is because of the government's interest in who and what comes in and leaves the United States. The border-search exception dates back to the creation of the Fourth Amendment when Congress "proposed the Fourth Amendment," and simultaneously "enacted the first far-reaching customs statute in 1790."[20] The authority at the border for customs officers to conduct warrantless searches of travelers without probable cause is historic and arguably as old as the country itself.[21] The Supreme Court recognized this exception to the Fourth Amendment almost a hundred years ago, when writing for the majority, Chief Justice Taft said in *Carroll v. United States*:

> Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in. But

---

[15] LINDA MONK, THE WORDS WE LIVE BY 161 (2015).

[16] STEPHEN DYCUS, ARTHUR L. BERNEY, WILLIAM C. BANKS, PETER RAVEN-HANSEN & STEPHEN I. VLADECK, NATIONAL SECURITY LAW 593–94 (6th ed. 2016).

[17] *Id*. at 594.

[18] *Id*. at 593.

[19] SOLOVE, *supra* note 9, at 14.

[20] United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005); Claudia G. Catalano, Annotation, *Border Search or Seizure of Travelers Laptop Computer, or Other Personal Electronic or Digital Storage Device*, 45 A L.R. FED. 2D 1 (2010).

[21] Catalano, *supra* note 20.

> those lawfully within the country, entitled to use the public highways, have a right to free passage without interruption or search unless a competent official who is authorized to search finds probable cause for believing that their vehicles are carrying contraband or illegal merchandise.[22]

In three seminal border-search exception cases,[23] the Supreme Court held in favor of both warrantless searches and searches involving no suspicion because the government's interest "is at its zenith at the international border."[24] Although, in certain contexts, the Court seems to curtail government action in favor of individual privacy,[25] the Supreme Court's precedent at the border is overwhelmingly in favor of the government doing what it needs to do to prevent contraband from entering the country.[26]

This paper addresses the border-search exception to the Fourth Amendment and anticipates the Supreme Court's treatment of electronic devices in the context of the Fourth Amendment at the border. Part I summarizes Supreme Court precedent on the border-search exception from the last few decades and analyzes its importance to today's challenges. Part II examines the Supreme Court's treatment of digital devices in recent years. Parts III, IV, and V explore the split between federal circuit courts of appeals as well as with federal district courts, regarding the standard that applies after *Riley v. California* to forensic searches of digital devices under the border exception to the Fourth Amendment. Part VI and VII attempt to predict how the current Supreme Court will hold if it ever decides a case involving electronic devices and the border-search exception, especially considering the cases discussed in Part II. In reaching a prediction, this paper will discuss the disputed standard: whether reasonable suspicion or no suspicion is required in the conduct of searches of electronic devices when individuals are crossing an international border into the United States. There are mounting reasons why the Supreme Court of the United States should require reasonable suspicion when the search is "other than a routine border

---

[22] Carroll v. United States, 267 U.S. 132, 154 (1925).

[23] *See generally* United States v. Ramsey, 431 U.S. 606 (1977); United States v. Montoya de Hernandez, 473 U.S. 531 (1985); United States v. Flores-Montano, 541 U.S. 149 (2004).

[24] *Flores-Montano*, 541 U.S. at 152 (citing *Ramsey*, 431 U.S. at 616).

[25] *See e.g., Riley*, 573 U.S. at 373–74 (holding that the government interest in officer safety and in avoiding evidence spoliation did not justify warrantless cell data searches).

[26] *Flores-Montano*, 541 U.S. at 153 (citing *Montoya de Hernandez*, 473 U.S. at 537).

search" based on the history and purpose of the border-search exception (national security, etc.), the Fourth Amendment, and case law—even considering the Supreme Court's recent decisions on privacy and electronic devices. Although the Supreme Court rejected the distinction between "routine" and "nonroutine" in one of its seminal border-search exception cases,[27] it has yet to review a case involving the more complex challenges associated with searches of digital devices at the border.

Disparity in outcomes across the circuit courts will require the Supreme Court make this distinction, or apply and better explain the meaning and application of "other than a routine border search," from *United States v. Montoya de Hernandez*.[28] Considering *Riley*, this is particularly important to prevent confusion for law enforcement at the tactical level in trying to apply the standards issued by the Court. Proof that the Court will likely find that reasonable suspicion is required to conduct a search of a digital device at the border comes from the Court's recent trend of favoring privacy when it comes to emerging technology over the government's interest in *Jones*,[29] *Riley*,[30] and *Carpenter*.[31] Finally, considering the Court's border-search exception precedent, the Eleventh Circuit's decision in *Touset* is correct because it honors the historic authority given to border officials to keep the United States safe. However, if the Supreme Court is given an opportunity to consider a case involving the search of a digital device at the border, it will likely rule consistent with the Fourth Circuit in *United States v. Kolsuz*,[32] and the Ninth Circuit in *United States v. Cotterman*,[33] as well as with other federal courts who have held that *Riley* applies to the border-search exception and demands at least individualized suspicion before a search of a digital device is executed. This paper will also explain how the Supreme Court could hold that *Riley* does not extend to the border-search exception and instead hold consistent with its three seminal border-exception cases.

---

[27] *Flores-Montano*, 541 U.S. at 512.

[28] *Montoya de Hernandez*, 473 U.S. at 540.

[29] United States v. Jones, 565 U.S. 400 (2012).

[30] *Riley*, 573 U.S. at 373.

[31] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[32] *Kolsuz*, 890 F.3d 133.

[33] United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).

II. THE SUPREME COURT AND THE BORDER-SEARCH EXCEPTION

a. *United States v. Ramsey*

United States v. Ramsey, is the first of three seminal border-search exception cases decided by the Supreme Court. *Ramsey* was decided in the 1970s, before the emergence of the current digital age, but the case still stands as binding precedent. In this case, customs officers became suspicious when they noticed several bulky envelopes inbound from Thailand, a well-established source of illegal drugs.[34] Each of the envelopes contained labels typed from the same typewriter, making the officers more suspicious.[35] Officers decided to open the packages when they realized that the envelopes weighed "some three to six times the normal weight of an airmail letter."[36] When the inspector opened one of the envelopes, he discovered a white powdery substance in a plastic bag and had the powder tested.[37] The substance tested positive for heroin.[38] Ultimately, the two individuals connected with the mail were indicted, convicted, and sentenced to imprisonment.[39]

Before trial, the two respondents sought to suppress the evidence seized by the mail inspector.[40] The United States Court of Appeals for the District of Columbia Circuit reversed the convictions, holding that probable cause is required before international mail can be opened.[41] In reviewing the District of Columbia Circuit's decision, the Supreme Court examined the applicable statute, the Fourth Amendment, and case law discussing the border-search exception.[42] The Court held that the postal regulations implicated in this case required "reasonable cause," which it stated was a "less stringent" standard than the probable cause standard required under the Fourth Amendment.[43] Furthermore, the inspector had reasonable cause, as required by the Congressional statute, because the letters were bulky and

---

[34] *Ramsey*, 431 U.S. at 609.
[35] *Id*.
[36] *Id*.
[37] *Id*. at 609–10.
[38] *Id*. at 610.
[39] *Id.* at 610–11.
[40] *Id*. at 610–11.
[41] *Id*. at 611.
[42] *Id*. at 611–12.
[43] *Id*. at 611–14.

they were being shipped from a country that was involved in narcotics trafficking.[44] The respondents in *Ramsey* asked the Court to recognize that mailed letters are different than other items that cross the international border, and therefore deserve the "full panoply of Fourth Amendment protections."[45] Although the Court of Appeals for the District of Columbia Circuit agreed with the respondents, the Supreme Court did not. The Court explained that the border-search exception,

> [I]s grounded in the recognized right of the sovereign to control . . . who and what may enter the country. . . [T]he critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another. It is their entry into this country from without it that makes the resulting search "reasonable."[46]

Justice Rehnquist recognized the historic roots of the border-search exception in United States history and the Court's precedent in reaching his conclusion regarding the reasonableness of the inspector's search of the mail in this case:

> Border searches . . . from before the adoption of the Fourth Amendment, have been considered "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself. We reaffirm it now.[47]

The Supreme Court distinguished this exception from the exigent circumstances exception, classified the border-search exception as being comparable to the search-incident-to-arrest exception, and referenced its

---

[44] *Id.* at 614–15.

[45] *Id*. at 619–20.

[46] *Id*. at 620.

[47] *Id.* at 616–617 (emphasizing the legislative history of the border-search exception by highlighting that the same Congress which proposed the Bill of Rights, including the Fourth Amendment, had previously enacted a customs statute giving customs agents broad power and authority to search ships and vessels where there was reason to suspect concealment of goods).

holding regarding this exception from *United States v. Robinson*.[48] Most people probably think for a postal inspector to open their mail, a warrant is required and in fact, since 1877 as a result of the holding in *Ex Parte Jackson*, and pursuant to 39 U.S.C. § 3623(d), that is generally true.[49] However, when it comes to letters coming from international destinations, the rules change and the government is permitted to perform a search.[50] These holdings illustrate the difference between searches within the interior of the United States and those done at the border, and how the Court views the reasonableness of searches at the border even when the search involves something as private as one's mail.

b. *United States v. Montoya de Hernandez*

If finding reasonableness in a warrantless search of an individual's mail does not convince the reader that the Supreme Court views the Fourth Amendment differently at the border, the holding in *United States v. Montoya de Hernandez*, likely will. In *Montoya de Hernandez*, the Court held that it was reasonable to detain a woman for an "other than [] routine" customs search based on reasonable suspicion that she was smuggling contraband in her gastrointestinal tract.[51]

Ms. Montoya de Hernandez flew into Los Angeles International Airport from Bogota, Columbia carrying her passport, $5,000 in cash, four changes of clothes and the shoes she was wearing.[52] When officials questioned her about her odd combination of personal items she stated that the purpose of her trip was to buy "goods" for her husband's business.[53] Her story triggered some suspicion and when border officials noticed that her passport reflected several trips from Columbia to Miami and Los Angeles within a very short timeframe, they referred her to a secondary inspection.[54] When asked more details about her trip, she could not recall how her plane ticket was purchased, she did not know where she was going to stay while

---

[48] *Id.* at 621 (citing United States v. Robinson, 414 U.S. 218, 224 (1973)).

[49] Ex Parte Jackson, 96 U.S. 727 (1877); 39 U.S.C. § 3623(d); SOLOVE, *supra* note 9, at 291–92.

[50] SOLOVE, *supra* note 9, at 292 (citing United States v. Various Articles of Obscene Merchandise*,* 395 F.Supp. 791 (S.D.N.Y. 1975), *aff'd*, 538 F.2d. 317)).

[51] *Montoya de Hernandez*, 473 U.S. at 540.

[52] *Id*. at 533–34.

[53] *Id*. at 533.

[54] *Id*.

in Los Angeles, and she had no appointments scheduled for making deals for her husband's business.[55] At that point, inspectors suspected Ms. Montoya de Hernandez was a "balloon swallower," or one who tries to bring narcotics into the United States by hiding them inside their body.[56] A pat-down of Ms. Montoya de Hernandez's stomach revealed that her stomach was unusually firm and full.[57] The inspectors put Ms. Montoya de Hernandez on notice that they suspected her stomach was full because she was smuggling drugs, and not because she was pregnant, as she claimed.[58] She was given the option to return to Colombia, submit to an X-ray, or remain in detention until she passed a monitored bowel movement.[59] Initially, she elected to submit to an X-ray but then opted for returning to Colombia.[60] When the good faith efforts of the U.S. Government to return her to Bogota failed, the inspectors told Ms. Montoya de Hernandez that she would remain in custody until she passed a supervised bowel movement.[61] It became evident that Ms. Montoya de Hernandez was willing to risk her own health to avoid revealing the true contents of her abdomen, and almost a day after her arrival, the inspectors sought a court order to have her pregnancy tested, and have an involuntary rectal exam and X-ray conducted.[62] The Magistrate issued the order.[63] The results came back, and the inspectors' suspicions were correct—she was not with child and her body contained more than 88 balloons filled with cocaine.[64]

The suppression motion filed before trial by Ms. Montoya de Hernandez was denied, and she was convicted of possession of cocaine with intent to distribute and of unlawfully importing cocaine into the United States.[65] The United States Court of Appeals for the Ninth Circuit reversed her convictions because the inspectors failed to seek an immediate warrant

---

[55] *Id*.
[56] *Id.* at 534.
[57] *Id*.
[58] *Id*.
[59] *Id*.
[60] *Id*. at 534–35.
[61] *Id.*
[62] *Id*. at 535.
[63] *Id*.
[64] *Id*. at 536.
[65] *Id*.

for an X-ray.[66] The Supreme Court granted certiorari and reversed the holding from the Court of Appeals.[67] In taking on the Court of Appeals decision, the majority opinion from Justice Rehnquist began its analysis with the Fourth Amendment's commandment of reasonableness in the context of government searches or seizures of an individual.[68] Reasonableness is defined by a totality of the circumstances as well as determining whether the action taken by law enforcement was a legitimate government interest that outweighs the individual's Fourth Amendment interest.[69] Citing *Ramsey*, the majority stated, "[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . . "[70] The Court justified this standard by explaining that it is the will of the people through Congress that the border is treated differently than the interior.[71] Congress gave the Executive unlimited authority to conduct warrantless searches and seizures at the border, even in the absence of probable cause, for "routine" searches "in order to . . . prevent the introduction of contraband into this country."[72]

The Court also provided examples from precedent where it had ruled that a search or seizure was lawful, applying standards that were less than probable cause, including no suspicion at all: opening first-class mail, stopping automobiles at the international border, and inspecting boats with access to the sea, based on a deeply rooted interest in monitoring what crosses the border.[73] Additionally, the Court explained, the government's interest is greater at the border than the privacy right of an individual, and therefore individuals should expect less privacy at the border than they are accustomed to inside the United States.[74]

---

[66] *Id.*
[67] *Id*. at 531.
[68] *Id* at 537.
[69] *Id*.
[70] *Id*. at 538 (citing *Ramsey*, 431 U.S. at 616–19).
[71] *Id.* at 538–39.
[72] *Id.* at 537–38.
[73] *Id*. at 538.
[74] *Id*. at 539.

Montoya de Hernandez is significant in border-search exception jurisprudence because it added to the Court's previous ruling in *Ramsey*, when it addressed the appropriate level of suspicion for searches at the border that are "other than [] routine."[75] For searches that are other than routine, reasonable suspicion is required—which means officials at the border are required to have a "particularized and objective basis for suspecting the particular person."[76] In reaching this conclusion, the Court analyzed the holding of the Ninth Circuit, which applied the "clear indication" standard as something that sits between reasonable suspicion and probable cause.[77] The majority found this application of the standard to be incorrect and noted that no other court "has ever adopted . . .'clear indication' language as a Fourth Amendment standard."[78] The Court also criticized the Ninth Circuit's approach as creating a "third verbal standard" in addition to those already falling within Fourth Amendment jurisprudence, and noted that such a standard "may obscure rather than elucidate the meaning of the provision in question."[79] Finally, the Court seemed to reject any distinction between "routine" and "nonroutine" searches at the border for the same reasons it rejected the Ninth's Circuit's "clear indication" standard.[80] The Court instead seemed to focus more on the intrusiveness of the search in finding that reasonable suspicion was required. In this case, a woman was forced to void the contraband border officials believed she had inside her body and intended to smuggle into the United States.[81] Justice Rehnquist was likely careful not to engage in a discussion regarding routine versus nonroutine searches at the border to avoid creating a precedent that could be unworkable in the future based on the facts.

If detaining a suspected alimentary canal smuggler at the border is analogous to detaining someone with a life-threatening communicable illness at the border,[82] it should follow that detaining someone with child pornography at the border is lawful until the suspicion is dispelled that the individual will introduce something harmful into this country. The analogy

---

[75] *Id*. at 540.
[76] *Id.* at 541.
[77] *Id.* at 540.
[78] *Id*.
[79] *Id*. at 541.
[80] *Id.*
[81] *Id.*
[82] *Id*. at 544.

between a drug smuggler and someone carrying tuberculosis at the border, drawn by the Court, reflects the Court's tolerance for the government's interest at the border.[83] The dissent disagreed and instead concluded that such an intrusive search is presumptively reasonable only if a judicial officer permitted the search,[84] implying that a warrant is required for searches at the border that are other than routine.

Currently, Customs and Border Protection officials follow policy consistent with the Ninth and Fourth Circuit conclusion that reasonable suspicion applies to "advanced" (rather than "nonroutine") searches of digital devices at the border.[85] This observation suggests that the digital era outpaces the law and, for at least the foreseeable future, courts will continue to sort through these things in the absence of action by the Executive or Legislative branches.

c. *United States v. Flores-Montano*

The most recent case the Supreme Court decided regarding the border-search exception is *United States v. Flores-Montano*. In *Flores-Montano*, the Court reversed the Ninth Circuit and held that reasonable suspicion was not required in seizing the respondent's gas tank at the international border in southern California.[86] This case began as the result of a secondary inspection conducted on respondent's vehicle after the respondent drove across the international border at the Otay Mesa port of entry in Southern California.[87] A customs inspector tapped the gas tank at the secondary station and noticed that it sounded solid.[88] Within an hour, the gas tank was removed by a mechanic and 37 kilograms of marijuana bricks were discovered inside the respondent's gas tank.[89] The respondent was indicted on charges related to the customs inspector's findings and he moved to suppress the marijuana discovered in his gas tank.[90] Despite the Supreme Court

---

[83] *Id*.

[84] *Id*. at 552 (Brennan, J., dissenting).

[85] U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES 5 (2018).

[86] *Flores-Montano*, 541 U.S. at 149–50.

[87] *Id*. at 150.

[88] *Id*. at 151.

[89] *Id*.

[90] *Id*.

upholding the search of a woman's "alimentary canal"[91] at the border in *Montoya de Hernandez*, the District Court and the Ninth Circuit granted respondent's motion on the basis that Ninth Circuit case law requires reasonable suspicion for the removal of a gas tank to satisfy the Fourth Amendment.[92] The Court analyzed the Ninth Circuit's decision as a misapplication of the Court's previous ruling in *Montoya de Hernandez*.[93] Although the Court discussed "routine" searches in the context of searches performed at the border in *Montoya de Hernandez*, the Court said that the balancing test applied by the Ninth Circuit to determine what is a "routine" search of a vehicle at the border is too complex and had "no place in border searches of vehicles."[94] The Court acknowledged that "the interference with a motorist's possessory interest is not insignificant when the Government removes, disassembles, and reassembles his gas tank," it said, "it nevertheless is justified by the Government's paramount interest in protecting the border."[95] The Court held that the government has the "authority to conduct suspicionless inspections at the border," even when it includes dismantling and reassembling pieces of a person's property, such as the car in this case.[96]

Ramsey, *Montoya de Hernandez*, and *Flores-Montano* establish that almost anything, but not quite everything, goes when it comes to searches at the border. The Court stated that either reasonable suspicion is required for "other than a routine border search,"[97] or that when the search of property is so "destructive," a different result than *Flores-Montano*'s no suspicion required may be necessary.[98] These cases illustrate the Court's stance on searches at the border versus searches in the interior. There is very clearly a different standard. The challenge in the digital age is determining the appropriate level of suspicion required before law enforcement can search a device such as a cell phone or a laptop coming across the international border. In the absence of a Supreme Court ruling on this currently, looking at how the Supreme Court views digital devices in the interior of the United States is valuable in anticipating how the Court might rule.

---

[91] *Montoya de Hernandez*, 473 U.S. at 544.
[92] *Flores-Montano*, 541 U.S. at 151.
[93] *Id*. at 152.
[94] *Id.*
[95] *Id*. at 155.
[96] *Id*.
[97] *Montoya de Hernandez*, 473 U.S. at 540.
[98] *Flores-Montano*, 541 U.S. at 156.

III. THE SUPREME COURT AND DIGITAL DEVICES

The Supreme Court's rulings in three important cases regarding digital devices can be summed up by quoting Chief Justice Roberts' advice to law enforcement in *Riley*, before searching—"get a warrant."[99] The Court sidestepped past cases that seemed to be binding on the Court, particularly in *Riley* and arguably to a greater extent in *Carpenter*, to reach conclusions that favored individual privacy in an era of rapidly evolving technology. The three cases are *Jones*, *Riley*, and *Carpenter.* The Court's willingness to depart from other cases might mean that the historic border-search exception is not immune from change.

a. *United States v. Jones*

Although only marginally related, *Jones* gave valuable insight in 2012 on how the Court viewed privacy in the world of digital devices. Justice Sotomayor's concurring opinion focused on how a digital device such as a GPS monitoring device can generate a wide-ranging "record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[100] She further demonstrated her concern for individual privacy in the context of emerging technology by adding, "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[101] Justice Alito's concurrence took a different approach, highlighting the complex circumstances in an era of "dramatic technological change."[102] Justice Alito also said that in the absence of federal and state legislation regulating these changes, the Court will "apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[103] *Jones* reflects the start of the Court's recent concern about emerging technology and its impact on individual privacy. The Court took this further in *Riley*.

---

[99] *Riley*, 573 U.S. at 403.

[100] *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

[101] *Id*. at 418.

[102] *Id*. at 429 (Alito, J., concurring).

[103] *Id*. at 430 (Alito, J., concurring).

b. *Riley v. California*

The most important of the three noteworthy emerging technology cases, in terms of its potential applicability to border-search exception cases, is *Riley v. California. Riley* is a consolidation of two unrelated cases, one from California and the other from the First Circuit. Both cases involved warrantless searches and seizures of defendants' cell phones by law enforcement during searches incident to arrest.[104] *Riley* is important for the border-search exception because it telegraphs how the Court views privacy on the modern-day cell phone. It also departs from prior search-incident-to-arrest case law, which could affect the border-search exception precedent.

In the first case, while conducting a search incident to arrest on defendant David Riley, a police officer seized Riley's smartphone from the pocket of his pants.[105] The term "CK" appeared during the officer's initial search of the cell phone, which the officer thought to mean "Crip Killers," a term used by members of the Bloods gang.[106] When the officer brought Riley into the police station, the police conducted a further review of his cell phone and discovered photographs that connected him to a recent shooting.[107] Riley was charged with multiple counts in connection to the shooting.[108] At trial, he moved to suppress the evidence obtained from his cell phone, stating that the police violated the Fourth Amendment by not obtaining a warrant before searching the contents of his phone and that the search was performed in the absence of exigent circumstances.[109] The trial court denied his motion.[110] Riley was convicted on all counts.[111] On appeal, the California Court of Appeal affirmed his conviction and sentence and he appealed to the United States Supreme Court.[112]

The second of the two cases involved the search incident to Brima Wurie's arrest. After the officers brought Mr. Wurie to the police station

---

[104] *Riley*, 573 U.S. at 373.
[105] *Id*. at 378–79.
[106] *Id*. at 379.
[107] *Id*.
[108] *Id*.
[109] *Id*.
[110] *Id*. at 380.
[111] *Id*.
[112] *Id*.

they seized the two cell phones he had on his person.[113] The one that is the source of his appeal was a "flip phone."[114] Mr. Wurie received several calls from "my house" on this phone while in custody.[115] Police officers opened the flip phone and used the call log to determine the number belonging to "my house." [116] Using that information, the police tracked down the address of "my house."[117] The police ultimately seized drugs, weapons, ammunition, and cash from "my house," pursuant to a warrant.[118] Mr. Wurie was charged in connection with the items seized.[119] At trial, Mr. Wurie sought to suppress the items obtained during the search of "my house," based on the argument that the items were the fruit of the poisoned search of his flip phone.[120] The district court rejected his argument and he was convicted on all counts and sentenced.[121] The First Circuit reversed the district court's order denying Mr. Wurie's motion and vacated two of his convictions.[122] The First Circuit held that cell phones are different from other objects that people possess, and they hold only a negligible threat to law enforcement.[123] The United States Supreme Court granted certiorari.

In *Riley*, the Court pivoted from its over-forty-year history regarding the search-incident-to-arrest exception to the Fourth Amendment by placing cell phones on a pedestal out of reach from the probable cause standard established by its trilogy of search-incident-to-arrest doctrine:[124] *Chimel v. California*,[125] *United States v. Robinson*,[126] and *Arizona v. Gant*.[127] In those prior cases, officer safety and the destruction of evidence were compelling interests that demanded analysis under the search-incident-to-arrest

---

[113] *Id*.
[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] *Id*.
[118] *Id*. at 381.
[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *Id.*
[123] *Id*.
[124] *Id.* at 382–90 (reviewing search-incident-to-arrest precedent).
[125] Chimel v. California, 395 U.S. 752 (1969).
[126] *Robinson*, 414 U.S. at 218.
[127] Arizona v. Gant, 556 U.S. 332 (2009).

exception, requiring probable cause rather than a warrant when the government's interest was more compelling than the privacy interest of the individual.[128] The Court differentiated the cell phone from the possessions seized in *Robinson* and *Chimel,* stating that the data contained in a cell phone "cannot itself be used as a weapon" against law enforcement or to help the arrestee flee.[129] In the majority opinion, Chief Justice Roberts focused immensely on the difference "in both [a] quantitative and a qualitative sense," between cell phones and other things that could be found on an arrestee.[130] He noted that cell phones have "immense storage capacity," and that they have the capacity to retain "millions of pages of texts, thousands of pictures, or hundreds of videos."[131] The impact of this storage capacity tipped the balance for the Court in favor of privacy over the government's interests. The Court was very concerned with the "types of information," that the "sum of an individual's private life can be reconstructed" by accessing the data on the phone, and that the data on the phone can "date back to purchase of the phone or even earlier."[132] The Court stated that cell phones can provide information on where people have been and what their interests are because of the applications they downloaded to their phones.[133] When viewed holistically, the cell phone reveals much more about a person than even the contents of their home in the Court's view because cell phone contents can reveal "where a person has been" through the data.[134] Cell phones can "just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[135] Chief Justice Roberts took great pains to distinguish cell phones from other items that could be discovered on a person during an arrest. He also acknowledged that the holding in *Riley* will impact law enforcement's ability to investigate and fight crime, but that privacy "comes at a cost."[136] Chief Justice Roberts concluded that the simplest reading of the landmark *Riley* ruling is for police to "get a warrant" "before searching a cell phone

---

[128] *Riley*, 573 U.S. at 384, 388.
[129] *Id.* at 388.
[130] *Id*. at 393.
[131] *Id*. at 393–94.
[132] *Id.* at 394.
[133] *Id*. at 393.
[134] *Id.* at 396.
[135] *Id*. at 401.
[136] *Id*.

seized incident to an arrest."[137] Chief Justice Roberts also left a small space for other exceptions to maneuver without a warrant even though the search-incident-to-arrest exception will not apply to cell phones.[138] Exigent circumstances are a possible exception to the warrant requirement that could still survive post-*Riley*. One could argue that the border-search exception, given the government's interest in keeping contraband from entering the country, is an exception that is exempt from *Riley*'s per se warrant requirement before searching a cell phone.

In trying to reach a decision that balanced the governmental interests and individual privacy, the Court recognized digital data did not trigger the same concerns such as risk to officer safety and destruction of evidence. *Riley* illustrated the Court's concern with safeguarding the Fourth Amendment's privacy right for individuals with the ever-changing technology of the digital age. The implications of *Riley* are that the physical analysis of how much a wallet or a container holds is no longer workable when a little bit of data can reveal so much about a person.

c. *Carpenter v. United States*

If there was only a little hope left for the third-party doctrine after *Jones* and *Riley*, there is much less since the June 2018 opinion led again by Chief Justice Roberts in *Carpenter*. The majority held that the subpoena obtained by the government for several days' worth of Mr. Carpenter's cell site location data was unreasonable.[139] The Court said that an individual has a reasonable expectation of privacy in their cell site location data which tracks a person's "physical movements."[140] It concluded that the government must generally obtain a warrant that is based on probable cause before it can search and seize the cell site location data from cell phone wireless carriers.[141] The significance of *Carpenter* for purposes of this paper is the attention cell phones received again from the Court throughout the majority opinion[142] and how the Court goes against its past precedent on the third-party doctrine from *Smith v. Maryland,* which held that there is no

---

[137] *Id.* at 403.
[138] *Id*. at 401–02.
[139] *Carpenter*, 138 S. Ct. at 2210.
[140] *Id*. at 2217.
[141] *Id*. at 2221.
[142] *See generally id.* at 2206–23.

expectation of privacy in telephone numbers dialed,[143] and *United States v. Miller*, which held that there is no expectation of privacy in financial records held by a bank, in order to reach a more favorable decision for individual privacy.[144] Chief Justice Roberts noted the unique qualities of a cell phone again in *Carpenter*: "Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called 'cell sites.'"[145] The Court seemed troubled by the fact that when a cell phone "connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI),"[146] and this presents a greater privacy concern than other recent cases because cell phones go everywhere their owner goes.[147] Although the majority held that the government's search of the cell site data of Mr. Carpenter was a seizure, the Court expressly said that *Carpenter* is a narrow holding.[148] The Court said that there are circumstances not in front of the Court in this case that would justify bypassing the warrant requirement, possibly leaving the door open for the border-search exception and other exceptions to the Fourth Amendment warrant requirement to survive.[149]

IV. CIRCUIT SPLIT ON DIGITAL DEVICES AT THE BORDER

a. *United States v. Cotterman*

Before *Riley*, whether any level of particularized suspicion is required to conduct searches of digital devices at the border varied across the nation. The Ninth Circuit made the distinction between "routine" and "non-routine" searches in multiple cases.[150] One example comes from *United*

---

[143] Smith v. Maryland, 442 U.S. 735, 741–42 (1979) (rejecting claim that "people in general entertain any actual expectation of privacy in the numbers they dial").

[144] United States v. Miller, 425 U.S. 435, 442–43 (1976) (finding no legitimate expectation of privacy in checks, deposit slips, microfilm copies of such, or information kept in bank records).

[145] *Carpenter*, 138 S. Ct. at 2211.

[146] *Id.*

[147] *Id*. at 2218.

[148] *Id.* at 2220.

[149] *Id*.

[150] *See e.g.*, United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008); United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005).

States v. Cotterman.[151] The Ninth Circuit held that because the border agents had reasonable suspicion that evidence of child pornography was on Mr. Cotterman's laptop, the search was reasonable under the border-search exception to the Fourth Amendment.[152] The Ninth Circuit reversed the district court's order granting Mr. Cotterman's motion to suppress the evidence of child pornography obtained through a forensic search of Mr. Cotterman's laptop when he came back into the United States after traveling to Mexico with his wife on vacation.[153] The ruling in this case indicates that the Ninth Circuit requires reasonable suspicion to conduct a forensic search of a digital device when conducting a border search.[154]

Since *Riley*, results continued to vary across the country regarding whether *Riley*'s holding limits the breadth of the border-search exception. In May of 2018, two circuit courts of appeals took two different approaches to the border-search exception considering *Riley*. Both courts held that a traveler's digital device may be searched without a warrant by border officials, however, their paths diverged regarding the level of suspicion that is required before the search can be conducted.

b. *United States v. Kolsuz*

On May 9, 2018, the Court of Appeals for the Fourth Circuit reached its decision in *United States v. Kolsuz*.[155] This case resulted from Mr. Hamzi Kolsuz's repeated attempts to smuggle firearms parts out of the United States to his native country of Turkey in 2012 and 2013, in violation of federal law.[156] When he re-entered the United States in January 2016 at Washington Dulles Airport, authorities watched him and stood ready to stop him when he departed the country again.[157] Authorities at Dulles asked to search Mr. Kolsuz's luggage for firearms parts when he came through for routine inspection for his flight.[158] An inspection of his belongings revealed Mr. Kolsuz had several firearms parts and he did not have the license

---

[151] *Cotterman*, 709 F.3d at 975–76 (Callahan, J., concurring in-part) (citing *Chaudhry*, 424 F.3d at 1054).

[152] *Id*.

[153] *Id*. at 957, 970.

[154] *See id*. at 986–70.

[155] *Kolsuz*, 890 F.3d at 148.

[156] *Id*. at 138–39.

[157] *Id*. at 139.

[158] *Id*.

required to possess these or take them out of the country.[159] Mr. Kolsuz was brought to a secondary inspection where the agents took his iPhone, which was not locked by a passcode, and conducted a manual search of its contents, looking through his calls and texts.[160] The Customs and Border Protection agents received confirmation through other channels that Mr. Kolsuz did not have a license to export the firearms parts in his possession and they arrested him.[161] Agents then transported his iPhone to a local field office a few miles from the airport and conducted a forensic search of the phone using a "Cellebrite Physical Analyzer."[162] The agents placed the phone in "airplane mode," to prevent the extraction from pulling data from the "cloud," limiting the search to only the data physically stored on the phone.[163]

Mr. Kolsuz was indicted on charges related to his attempts to take firearms parts out of the United States without the proper license.[164] He attempted to suppress the report produced from the forensic search of his iPhone prior to trial, but his motion was denied by the District Court.[165] Mr. Kolsuz attempted to invoke *Riley* by arguing that the forensic search was incident to his arrest and was executed away from the border such that the border-search exception should not apply, requiring the authorities to get a warrant before conducting the more advanced search of his phone.[166] The district court concluded that the forensic search of Mr. Kolsuz's phone was a "nonroutine" border search citing *United States v. Ickes*, where the Fourth Circuit held that a search conducted away from the border and after the suspect is arrested can still be classified as a border search such that the border-search exception applies.[167] The *Kolsuz* court reached the conclusion that a "nonroutine" border search required reasonable suspicion before it could be executed, even though it acknowledged the *Riley* court's holding that "a forensic search of a phone no longer can be analogized to an ordinary search

---

[159] *Id.*
[160] *Id.*
[161] *Id*.
[162] *Id*.
[163] *Id*.
[164] *Id.*
[165] *Id.* at 139–40.
[166] *Id*.
[167] *Id*. at 140 (citing *Ickes*, 393 F.3d at 507).

of luggage or some other container at the border."[168] Still, the district court stated that no other court had ever held that anything more than reasonable suspicion was required during a "nonroutine" border search, and it refused to hold that a "nonroutine" border search required a warrant based on probable cause.[169]

During a bench trial, the district court found Mr. Kolsuz guilty of all three charges.[170] On appeal to the Fourth Circuit, Mr. Kolsuz challenged only the forensic search of his phone and argued that the border-search exception did not apply to that search because he was in custody already, and agents transported his phone miles away from the airport.[171] Reviewing *de novo* only the issue of whether the forensic search of Mr. Kolsuz's phone was lawful under the border-search exception, the Fourth Circuit affirmed the district court.[172] In reaching its holding, the court acknowledged the Supreme Court's discussion of the unique quality of a modern-day cell phone in *Riley*.[173] The Fourth Circuit discussed the distinction between "routine" and "nonroutine" border searches and concluded that, because of the *Riley* holding, a forensic search of a digital phone is a "nonroutine" border search, and therefore requires some form of individualized suspicion.[174] The court also disagreed with Mr. Kolsuz that the border-search exception did not apply.[175] It concluded that "a direct link between the predicate for the search and the rationale for the border exception" applied based on the fact that the purpose of the search was the agent's belief that evidence of Mr. Kolsuz's attempt to transport firearms illegally outside of the United States without a license would be found during the forensic search of his phone.[176] The court also disagreed with Mr. Kolsuz's back-up argument that even if the border-search exception applies, a "nonroutine" border search requires more than reasonable suspicion.[177] The court noted that the Supreme Court had not "delineated precisely what makes a search nonroutine," but stated that pre-

---

[168] *Id*.
[169] *Id*. at 140–41.
[170] *Id.* at 141.
[171] *Id*. at 141–42.
[172] *Id*.
[173] *Id*. at 145–46.
[174] *Id*. at 137–38, 146.
[175] *Id.* at 143.
[176] *Id*.
[177] *Id*. at 144.

Riley case law indicated "a convincing case for categorizing forensic searches of digital devices as nonroutine."[178] In reaching this conclusion, the court relied on holdings from other federal courts to show the trend of requiring reasonable suspicion where forensic searches are performed on digital devices at the border.[179]

The key difference between the Fourth Circuit's decision in *Kolsuz* and the Eleventh Circuit's decision in *Touset*, is that the Fourth Circuit held that *Riley* established precedent that "a forensic search of a digital phone must be treated as a 'nonroutine' border search, requiring some form of individualized suspicion," and that the most any court has required of a "nonroutine" border search is reasonable suspicion, despite the Supreme Court's holding in *Riley*.[180]

If a defendant finds him or herself in the Fourth Circuit, law enforcement agents are required to have reasonable suspicion before they can conduct forensic searches of digital devices. In the Eleventh Circuit, no suspicion is required to search a digital device at the border because the court held in two recent rulings that the border-search exception to the Fourth Amendment protection against unreasonable searches and seizures is not limited by *Riley* distinction of cell phone searches.[181]

c. *United States v. Touset*

Only a few weeks after the Fourth Circuit's *Kolsuz* decision, the Eleventh Circuit ruled in *United States v. Touset*, holding that no suspicion is required for searches of electronic devices.[182] Still, the court reached an alternate holding that the border agents had reasonable suspicion to search Mr. Touset's electronic devices.[183] It distinguished *Riley* as a search-incident-to-arrest case only, therefore having very little influence over a border-search exception case.[184]

---

[178] *Id*. (citing *Cotterman*, 709 F.3d at 963–68).

[179] *Id*. at 145–46 (citing *Cotterman*, 709 F.3d at 964; United States v. Saboonchi, 990 F. Supp. 2d 536, 549–69 (S.D. Md. 2014)).

[180] *Id.* at 146.

[181] *Id.* at 147.

[182] *See e.g.*, *Touset*, 890 F.3d at 1238.

[183] *Id*. at 1237–38.

[184] *Id*. at 1234.

In this case, the Cyber Center of the Department of Homeland Security received notification from the National Center for Missing and Exploited Children that both Xoom and Yahoo suspected a subscriber account to be involved in several purchases of child pornography based on the frequency and destination of certain money transfers.[185] The Cyber Center conducted its own investigation into the tips received from Xoom and Yahoo which revealed that the person conducting these transactions was Karl Touset. Based on its leads, the Cyber Center put an alert out for Mr. Touset's return to the United States through Atlanta International Airport.[186] Inspection of Mr. Touset's luggage revealed multiple digital devices.[187] A Customs and Border Protection agent performed a "manual" search of these devices and did not find any child pornography.[188] The agent returned several devices to Mr. Touset but kept two laptops and two external hard drives.[189] Agents discovered child pornography on the remaining devices pursuant to forensic searches.[190] Agents obtained a warrant to search Mr. Touset's home based on the findings from the forensic searches of his digital devices, and upon executing the warrant, they uncovered even more child pornography and evidence of webcam sessions between Mr. Touset and young girls.[191] Mr. Touset was indicted on multiple counts of receiving, possessing, and transporting child pornography.[192] Before trial, he sought suppression of the evidence obtained from his digital devices as well as the evidence obtained from his home.[193] Mr. Touset's motion was denied.[194] The district court applied the ruling in *Cotterman* and determined that the Customs and Border Protection agents had the necessary reasonable suspicion prior to conducting a forensic search of digital devices at the border.[195]

On appeal from his conviction, the Eleventh Circuit reviewed the district court's ruling on Mr. Touset's suppression motion for clear error

---

185 *Id*. at 1230.
186 *Id*.
187 *Id*.
188 *Id.*
189 *Id*.
190 *Id*.
191 *Id.* at 1230–31.
192 *Id*. at 1231.
193 *Id.*
194 *Id.*
195 *Id.*

regarding the factual findings and *de novo* for the questions of law.[196] First, the Eleventh Circuit tackled the challenge of ruling on the appropriate level of suspicion required before searching a digital device at the border.[197] Second, the court reached an alternative finding that the agents had reasonable suspicion when they searched Mr. Touset's devices.[198]

The Eleventh Circuit concluded that no suspicion is required to conduct a forensic search of a digital device because such a search is not as intrusive as the search of a person.[199] In doing so, the court focused on the difference between the search of people and the search of property.[200] In the Eleventh Circuit, reasonable suspicion is required only "for highly intrusive searches of a person's body," hinging on the level of indignity endured by the person searched.[201] This allowed the court to distinguish from the facts in *Montoya de Hernandez,* where the agents lawfully required, based on reasonable suspicion, Ms. Montoya de Hernandez to pass the contraband in her "alimentary canal."[202] The court also stated that a forensic search of an electronic device does not trigger its intrusive search analysis, requiring reasonable suspicion, because its "precedents do not require suspicion for intrusive searches of any property at the border."[203] The court acknowledged that other circuits such as the Fourth in *Kolsuz* and the Ninth in *Cotterman* held that reasonable suspicion is required for forensic searches of digital devices because of the intrusive nature of engaging in what amounts to a "computer strip search."[204] The court also stated that the Fourth Circuit reached its decision based on classifying a search of property at the border as "routine" or "nonroutine" and explained that this reasoning was faulty because the Supreme Court rejected these classifications in *Flores-Montano*.[205]

Although the Eleventh Circuit is correct in its assessment of the Supreme Court's rejection of "routine" and "nonroutine" distinctions, the

---

196 *Id*.
197 *Id.*
198 *Id.* at 1231–32.
199 *Id.* at 1233.
200 *Id.* at 1233–34.
201 *Id.* at 1234.
202 *Montoya de Hernandez*, 473 U.S. at 544.
203 *Touset*, 890 F.3d at 1234.
204 *Id.*
205 *Id.*

complexity of issues pertaining to searches of electronic devices arguably calls for such a distinction to be made. The Supreme Court also has the option of taking its "other than [] routine" language from *Montoya de Hernandez* and applying it to digital devices.[206] Whether the Supreme Court will recognize the distinction now because of *Riley* and emerging technology remains to be seen. Given the route the Supreme Court took in *Riley*, the Court distinguishes cell phones from other objects because of the amount of private information cell phones can carry. Still, the Eleventh Circuit was "unpersuaded" that *Riley* created a new standard for searches of property at the border.[207] The Eleventh Circuit was also not persuaded by the Fourth and Ninth Circuits' concerns that "travelers have no practical options to protect their privacy when traveling abroad."[208] The Eleventh Circuit precedent dictates that at the border, travelers "are on notice that a search may be made" of their property and though they are unable to leave their "bodies at home," they are free to leave their property at home.[209] In reaching its conclusion that no suspicion is required, the court discussed the fact that the government's interest is at its "zenith" at the border. [210] It noted that to "invent heightened constitutional protection for travelers who cross our borders"[211] with illegal items, would create "special protection for the property most often used to store and disseminate child pornography."[212] The court said that it was a congressional responsibility to create laws that provide more protection and in reaching its conclusion, it was giving Congress the room to create the appropriate standard.[213] Finally, the Eleventh Circuit concluded that in the alternative, the district court correctly denied Mr. Touset's motion to suppress because the agents had reasonable suspicion when they executed the forensic search of his devices.[214]

In summary, if a defendant finds himself or herself in the Fourth Circuit or the Ninth Circuit, law enforcement agents are required to have reasonable suspicion before they can conduct searches of digital devices. In

---

[206] *See Montoya de Hernandez*, 473 U.S. at 540.
[207] *Touset*, 890 F.3d at 1234.
[208] *Id.* at 1235.
[209] *Id.*
[210] *Id.*
[211] *Id.* at 1236.
[212] *Id.* at 1235.
[213] *Id.* at 1236–37.
[214] *Id.* at 1237.

the Eleventh Circuit, no suspicion is required to search a digital device at the border because the Eleventh Circuit held in two recent rulings that the border exception to the Fourth Amendment protection against unreasonable searches and seizures is not limited by *Riley*.[215] The Fourth Circuit's analysis that cell phones require different treatment than other items seems more in line with where the Supreme Court is headed based on *Jones*, *Riley*, and *Carpenter*.

Even at the border where the government's interests typically overcome a traveler's right to individual privacy, the Supreme Court will likely continue to hold the government to a higher standard when it comes to cell phones and potentially other digital devices. At this point, neither circuit is incorrect because the Supreme Court has not yet decided a case implicating the border-search exception and digital devices. If the Supreme Court rules on a case factually similar to *Kolsuz* or *Touset*, it is unlikely that it will rule that no suspicion is required for forensic searches of digital devices even at the border, despite its past rulings on border-search exception cases. An argument can be made that the search in *Montoya de Hernandez* was much more invasive than the forensic search of a digital device, but that is not the direction the Court is headed when it comes to the treatment of digital devices. The Eleventh Circuit made a compelling case for a no suspicion standard when it distinguished the search of a person in *Montoya de Hernandez* from the searches of digital devices, which are property. Despite this persuasive ruling, it is reasonable to conclude that per *Riley*, a cell phone search can be equally as intrusive as requiring Montoya de Hernandez to expel the contraband hidden inside of her body, due to the private information likely stored within.

V. COURTS FAVORABLE TO APPLYING *RILEY* AT THE BORDER

Other courts have struggled in interpreting how *Riley* might apply to the border-search exception when agents conduct a search of digital devices. Although not an exhaustive summary of all cases that applied *Riley*, this section explains how some courts reach the conclusion that *Riley* is binding on searches of digital devices at the border.

---

[215] *Id.* at 1235; United States v. Vergara, 884 F.3d 1309, 1312–13 (2018).

a. *United States v. Kim*

Investigators with the Department of Homeland Security suspected Mr. Kim, the defendant, of violating "export control laws and the trade embargo with Iran."[216] They awaited his arrival at Los Angeles International Airport because he was departing for his native country, so they could search his belongings and, hopefully, find evidence of the crimes they believed he committed.[217] The Special Agent eventually took possession of the defendant's laptop and had it transported to a lab in San Diego in order to create a digital copy of the defendant's hard drive.[218] The copy of the defendant's hard drive and subsequent use of various programs and keyword searches within the files revealed information that led to the charges against the defendant.[219] The U.S. District for the District of Columbia held that the warrantless search of the defendant's laptop computer was unreasonable and violated the Fourth Amendment.[220] The government argued that the search occurred at the border. However, the court disagreed and concluded that this was more like a "nonborder search," which requires a warrant based upon probable cause.[221] The court also rejected the government's argument that a cell phone is like a container and discussed the *Riley* majority's definition of the difference between a cell phone (and other digital devices) and other types of property.[222] In reaching its conclusion regarding reasonableness, the court applied *Riley* as well as the border-search exception cases.[223] The court's reasoning for applying *Riley* was that *Riley* dealt with a search of a digital device and, in *Ramsey*, the court said that searches incident to arrest are comparable to border searches.[224]

b. *Alasaad v. Nielsen*

Although not a criminal case, the U.S. District Court in Massachusetts discussed *Riley* in the context of border-searches in its decision covering a lawsuit against the Secretary of the Department of Homeland Security

---

[216] United States v. Kim, 103 F. Supp. 3d 32, 34 (D.C. 2015).
[217] *Id*. at 38–39.
[218] *Id*. at 39–40.
[219] *See id*. at 41.
[220] *See id.* at 59.
[221] *Id.* at 58 (citing *United States v. Brennan*, 538 F.2d 711, 716 (5th Cir. 1976)).
[222] *Id.* at 56.
[223] *Id*.
[224] *Id*. at 55.

and it held that *Riley* applies to border-searches at least to some degree.[225] The court stated that *Riley* must have "some persuasive weight," because the Supreme Court compared the border-search exception to the search-incident-to-arrest exception in *Ramsey*, calling them "similar."[226] The court also advocated for applying *Riley* because both the border-search exception and the search-incident-to-arrest exception have historic roots in "English and American law."[227] In deciding whether *Riley*'s warrant requirement was controlling in the case before them, the court concluded that it could not "rule that this Fourth Amendment principle," from *Riley*, "would not extend in some capacity at the border."[228] In the absence of a Supreme Court case that deals with the border exception and digital devices, courts attempt to predict how the Court would approach the issue. Moreover, as demonstrated in the next section, the results vary from court to court. These two cases show that even though the Supreme Court in *Riley* examined cell phones in the context of a search incident to an arrest, the border-search exception may not be outside *Riley*'s reach.

VI. COURTS THAT DID NOT EXTEND *RILEY* AT THE BORDER

Whether *Riley* controls how courts should interpret searches of digital devices at the border remains disputed. This section provides examples of a few cases, although there are many more, where courts rejected *Riley* as controlling. These federal courts' opinions were issued after *Riley*, and thus took *Riley* into account in their holdings.

a. *United States v. Caballero*

This case is significant because the U.S. District Court for the Southern District of California held that it was bound by the Ninth Circuit's decision in *United States v. Cotterman*, not the Supreme Court's *Riley* decision because the government's search was conducted at the border.[229] Defendant Caballero drove his car from Mexico to Calexico, California, a United States Port of Entry.[230] Customs and Border Protection agents

---

[225] Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *21 (D. Mass. May 5, 2018).

[226] *Id*. at *16.

[227] *Id*. at *18 (quoting *Riley*, 573 U.S. at 382).

[228] *Id*. at *20.

[229] United States v. Caballero, 178 F.Supp.3d 1008, 1012 (S.D. Cal. 2016).

[230] *Id*. at 1011.

searched his car and discovered illegal drugs and he was subsequently arrested.[231] An agent conducted a manual search of his cell phone during his questioning several hours after his arrest.[232] The defendant argued the evidence seized from his phone, a photo of a great deal of money, should be suppressed as the product of an illegal search pursuant to *Riley*.[233]

The court accepted that it stood at an intersection between the Ninth Circuit's holding in *Cotterman* and the Supreme Court's holding in *Riley*, discussed the potential application of each, and reached the conclusion that it was bound by *Cotterman*, not *Riley*.[234] Its justification is that the facts of the case before it fell within the border-search exception, not the search-incident-to-arrest exception that the facts of *Riley* discussed.[235] The court said that *Riley* did not cover the border-search exception and recognized the most recent Supreme Court case involving the border-search exception, *Flores-Montano*, in which the Court held that the government's interest is "at its zenith at the international border," and "'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'"[236] The court argued that no other court found *Riley* and *Cotterman* to be "clearly irreconcilable," citing several cases within the Ninth Circuit as well as others that reached the conclusion that *Riley* does not control searches performed pursuant to the border-search exception.[237] "In order for this [c]ourt to disregard *Cotterman*, *Riley* would need to be 'clearly inconsistent' with the prior circuit precedent."[238] Although the district court stated it preferred to apply *Riley*,[239] it was bound by the Ninth Circuit's ruling on the border-search exception, applied *Cotterman*, and held that because the "agents conducted a cursory search," [240] of the cell phone rather than an extensive

---

231 *Id*.
232 *Id*.
233 *Id*. at 1012.
234 *Id.* at 1014.
235 *Id*.
236 *Id*.
237 *Id*. at 1018–19.
238 *Id*. at 1020 (quoting Lair v. Bullock, 687 F.3d 1200, 1207 (9th Cir. 2012)) (capitalization removed).
239 *Id.* at 1017.
240 *Id*. at 1014.

forensic search, "[N]either a warrant nor reasonable suspicion" are required.[241] Consequently, the defendant's motion to suppress was denied.[242] Although the court wanted to apply *Riley* out of the belief that digital devices are different than other property, the court interpreted case law within its circuit to be controlling.[243]

b. *United States v. Feiten*

In an unreported opinion, the U.S. District Court for the Eastern District of Michigan held that *Riley* does not trump previous Sixth Circuit rulings regarding searches at the border, nor does *Riley* limit the Supreme Court's own rulings regarding reasonableness of searches at the border.[244] In *United States v. Feiten*, the court denied the defendant's motion to suppress and held that all three searches of the defendant's laptop were lawful: the initial search with the defendant's consent, the subsequent "more extensive search" using "OS Triage" software, and the final forensic search, all of which were performed at the border.[245]

This case begins when the defendant traveled by plane from Cancun, Mexico to Detroit and caught the attention of the Customs Officers who noted that the defendant acted in a nervous manner.[246] They sent the defendant on for a secondary inspection and gained his consent to search his electronic devices.[247] It was during the secondary inspection that the Customs Officer discovered what appeared to be child erotica on the defendant's laptop.[248] The officer stopped the search and contacted a United States Customs and Border Protection Agent who specialized in child pornography.[249] The specially trained Special Agent attempted using OS Triage software on the defendant's laptop while at the airport.[250] Due to technical difficulties with the software, the Officer had to take the laptop to an office many miles

---

241 *Id.* at 1020.
242 *Id*.
243 *Id*.
244 United States v. Feiten, No. 15-20631, 2016 WL 894452, at *7–8, (E.D. Mich. Mar. 9, 2016).
245 *Id*. at *1–2.
246 *Id*. at *1.
247 *Id*.
248 *Id*.
249 *Id*.
250 *Id.*

from the airport.[251] A search using OS Triage revealed 178 verified images of child pornography.[252] The laptop was turned over to a forensic analyst who performed a "full forensic examination," which yielded 446 more images of child pornography, bringing the total to 624 child pornography images on the defendant's laptop.[253] The court held that each of the three searches were performed at the border "or its functional equivalent."[254]

The district court rejected the defendant's argument that *Riley* controls and therefore, the warrantless searches performed on his laptop were unreasonable and violated the Fourth Amendment, because of Sixth Circuit and Supreme Court precedent placing the government's interest at its "zenith" at the border.[255] The district court also held that *Riley* did not create a "blanket rule applicable to any data search of any electronic device in any context."[256] In finding that *Riley* does not control searches at the border, the district court discussed the many times the Supreme Court recognized the importance of the government's interest in preventing contraband from entering the country.[257] Additionally, the court rejected the defendant's argument that *Riley* means that cell phones and electronic devices should be treated differently, even at the border.[258] The court said, "Laptops and cell phones are indeed becoming quantitatively, and perhaps qualitatively, different from other items, but that simply means there is more room to hide digital contraband, and therefore more storage space that must be searched."[259] The court acknowledged that the Sixth Circuit and the Supreme Court placed the standard for "highly intrusive searches . . . carried out in a 'particularly offensive manner'" at the reasonable suspicion level.[260] The court concluded that the first two searches were reasonable warrantless searches and that the third, most intrusive search, was also permissible because it was done with reasonable suspicion.[261] The ruling in this

---

[251] *Id*. at *2.
[252] *Id*.
[253] *Id*.
[254] *Id*.
[255] *Id*.
[256] *Id*. at *4.
[257] *Id*. at *5.
[258] *Id*. at *5–6.
[259] *Id*. at *5.
[260] *Id.* at *6.
[261] *Id*. at *6–7.

case suggests that the reasonableness of a border search hinges on the intrusiveness of the search. It also shows again that courts are unwilling to jump to the conclusion that *Riley* constrains the border-search exception into an exception that looks like searches incident to arrest.

c. *United States v. Molina-Isidoro*

Ms. Maria Isabel Molina-Isidoro asked the Fifth Circuit to extend the principles of *Riley* to the border-search exception and suppress the evidence obtained from a warrantless search of her cell phone at the United States border located in El Paso, Texas.[262] During the inspection of her suitcase as she attempted to cross the border, an officer noticed that part of the interior of her suitcase had been altered and after scanning with the X-ray again, they discovered a hidden compartment concealed by electrical tape.[263] Officers discovered a "white crystal substance" in the hidden compartment and their drug detection dog smelled drugs.[264] Tests of the substance confirmed that the substance was methamphetamine.[265] Department of Homeland Security agents arrived to question the defendant and her story seemed senseless and disjointed.[266] For example, she could not remember the address of the brother she allegedly just came from visiting in Juarez.[267] When the agents confronted Ms. Molina-Isidoro with their opinion that her story was nonsensical, she concluded the questioning and asked for an attorney.[268] "Either at that point, or during the questioning," the agents searched the defendant's apps on her phone, which included the Uber and WhatsApp applications, and did so without her consent.[269] The agents found a conversation on her WhatsApp application that indicated that, among other things, "[S]he got the stuff and was headed back to El Paso."[270] Ms. Molina-Isidoro was indicted on drug possession charges.[271]

---

[262] *Molina-Isidoro*, 884 F.3d at 289.
[263] *Id*.
[264] *Id*.
[265] *Id*.
[266] *Id*.
[267] *Id*.
[268] *Id*.
[269] *Id.*
[270] *Id*. at 290.
[271] *Id*.

Before trial, she filed a motion to suppress the evidence taken from the search of her cell phone.[272] The district court held *Riley* did not apply to border searches of cell phones and denied her motion.[273] Ms. Molina-Isidoro was convicted and sentenced at a stipulated bench trial.[274] Her appeal was preserved and made it to the Fifth Circuit.[275] The majority opinion analyzed her motion to suppress and held that the good-faith exception applied and affirmed her conviction and the denial of her motion to suppress.[276] Still, the Fifth Circuit discussed its take on whether *Riley* controls the border-search exception and reached the conclusion that "it is reasonable for government agents" to believe that *Riley* does not swallow "the caselaw allowing warrantless border searches of cell phones."[277] The Fifth Circuit supported its conclusion with the fact that no other court decision since *Riley* ruled that a warrant is required for border searches of digital devices and Professor LaFave's doubts that *Riley* will wipe away the historic warrantless border-search exception entirely.[278]

These cases illustrate how most district courts across the country conduct their analyses regarding searches of electronic devices under the border-search exception even after *Riley*. Courts still see the overwhelming government interest in keeping illegal things and people out of the country as weightier than an individual's privacy interest. Courts also seem reluctant to decide a heightened standard of suspicion in the absence of legislation or a Supreme Court ruling

VII. FACTORING IN THE CURRENT SUPREME COURT JUSTICES

The Supreme Court's composition is different since the last time it decided a border-search exception case in 2004. Chief Justice Rehnquist authored the last three seminal border-search exception cases and his approach is likely very different than that of his successor, Justice Roberts, who led the majority in *Riley* and *Carpenter*. There are three remaining justices on the current Court who participated in *Flores-Montano* the last

---

[272] *Id*.
[273] *Id*.
[274] *Id.*
[275] *See generally id*.
[276] *Id.* at 290, 293.
[277] *Id.* at 292.
[278] *Id*.

border-search exception case. Justices Thomas, Ginsburg, and Breyer, all three of whom voted with the majority in *Riley*.

The only justices on the current Court who did not participate in *Riley* are Justices Gorsuch and Kavanaugh. Justice Gorsuch's dissent in *Carpenter* suggests that he believes in abandoning the third party doctrine created by *Smith* and *Miller*.[279] He also argued that "cell-site data could qualify as [a person's] papers or effects under existing law" and that, "Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right."[280]

It is difficult to draw a direct analogy between Justice Gorsuch's dissent and how he might rule on a border-search exception case. Unfortunately, there does not seem to be any evidence from Justice Kavanaugh's time on the D.C. Circuit to hint where his analysis would land. The majority opinions in *Jones*, *Riley*, and *Carpenter* suggest the Court is willing to depart or distinguish from precedent and find in favor of individual privacy.

VIII. CONCLUSION

Judge Gregg Costa of the Fifth Circuit argued in his concurring opinion in *Molina-Isidoro* that the ability of law enforcement to find physical contraband such as illegal drugs is the greatest justification for the border-search exception.[281] Because drugs do not fit inside the "data of a cell phone," Judge Costa pointed out, the government's interest in searching a cell phone is not necessarily at its zenith.[282] Still, he accepted that one way the warrantless or even suspicionless border-search exception survives the digital age is that the Supreme Court held in *Montoya de Hernandez* that "expectation of privacy [is] less at the border than in the interior."[283] Judge Costa's concurring opinion made several points not discussed by the majority in *Molina-Isidoro* that could be important in future discussions regarding digital devices and border searches. He noted that the Department of

---

[279] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) ("I do not agree with the Court's decision today to keep *Smith* and *Miller* on life-support . . . .").

[280] *Id*. at 2272 (Gorsuch, J., dissenting).

[281] *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., concurring).

[282] *Id*. (Costa, J., concurring).

[283] *Id*. at 295–96. (Costa, J., concurring) (quoting *Montoya de Hernandez*, 473 U.S. at 539–40).

Homeland Security changed its policy regarding border searches of digital devices in 2018, reflecting the ever-evolving law of digital devices.[284] Judge Costa's treatment of a cell phone and emerging digital technology seems in line with the majority's opinions in *Jones*, *Riley*, and *Carpenter*.

Even post-*Riley*, most federal courts resolved the disputed standard of whether reasonable suspicion or no suspicion is required in the conduct of more advanced or "nonroutine" searches of electronic devices when individuals are crossing the United States border in favor of some level of suspicion. The Court stated in its last two border-search exception cases (*Montoya de Hernandez* and *Flores-Montano*) that either reasonable suspicion is required for "other than routine" searches or, when the search of property is so "destructive,"[285] a different result than *Flores-Montano*'s no suspicion required may be necessary.[286] The Eleventh Circuit's decision in *Touset* still honors the historic authority given to border officials to keep the United States safe through the alternative finding that the border official had reasonable suspicion before conducting the search at issue.[287] However, the Fourth Circuit in *Kolsuz* and the Ninth Circuit in *Cotterman*, took the next logical step by holding that *Riley* extends to the border by requiring reasonable suspicion for more intrusive searches. A reasonable suspicion requirement for forensic search of a digital device at the border would match with both the precedent set for "other than routine searches" in *Montoya de Hernandez* and fit within Court's recent trend of favoring privacy when it comes to emerging technology over the government's interest in *Jones*, *Riley*, and *Carpenter*. While the Eleventh Circuit was correct that the Supreme Court rejected drawing a distinction between different types of searches in *Montoya de Hernandez*, the Court's decision in *Riley* appears to signal that the Court has become concerned that the law is not keeping up with technology to the detriment of individual privacy.

When and if the Supreme Court weighs in on searches and seizures of digital devices pursuant to the border-search exception, the Court will have to choose between sticking to its line of cases such as *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano*, or it will have to abandon or distinguish those cases if it chooses to stretch the approach taken in *Riley* and

---

[284] *Id*. at 294 (Costa, J., concurring).

[285] *Flores-Montano*, 541 U.S. at 156.

[286] *Id.*; *Montoya de Hernandez*, 473 U.S. at 541.

[287] *Touset*, 890 F.3d at 1237.

tell border officials they need a warrant to search a cell phone. When reading *Jones*, *Riley*, and *Carpenter* together, it is reasonable to conclude that the Supreme Court might be discontent with the political branches lack of action on privacy and digital devices and could come down in favor of individual privacy at the border. The Court certainly has the option to stick to its *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano* roots and distinguish *Riley*'s exception for searches incident to arrest from the border-search exception, holding, at most, that reasonable suspicion is required to conduct an "advanced"[288] or an "other than routine" search [289] of a digital device. The history of the border-search exception should lead the Court towards that result because the government's interest in protecting the nation is different and stronger at the border.

The Court also left room in *Riley* for other exceptions to the warrant requirement before searching cell phones.[290] The Court could find that the border-search exception falls within the category of exceptions that are distinguishable from *Riley,* and the Court could rule in a manner consistent with the Eleventh Circuit by holding that no suspicion is required before searching digital devices. Still, it is more likely that the Court will change its approach to the border-search exception based on its concern for individual privacy in the digital era. This prediction is backed up by the fact that in one of the seminal border-exception cases, *Ramsey*, the Court compared the border-search exception to searches incident to arrest.[291] The Court in *Riley* shifted away from its previous position on searches of property incident to arrest, which was a position it had held for over forty years.[292] If given the opportunity, this current Court will likely shift away from the anything-goes level of suspicion required to conduct searches at the border and apply at least a reasonable suspicion standard to digital devices. The Court will likely either choose to follow federal courts below it and start distinguishing between routine and nonroutine searches at the border, or it will take its own "other than routine" language and mold it to fit the case that eventually gets in front of them. The challenges and concerns

---

[288] U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, *supra* note 85, at 5.

[289] *Montoya de Hernandez*, 473 U.S. at 540.

[290] *Riley*, 573 U.S. at 401–02.

[291] *Ramsey*, 431 U.S. at 621.

[292] *Riley*, 573 U.S. at 382–85 (citing *Chimel*, 395 U.S. at 762–63; *Robinson*, 414 U.S. at 235–36; *Gant*, 556 U.S. at 343).

associated with how much access the government can have to a person's life and privacy demand such distinctions in the law.

ASBESTOS AND ADDITIVE MANUFACTURING: ADDRESSING EARLY CONCERNS SURROUNDING MANUFACTURING 3D-PRINTING TECHNOLOGY USING ASBESTOS AS A LITIGATION MODEL

Corban Snider*

TABLE OF CONTENTS

* The author is a 2020 Juris Doctor Candidate at the University of Mississippi School of Law, a member of the Moot Court Board, and serves as both the Executive Notes and Comments Editor and an Associate Cases Editor for Volume 89 of the *Mississippi Law Journal*. He graduated from Mississippi State University with a Bachelor of Science in Biochemistry & Molecular Biology in May 2017. The author wishes to thank the following: Chris Steere, Zack Donnelly, Taylor Bush, Logan Coney, Marcus King, Jack Lantrip, Meghan Tanaka, Brandon Wilson, Jordan Gasc, and Robert Loper. Most importantly, he would like to thank his wife, Murphy, for her unwavering and unconditional love, support, and friendship.

I. INTRODUCTION

> *It's so difficult, isn't it? To see what's going on when you're in the absolute middle of something? It's only with hindsight we can see things for what they are.*[1]

Here we stand, at the very precipice of the next asbestos litigation crisis,[2] and we have critical decisions to make. Will we reproduce the mistakes of the past, subjecting millions of Americans to the medical and financial uncertainty that accompanies latent-disease litigation?[3] Or, will we instead take steps to prevent the causes of latent diseases, to simplify the laws surrounding latent-disease litigation, and to provide both plaintiffs and defendants with fast, efficient, and predictable outcomes? This Article addresses how industrial additive manufacturing, colloquially known as "3D printing," may trigger the new generation of latent-disease litigation. Further, this Article highlights key issues in asbestos litigation that require substantial clarification to operate effectively in the industrial 3D-printing context.

Asbestos, once thought to be a magical material,[4] quickly rose to prominence after the Industrial Revolution.[5] Lauded for its low flammability and high tensile strength, manufacturers across numerous industries used asbestos in everyday products including insulation and automobiles.[6] Although previously unknown or ignored during asbestos's rise, today it is well-known that there are severe health implications of exposure to asbestos. The miniscule asbestos fibers have been labeled as a cause of several diseases, namely asbestosis, lung cancer, and, perhaps most notably, mesothelioma.[7]

---

[1] S.J. WATSON, BEFORE I GO TO SLEEP 266 (2011).

[2] James L. Stengel, *The Asbestos End-Game*, 62 N.Y.U. ANN. SURV. AM. L. 223 (2006); *see also* Victor E. Schwartz, *A Letter to the Nation's Trial Judges: Asbestos Litigation, Major Progress Made over the Past Decade and Hurdles You Can Vault in the Next*, 36 AM. J. TRIAL ADVOC. 1 (2012) (asserting that asbestos litigation had reached "crisis proportions" around the year 2000).

[3] Francis E. McGovern, *The Tragedy of the Asbestos Commons*, 88 VA. L. REV. 1721, 1725 (2002).

[4] Daniel King, *History of Asbestos*, THE MESOTHELIOMA CENTER (Aug. 8, 2019), https://www.asbestos.com/asbestos/history/.

[5] *Id*.

[6] *Id*; *see also* Stengel, *supra* note 2, at 226–27 (discussing the growth in the use of asbestos across various industries).

[7] *See* Daniel J. Penofsky, *Asbestos Injury Litigation*, 60 AM. JUR. TRIALS 73, § 1 (2018).

Similar to the rise of asbestos, 3D-printing technologies are rapidly growing in popularity[8] and have already garnered the label of miracle-maker.[9] Perhaps to a much larger degree, 3D printing has the potential to forever change the world's manufacturing landscape.[10] However, 3D printing is not without its concerns, and those concerns may mirror the same risks posed by asbestos exposure. Notably, 3D printers can be categorized as "high emitters" of ultra-fine particles, or particles small enough to penetrate the lungs and reach the bloodstream.[11] Many of these particles come from known or suspected carcinogens which, in time, can lead to the development of various cancers.[12]

However, because the diseases in these contexts do not manifest until years and sometimes decades later, unique and difficult issues have arisen in these latent-disease cases.[13] Among those difficulties are two issues that plague both plaintiffs and defendants alike: identifying the true party at fault[14] and applying a proper standard in establishing causation.[15]

In Part II, this Article will fully illustrate the similarities between the rise of asbestos and the present ascension of 3D printing in manufacturing contexts. Additionally, it will explore the latent dangers of both asbestos

---

[8] Thomas Campbell et al., *Could 3D Printing Change the World? Technologies, Potential, and Implications of Additive Manufacturing*, STRATEGIC FORESIGHT REPORT, (The Atl. Council of the U.S., D.C.), Oct. 2011, at 9, http://www.cbpp.uaa.alaska.edu/afef/Additive%20MFG%20.pdf.

[9] Beth Stackpole, *3D Printing: The Next Medical Miracle?*, DIGITAL ENGINEERING 247 (May 1, 2015), https://www.digitalengineering247.com/article/3d-printing-the-next-medical-miracle/.

[10] Joel Fyke et al., *Searching For a Predictable Liability Regime: Direct-to-Consumer 3D Printing Protection*, 58 NO. 11 DRI FOR DEF. 45 (2016) (stating "[t]he potential for 3D printing, formally known as additive manufacturing, to forever change traditional manufacturing processes has been well documented"); *see also* Barack Obama, President, United States of America, State of the Union Address, (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address (stating that "3D printing . . . has the potential to revolutionize the way we make almost everything").

[11] *See 3D Printer Safety – Pollution and Their Health Risks*, BOX3D (Nov. 1, 2017), https://box3d.eu/3d-printing-safety-pollution-health/.

[12] *See id*.

[13] *See generally* Donald G. Gifford, *The Peculiar Challenges Posed by Latent Diseases Resulting from Mass Products*, 64 MD. L. REV. 613, 613 (2005).

[14] *Id*. at 653–54.

[15] *Id*. at 688–89.

and 3D printing to give the reader a more complete understanding of the parallel risks that arise in each context.

Part III will explore two key issues affecting plaintiffs and defendants: identifying the party at fault and establishing a proper causation standard. This section will also highlight how these issues have created critical problems in asbestos litigation.

Part IV will then illustrate why those two issues are likely to arise in litigation involving industrial 3D printing. This section will further provide suggestions that help clarify the law surrounding these issues and allow for a more efficient and fair assessment of both causation and liability in the 3D-printing context.

Finally, Part V will outline other potential issues that are presented by the rise in 3D printing.

II. OVERVIEW OF ASBESTOS AND 3D-PRINTING

The rise of asbestos before, during, and after the Industrial Revolution and the current emergence of industrial-based 3D printing share a startling number of parallel themes. Ultimately, the similarities in emergence, widespread adoption, and long-term exposure-related risks are the factors that make asbestos litigation a proper model for analyzing and solving future problems in the industrial 3D-printing context. It is critical, then, to explore the development of each respectively.

a. Asbestos: An Overview

Asbestos is a naturally occurring mineral that has been in use for approximately 10,000 years.[16] In ancient times, potters and alchemists alike noticed the heat-resistant nature of asbestos as well as its ability to seemingly improve various products in every way imaginable.[17] Indeed,

---

[16] King, *supra* note 4.

[17] *Id.* (stating that "[i]t is believed that as early as 4000 B.C., asbestos' long hair-like fibers were used for wicks in lamps and candles. Between 2000–3000 B.C., embalmed bodies of Egyptian pharaohs were wrapped in asbestos cloth to protect the bodies from deterioration. In Finland, clay pots dating back to 2500 B.C. contained asbestos fibers, which are believed to strengthen the pots and make them resistant to fire. Around 456 B.C., Herodotus, the classical Greek historian, referred to the use of asbestos shrouds wrapped around the dead before their bodies were tossed onto the funeral pyre to prevent their ashes from being mixed with those of the fire itself.").

asbestos-woven materials were used in varying context throughout history to contain fire.[18]

Asbestos was used throughout the Middle Ages, by the likes of King Charlemagne and Russia's Peter the Great.[19] Charlemagne used asbestos for tablecloths to prevent fires at large feasts, but asbestos ultimately found its way into numerous medieval contexts—even war.[20] It is evident that the ability of asbestos to be used in a myriad of products had been recognized even in ancient times.

The versatility of asbestos became its greatest asset during the Industrial Revolution, as demand for the material skyrocketed.[21] Once the mid-to-late 1800s arrived, worldwide demand grew from steady to explosive.[22] By the twentieth century, asbestos was widely used across several industries as insulation for buildings, steam engines, turbines, and electrical generators, among other applications.[23]

However, throughout asbestos's history, the negative effects of its use and exposure thereto have been extensively noted. Strabo, a Greek geographer, and Pliny the Elder, a Roman historian and naturalist, spoke of a "disease of slaves" among enslaved persons who worked with or around asbestos-containing materials.[24] Both men also described the disease as a "sickness of the lungs"[25] and discussed how some slaves would use a thin

---

[18] *Id.*

[19] *Id*.

[20] *Id.* ("By the end of the first millennium, cremation cloths, mats and wicks for temple lamps were fashioned from chrysotile asbestos from Cyprus and tremolite asbestos from northern Italy. In 1095, the French, German and Italian knights who fought in the First Crusade used a catapult, called a trebuchet, to fling flaming bags of pitch and tar wrapped in asbestos bags over city walls during their sieges. In 1280, Marco Polo wrote about clothing made by the Mongolians from a 'fabric which would not burn'").

[21] King, *supra* note 4.

[22] *Id.*

[23] *Id.*; Paul D. Carrington, *Asbestos Lessons: The Unattended Consequences of Asbestos Litigation*, 26 REV. OF LITIG. 583, 585 (2007) ("In 1931, a technique was developed for mixing the [asbestos] in cement. It came to be used in brake linings that might overheat. And it was also widely used to cover pipes used to transmit heated air or fluids."). For a longer list of the uses of asbestos see *Fact Sheet: Asbestos*, UNIV. OF KY. OCCUPATIONAL HEALTH & SAFETY, https://ehs.uky.edu/ohs/fs_asbestos.php (last visited Jan. 16, 2010).

[24] *Earliest Known Facts About Asbestos*, UNIV. OF MONT. ETHICS & ENVTL. HEALTH, http://www.umt.edu/bioethics/libbyhealth/introduction/background/asbestos_timeline.aspx (last visited Jan. 16, 2020); King, *supra* note 4.

[25] King, *supra* note 4.

membrane from the bladder of a goat or lamb as a make-shift respirator to protect them from inhalation of the fibers.[26] In the early twentieth century, Dr. Montague Murray became the first physician to report a case of asbestosis.[27] As of the 1930s, executives of the major manufacturers using asbestos, such as Johns-Manville Corp., were likely aware of the risks to workers exposed to the material.[28]

Initially, the fears surrounding asbestos exposure were stifled by a belief that the only people at risk of coming in contact with dangerous levels of asbestos were people exposed in occupational contexts.[29] However, it would become clear over the coming decades that asbestos fibers were somewhat ubiquitous[30] and that millions of people had been exposed to asbestos.[31] As a result, those millions of people were all at an increased risk

---

[26] *Id*.

[27] Richard A. Lemen, *Challenge for the 21st Century – A Global Ban On Asbestos*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.5820&rep=rep1&type=pdf.

[28] Carrington, *supra* note 23, at 585.

[29] Penofsky, *supra* note 7, at § 1 ("It was once thought that only asbestos miners, shipyard workers, and pipe fitters were in danger, because of their occupations, of coming into contact with dangerous levels of asbestos fibers").

[30] *Id*. ("However, it is now known that asbestos fibers are a ubiquitous pollutant of the air we breathe, the food we eat, and the water we drink. According to Laurence Malloy, a New York-based asbestos investigator, asbestos fibers are in the air throughout the U.S. and we breathe them in on a daily basis without realizing it. Consider, for example, that every single time an automobile or train applies its brakes, thousands of potentially lethal asbestos fibers from the brake linings are released into the atmosphere. Every time there is an unskilled effort to remove or abate asbestos from a building—a dangerous process that involves ripping and scraping asbestos fibers from a building's superstructure—hundreds of thousands of asbestos fibers may be released. It is estimated that significant amounts of asbestos are present in 20% of all U.S. public and commercial buildings, a total of 733,000 structures. At present, there is considerable debate as to the true hazard of the millions of tons of such "in place" asbestos. Every time there is a rainfall or windstorm, there is an erosion of asbestos fibers from asbestos mining sites. As a result of this activity, it is estimated that the typical American breathes in, unwittingly, about one million asbestos fibers a year.").

[31] Gifford, *supra* note 13, at 620 ("Millions of people were exposed to asbestos dust generated, for example, by insulation materials").

of developing asbestosis, mesothelioma,[32] and other cancers and lung conditions.[33]

At this point, it is critical to discuss exactly how asbestos fibers cause this catastrophic harm. This explanation will be integral to understanding why asbestos is a proper model for the problems facing industrial 3D printing. Ultimately, both products are fraught with risks due to the particulate nature of their dangerous components.

Dangerous exposure to asbestos, whether occupational or otherwise,[34] usually results from the inhalation of asbestos fibers.[35] Asbestos fibers can be "hundreds of times thinner than a human hair"[36] and, after entering the body through inhalation, can become lodged in the pleura.[37] These fibers, after some time, can cause inflammation, scarring, and genetic

---

[32] Curtis W. Noonan, *Environmental Asbestos Exposure and Risk of Mesothelioma*, 5 ANNALS TRANSLATIONAL MED. 1, 1 (2017) ("Malignant mesothelioma is an aggressive form of cancer that typically originates in the pleural but can also occur in the peritoneum, pericardium and around the testes. Asbestos exposure is the only established risk factor known to be causally related to mesothelioma.").

[33] Gifford, *supra* note 13, at 620–21 ("The inhalation of asbestos fibers causes diseases ranging from asbestosis, a lung disease resulting in the destruction of air sacs in the lung, to mesothelioma and other lung cancers. Medical research had begun to reveal the health hazards resulting from exposure to asbestos by the early decades of the twentieth century. Manufacturers of asbestos products not only failed to warn consumers of these hazards, but also actively concealed the risks of exposure to asbestos by, among other means, altering and censoring research results.").

[34] *See* Noonan, *supra* note 32, at 2 (describing para-occupational exposure to asbestos stating that "[t]he term para-occupational exposure refers to an asbestos exposed worker serving as a vector for the transport of fibers to the household setting.").

[35] Kristina Luus, *Asbestos: Mining Exposure, Health Effects and Policy Implications*, 10 MCGILL J. MED. 121, 122 (2007) ("Exposure to asbestos fibres occurs through ingestion, skin contact or inhalation. Inhalation of asbestos fibres is dangerous and results in asbestos related diseases. Skin contact with raw asbestos fibres results in relatively harmless epidermal overgrowth. Ingestion of water from asbestos-contaminated pipes has not been found to increase the incidence of asbestos-related diseases.").

[36] *Causes of Mesothelioma*, MESOTHELIOMA GRP. (last visited Dec. 30, 2019), https://www.mesotheliomagroup.com/mesothelioma/causes/.

[37] *Id.* ("After inhalation, roughly two-thirds of the fibers are breathed out from the body. Some fibers remain and become lodged in the lining of the lungs (the pleura), abdominal cavity (the peritoneum) or heart (pericardium).").

changes that lead to the development of mesothelioma along with other cancers and lung conditions.[38]

Another crucial attribute of asbestos is the existence of multiple strains of asbestos, each of which possibly have a different effect on those exposed. Asbestos fibers can be categorized as either chrysotile or amphibole.[39] The amphibole category can be divided into five sub-strains, named actinolite, amosite, anthophyllite, crocidolite, and tremolite.[40] While many studies indicate that all forms of asbestos are equally dangerous,[41] some studies indicate and some organizations maintain that the chrysotile form of asbestos is safer than the amphibole forms.[42] Despite the lingering belief that some forms of asbestos may be safe enough for use, many countries around the globe have banned asbestos entirely, suggesting that there is no way to safely use the material.[43]

---

[38] *Id*. (Additionally, while research has not yet revealed how exactly the fibers cause the requisite genetic changes to produce mesothelioma, a few theories exist such as: "(1)The microscopic size and needle-like shape of asbestos could prevent cells in the immune system from clearing the fibers out. Cells in the mesothelial lining then absorb the fibers, which in turn interfere with normal cellular division; (2) Inhaled fibers irritate mesothelial cells, causing them to swell. This results in cellular damage and tumor development; (3) Asbestos fibers may influence the production of molecules that damage DNA and disrupt cellular reproduction. This damage leads to the production of tumors; (4) Asbestos fibers may also influence the production of proteins that can mutate regular mesothelial cells into tumor cells.") (numerals and semi-colons added); *see also* Piero Mustacchi, *Lung Cancer Latency and Asbestos Liability*, 17(2) J. LEGAL MED. 277, 278 (1996).

[39] *See* IARC MONOGRAPHS ON THE EVALUATION OF CARCINOGENIC RISKS TO HUMANS, INT'L AGENCY FOR RESEARCH ON CANCER, WORLD HEALTH ORG., ARSENIC, METALS, FIBRES, AND DUSTS: A REVIEW OF HUMAN CARCINOGENS 219 (2012), https://www.ncbi.nlm.nih.gov/books/NBK304374/.

[40] *Id.*

[41] *See id*. at 294 ("There is sufficient evidence in humans for the carcinogenicity of all forms of asbestos (chrysotile, crocidolite, amosite, tremolite, actinolite, and anthophyllite).").

[42] *See* Ferro et al., *Amphibole, But Not Chrysotile, Asbestos Induces Anti-Nuclear Autoantibodies and IL-17 in C57BL/6 Mice*, 11 J. IMMUNOTOXICOLOGY 283 (2014). *See also* Faith Franz, *Study Revisits Health Risk of Chrysotile: Why is This Still a Debate in 2013?*, THE MESOTHELIOMA CTR. (Feb. 1, 2013), https://www.asbestos.com/news/2013/02/01/health-risk-of-chrysotile/; Luus, *supra* note 35, at 123 ("Research on in vivo rats has found that chrysotile promotes genotoxicity more rapidly than crocidolite.").

[43] Lemen, *supra* note 27, at 2 ("Austria, Belgium, England, The Czech Republic, Denmark, Finland, France, Germany, Italy, the Netherlands, New Zealand, Poland, Saudi Arabia, Sweden, and Switzerland have all banned asbestos. . . . Further substantiation that asbestos cannot be used safely comes from the most recent International Programme for Chemical

Whatever the case may be regarding the effects of different strains of asbestos, one absolute certainty is that asbestos use has led to an overwhelming amount of litigation. In 1973, the United States Court of Appeals for the Fifth Circuit ruled against asbestos manufacturers in *Borel v. Fibreboard Paper Products Corp.*[44] This decision "began the onslaught" of asbestos litigation.[45] Following the *Borel* decision in 1973, and since 2005, more than 600,000 claims based on allegations of asbestos-related illnesses were filed.[46] During that same timeframe, sixty different companies filed for bankruptcy due to asbestos litigation and more than fifty-four billion dollars were paid in litigation expenses and compensation.[47] In the 1990s alone, the number of pending asbestos cases in the United States doubled from 100,000 to 200,000.[48] The asbestos litigation problem resulted in a full-blown crisis.[49]

The problems caused by the glut of asbestos litigation have been borne by both claimants and defendants, and the litigation itself has been "a disaster of major proportions to both the victims and the producers of asbestos products."[50] Our court systems are not equipped to handle this "avalanche of litigation,"[51] and as a result, claimants have been left to claim mere pennies on the dollar in compensation for their injuries.[52] The litany

---

Safety Environmental Health Criteria 203-Chrysotile Asbestos (IPCS, 1998). The document concluded 'Exposure to chrysotile asbestos poses increased risks for asbestosis, lung cancer and mesothelioma in a dose dependent manner. No threshold has been identified for carcinogenic risks.'").

[44] Borel v. Fibreboard Paper Prods. Corp., 493 F.2d 1076 (5th Cir. 1973).

[45] Gifford, *supra* note 13, at 620.

[46] *Id*. at 621.

[47] *Id*.

[48] Schwartz, *supra* note 2, at 1–2 (also noting that "[t]he vast majority of asbestos claimants in that era had little or no actual physical impairment. Mass screenings arranged by personal injury law firms and their agents drove the litigation.").

[49] Stengel, *supra* note 2, at 226.

[50] *Id*. at 226 (noting that "absent some solution, litigation will continue into the foreseeable future: 'It is possible that millions of claims have yet to be made.'").

[51] Jenkins v. Raymark Indus., Inc., 782 F.2d 468, 470 (5th Cir. 1986).

[52] *Id*. at 483; Mark A. Behrens & Phil Goldberg, *The Asbestos Litigation Crisis: The Tide Appears to be Turning*, 12 CONN. INS. L.J. 477, 482 (2005–2006) ("The current asbestos litigation system is a tragedy for our clients. . . . It used to be that I could tell a man dying of mesothelioma that I could make sure that his family would be taken care of. . . . Today, I often cannot say that any more. And the reason is that other plaintiffs' attorneys are filing tens of thousands of claims every year for people who have absolutely nothing wrong with them.").

of problems embedded in this litigation has led courts, including the United States Supreme Court, to call for Congress to provide answers to the growing problems.[53] Nevertheless, asbestos litigation has persisted and continues to present problems for our judiciary that we cannot afford to recreate in other contexts.

b. 3D Printing: An Overview and Analog to Asbestos

3D-printing technologies share many of the same qualities that contributed to the rise in use of asbestos. Before addressing those similarities, this section provides a brief primer on the function of 3D printers. A foundation on how 3D printers operate will allow for an easier understanding of similarities between the health risks associated with exposure to asbestos and those associated with exposure to 3D printers. Moreover, the ongoing proliferation of 3D printers makes for a helpful comparison to asbestos.

3D printers create objects by referencing digital blueprints, which are often stored as Computer-Aided-Design (CAD) files.[54] Once a blueprint has been chosen, a 3D printer will construct the desired product layer-by-layer, or in a material-binding fashion, cutting down on waste and making the process more cost-effective.[55] Due to its ground-up manufacturing scheme, 3D printing avoids the waste typically created by the usual

---

[53] *Id.* at 865 (highlighting that the problems in asbestos litigation "[cry] out for a legislative solution.") (Rehnquist, J., concurring); Ortiz v. Fibreboard Corp., 527 U.S. 815, 821 (1999) (noting that the "elephantine mass of asbestos cases . . . defies customary judicial administration and calls for national legislation.") (Souter, J).

[54] Shen Wang, *When Classical Doctrines Of Products Liability Encounter 3d Printing: New Challenges In The New Landscape*, 16 HOUS. BUS. & TAX L.J. 104, 105 (2016).

[55] *See generally id*. at 105*;* James M. Beck & Matthew D. Jacobson, *3D Printing: What Could Happen To Products Liability When Users (And Everyone Else In Between) Become Manufacturers*, 18 MINN. J. L. SCI. & TECH. 143, 149 (2017) (While 3D printing is almost always a layer-by-layer process, there are various methods used in additive manufacturing such as: "(1) Material extrusion—material is selectively dispensed through a nozzle or orifice; (2) Material jetting—droplets of build material are selectively deposited; (3) Binder jetting—a liquid bonding agent is selectively deposited to join powder materials; (4) Sheet lamination—sheets of material are bonded to form an object; (5) Vat photopolymerization—liquid photopolymer in a vat is selectively cured by light-activated polymerization; (6) Powder bed fusion—thermal energy selectively fuses regions of a powder bed; (7) Directed energy deposition—focused thermal energy is used to fuse materials by melting as the material is being deposited.") (numerals and semi-colons added).

subtractive manufacturing processes.[56] Furthermore, because creators and manufacturers are dealing with digital CAD files, the designs stored in those files can be duplicated, modified, and shared by designers collaborating around the world.[57]

In addition to the various cost-effective ways by which 3D printers can create products, 3D printers can use a wide range of manufacturing materials. At a basic manufacturing level, 3D printers can use sawdust, metals, cements, plastics, and powders.[58] However, as the technology develops and becomes more sophisticated, 3D printers are beginning to find use with electric materials, silicone, biomaterials, and carbon fiber.[59] Perhaps most indicative of 3D printing's potential is the fact that 3D printers are being used to print "organoids"—small scale models of human organs and tissues—using actual living tissues as a construction material.[60]

With the world of materials and designs at the fingertips of creators everywhere, it is not hard to see why then-President Barack Obama stated that 3D printing "has the potential to revolutionize the way we make almost everything."[61] Indeed, observers have remarked on the arrival of the new manufacturing method by consistently singing the praises of 3D printing.[62] 3D printing is today's manufacturing miracle and its arrival has already begun to take the world by storm in the same way that asbestos did after the

---

[56] Beck & Jacobson, *supra* note 55, at 150 ("Because additive manufacturing only uses materials that are needed for the final object, the process can be more efficient and cost-effective, and waste can be reduced.").

[57] Wang, *supra* note 54, at 105.

[58] Lucas S. Osborn, *Regulating Three-Dimensional Printing: The Converging Worlds of Bits And Atoms*, 51 SAN DIEGO L. REV. 553, 559 (2014).

[59] Beck & Jacobson, *supra* note 55, at 151.

[60] Allie Nawrat, *3D Printing in the Medical Field: Four Major Applications Revolutionising the Industry*, VERDICT MED. DEVICES (Aug. 7, 2018), https://medicaldevicescommunity.com/md_news/3d-printing-in-the-medical-field-four-major-applications-revolutionising-the-industry/ (3D printers are capable of printing shapes and objects that would be impossible to create using traditional machining and molding, and allow manufacturers to mix materials in complex fashions leading to wholly new construction choices.).

[61] Obama, *supra* note 10.

[62] Osborn, *supra* note 58, at 560 ("3D printing will revolutionize society, affecting manufacturing, the environment, 3D art, entrepreneurship, and global trade."); Beck & Jacobson, *supra* note 55, at 152 ("Simply put, 3D printing is a potentially disruptive technology, and we undoubtedly have not yet envisioned all the changes it will bring."); Wang, *supra* note 54, at 105 ("In short, 3D printing signals a new era of manufacturing, production, and commercial activities.").

Industrial Revolution.[63] Additionally, it is worth noting that as efficiency and applications continue to rise, use of 3D-printing technology will also expand.[64] Put simply, "[3D-printing] technology brings hope of new freedoms, innovation, and creativity."[65]

The market has taken notice of the new hopes brought by 3D printing. Sales of simple desktop 3D printers continue to rise as industrial applications burst onto the scene. According to a Wohlers Associates report in 2018, the additive manufacturing industry experienced 21% growth over the previous year, exceeding $7.3 billion in sales.[66] In fact, sales of metal additive manufacturing systems alone had increased 80% from 2017 to 2018.[67] Roughly forty new companies had begun constructing 3D printers in 2018 and it is estimated that approximately 529,000 printers were sold between 2016 and 2018.[68] Although studies suggest that 3D printers are more widely used for prototyping and product testing, companies like Bentley are already looking to incorporate the technology in their vehicle parts.[69] Ubiquitously, 3D printers now have applications in homes,[70] hospitals,[71]

---

[63] Osborn, *supra* note 58, at 560 ("The coming ubiquity of 3D printing signals a new era of individual empowerment and creativity.").

[64] *Id*. at 561 ("Already, 3D printers can make a remarkable range of products. Fascinating examples include food, shoes, human body parts, working guns, clothes, and bicycles. Of course, at this stage, inexpensive home 3D printers are relatively simple and print only in plastic. But over time, the costs will fall, and the capabilities will rise.").

[65] *Id*. at 562.

[66] TJ McCue, *Wohlers Report 2018: 3D Printer Industry Tops $7 Billion*, FORBES (June 4, 2018), https://www.forbes.com/sites/tjmccue/2018/06/04/wohlers-report-2018-3d-printer-industry-rises-21-percent-to-over-7-billion/.

[67] *Id*.

[68] *Id*.

[69] Miller Allen et al., *3D Printing Standards and Verification Services*, 2 APPLIED INNOVATION REV. 34, 38 (June 2016), http://scet.berkeley.edu/wp-content/uploads/AIR-2016-3D-Printing.pdf.

[70] YaleGlobal Online, *Beyond the Hype: The Industrial Challenges for 3D Printing*, YALE UNIV. (Apr. 16, 2014), https://yaleglobal.yale.edu/content/beyond-hype-industrial-challenges-3d-printing.

[71] *3D Printing*, 8 E. VA. MED. SCH. MAG. 13, 13–17 (2015–2016), https://www.evms.edu/uploads/magazine/8-5/downloads/evmsMag_8.5.pdf.

and schools.[72] Suffice it to say, 3D printers are going to be everywhere; however, where the printers go, so do their risks.[73]

This newfound miracle is not without its Achilles heel. Unfortunately, much like asbestos, 3D printers come with latent dangers. If latency is not accounted for, and if our current law in these contexts does not adapt, these dangers are likely to usher in the next era of asbestos-like litigation.

Most 3D printers operate by taking the reagent materials—such as metals, dusts, cements, thermoplastics[74] or otherwise—heating them, and then depositing those materials layer-by-layer to build the desired product. As those materials are heated, they release gas and particulate emissions as they experience both physical and chemical changes in their structures.[75] These emissions are referred to as "volatile organic compounds" (VOCs), and exposure to the emissions in indoor environments "is of concern for workplaces, public venues, and private homes."[76] Exposure to these VOCs can potentially lead to the development of respiratory and mucous membrane irritation, asthma,[77] and, most notably, cancer.[78] Some studies suggest

---

[72] *See, e.g.*, *MSU Libraries offers 3D printing*, MISS. ST. UNIV. (Aug. 24, 2015), http://lib.msstate.edu/news/2015/3d.php; *Is the Implementation of 3D Printing in Education a Necessity*, 3D NATIVES (Aug. 29, 2018), https://www.3dnatives.com/en/3d-printing-in-education-290820184.

[73] *See* Aleksandr B. Stefaniak et al., *Characterization of chemical contaminants generated by a desktop fused deposition modeling 3-dimensional Printer*, 14 J. OCCUPATIONAL & ENVTL. HYGIENE 540, 541 (July 2017) ("3-dimensional (3-D) printers are becoming common in offices, libraries, schools, universities, and the home. With increased use of desktop and small-scale 3-D printers in non-industrial settings comes the concern for user health and safety.").

[74] *Id*. ("Thermoplastics are composed of a polymer that is mixed with a complex blend of materials known collectively as additives.").

[75] *Id*.

[76] *Id*.

[77] *Id*.

[78] *3D Printer Safety – Pollution and Their Health Risks*, *supra* note 11 ("The chemicals that are released during the heating of thermoplastic materials are known or suspected irritants and carcinogens, therefore exposure to 3D printer emissions should be minimized."); *see also* Janet Pelley, *Safety Standards Aim to Rein in 3-D Printer Emissions*, 4 ACS CENT. SCI. 134, 134–35 (Feb. 15, 2018) ("Petroleum-based acrylonitrile butadiene styrene (ABS), a plastic used in Lego blocks, gives off styrene and formaldehyde the first a suspected human carcinogen and the second a known one.").

that 3D-printing technology will cause cancer in approximately 4.45 out of every 10,000 people that come into contact with 3D printers.[79]

Further, these emissions often spread in the form of "ultrafine particles" (UFPs), which are particles less than 100 nanometers in diameter, allowing them to penetrate the lung tissue and enter the bloodstream.[80] This means that these cancer-causing particles can reach virtually every inch of the human body.[81] 3D printers are duly categorized as high emitters of ultrafine particles, even at the desktop size.[82] A rapidly growing and expanding product, heralded as the next manufacturing miracle, is pumping out high amounts of carcinogenic and otherwise disease-causing emissions. Does this sound familiar?

Some studies suggest that different filaments in 3D printing, and even different colors of the filaments, can affect particle output.[83] However, while these factors can affect the amount or size of particles released, it is not clear that these changes affect the release of carcinogens like styrene.[84] Thus, much like the studies indicating that there may have been a safe form of chrysotile asbestos, there are studies that indicate not all 3D-printing reagents are created equally dangerous.

Both asbestos and 3D printing are respectively viewed as manufacturing miracles. Asbestos rose to prominence and found itself ubiquitously involved in manufacturing processes and structures post-Industrial Revolution. Similarly, 3D printers are becoming universally adopted throughout this country in nearly every industry imaginable—including hospitals,

---

[79] Beuy Joob & Viroj Wiwanitkit, *Estimation of Cancer Risk Due to Exposure to Airborne Particle Emission of a Commercial Three-dimensional Printer*, 38 INDIAN J. MED. PAEDIATRIC ONCOLOGY 409 (Jul–Sep. 2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5686999/.

[80] Pelley, *supra* note 78, at 134–35 ("And all the filament types spew UFPs, particles with a diameter less than 100 nm that can penetrate deep into the lungs and enter the bloodstream. *These particles are known to cause respiratory and cardiovascular diseases.*") (emphasis added).

[81] *See generally* Jinghai Yi et al., *Emission of Particulate Matter From a Desktop Three-Dimensional (3D) Printer*, 79 J. TOXICOLOGY & ENVTL. HEALTH 453, 463 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4917922/pdf/uteh-79-453.pdf.

[82] *Id*. at 453; *see also 3D Printer Safety – Pollution and Their Health Risks*, *supra* note 11.

[83] *See* Yi et al., *supra* note 81, at 456–57; *see also* Pelley, *supra* note 78, at 135 (suggesting that "manufacturers can substitute better, safer filaments").

[84] Stefaniak et al., *supra* note 73, at 540 (stating "3-D printed objects continued to off-gas styrene, indicating potential for continued exposure after the print job is completed").

schools, libraries, and factories. The miniscule asbestos fibers, when inhaled, wrought havoc by causing mesothelioma, other cancers, and other lung conditions in those exposed. Likewise, the ultra-fine emissions from 3D printers have the capability to cause asthma, cancer, and various other diseases and irritations in those exposed. With the similarities of both form and effect now in frame, we turn to two befuddling legal issues that plagued both claimants and defendants in asbestos litigation: identifying the party at fault and establishing causation. These two prominent problems in asbestos litigation are likely to arise in the 3D-printing context.

III. CRITICAL ISSUES IN ASBESTOS LITIGATION: IDENTIFYING PARTY AT FAULT AND ESTABLISHING CAUSATION

a. The Role of Defendant Indeterminacy in the Asbestos Litigation Crisis

The early stages of latent-disease litigation involved plaintiffs who are, in many cases, incapable of identifying the precise defendants who caused their ailments—otherwise known as "defendant indeterminacy." Latent-disease cases present defendant indeterminacy issues for plaintiffs. When products are fungible, numerous manufacturers use or produce them. When injuries and harms are latent, exposure to various offending products over time is likely. As such, identifying the actor who caused injury becomes a herculean task. Plaintiffs involved in latent-disease litigation—namely "Agent Orange," asbestos, cigarettes, and lead pigment litigation—have been unable to obtain recovery because of their inability to prove which specific defendant manufactured the product that caused their harm.[85]

Because of defendant indeterminacy, new legal theories have emerged to establish liability. Plaintiffs' lawyers have tried to impose liability upon entities who did not actually cause injury by applying legal theories that assign liability to manufacturers of the offending products for their roles in the market.[86] The first such theory was aptly called the doctrine of "market share liability."[87]

---

[85] Gifford, *supra* note 13, at 653–54.

[86] Victor E. Schwartz & Mark A. Behrens, *Asbestos Litigation: The Endless Search for a Solvent Bystander*, 23 Widener L.J. 59, 62–63 (2013).

[87] *Id*. at 63; *see also* Gifford, *supra* note 13, at 654–56.

Market share liability was first introduced by the Supreme Court of California in *Sindell v. Abbott Laboratories*.[88] In *Sindell*, the plaintiffs were women who alleged that the drug DES,[89] ingested by their mothers during pregnancy, caused birth defects.[90] Both the fungibility of DES and the delay of its harmful effects created problems with assessing liability in *Sindell*.[91] The plaintiffs could not point to any defendant as the precise entity that had manufactured the DES taken by any individual mother.[92] Typically, if the plaintiff cannot identify the entity that caused her harm, she cannot meet her burden in establishing liability.

The California Supreme Court, however, permitted liability based on a theory of market share liability.[93] This theory can be best articulated as holding each defendant "liable for the proportion of the judgment represented by its share of that market unless it demonstrates that it could not have made the product which caused [the] plaintiff's injuries."[94] In adopting this theory, the court shifted the burden to defendants to prove that their product had not caused the injury or harm at issue.[95] The court reasoned that the imposition of liability, should a defendant fail to meet its burden, would only amount to that defendant's share of the product's market.[96]

---

[88] Sindell v. Abbott Laboratories, 607 P.2d 924, 937 (Cal. 1980).

[89] Schwartz & Behrens, *supra* note 86, at 63 ("DES was the common name for diethylstilbestrol, an artificial hormone that was widely prescribed to pregnant women from about 1950 to 1970 to prevent miscarriages or premature deliveries.").

[90] *Id.* at 63 ("Unfortunately, some two decades after DES was first widely prescribed, it was discovered that the drug was associated with a rare form of vaginal cancer and abnormalities of the reproductive tract in so-called 'DES daughters' who had been exposed to the drug in utero.").

[91] *Sindell*, 607 P.2d at 937.

[92] *Id.*

[93] *Sindell*, 607 P.2d 924, 937–38 (Cal. 1980).

[94] *Id*. at 937.

[95] *Id*. at 936.

[96] *Id*. at 938; *see also* Gifford, *supra* note 13, at 656 ("In *Sindell*, the court justified its adoption of this theory on the basis of Calabresian concepts—primary cost avoidance and the determination of the cheapest cost avoider: 'The manufacturer is in the best position to discover and guard against defects in its products and to warn of harmful effects; thus, holding it liable for defects and failure to warn of harmful effects will provide an incentive to product safety.'") (quoting *Sindell*, 607 P.2d at 936).

In the asbestos context, courts have "almost uniformly" rejected the theory of market share liability.[97] In effect, courts have barred this convenient option from plaintiffs' arsenal, reasoning that application of this "novel theory of causation would raise serious questions of fairness due to the fact that different manufacturers' asbestos products differ in degrees of harmfulness."[98]

Courts have likewise refused to adopt other similar theories in asbestos cases. Of note is "enterprise liability," which stems from a New York federal case, *Hall v. E.I. Du Pont De Nemours & Co*.[99] In *Hall*, children were injured by exploding blasting caps.[100] These explosions made the manufacturer of the caps impossible to determine.[101] "Because there was a strong likelihood that the blasting caps were produced by one of six major manufacturers, the court . . . indicated that it might be appropriate to shift the burden of causation to the defendants."[102] Courts have almost universally determined that this doctrine was inappropriate in asbestos cases, reasoning the case it springs from dealt with a very limited number of manufacturers in a tightly-centralized industry.[103] Additionally, courts have

---

[97] Schwartz & Behrens, *supra* note 86, at 64–65. *See generally* Celotex Corp. v. Copeland, 471 So. 2d 533, 537, 539 (Fla. 1985); Goldman v. Johns-Manville Sales Corp., 514 N.E.2d 691, 702 (Ohio 1987); Case v. Fibreboard Corp., 743 P.2d 1062, 1067 (Okla. 1987); Sholtis v. Am. Cyanamid Co., 568 A.2d 1196, 1204 (N.J. Super. Ct. App. Div. 1989); Stark v. Armstrong World Indus., Inc., 21 F. App'x 371, 375 n.4 (6th Cir. 2001); Cimino v. Raymark Indus., Inc., 151 F.3d 297, 314 (5th Cir. 1998); Jackson v. Anchor Packing Co., 994 F.2d 1295, 1303 (8th Cir. 1993).

[98] Blackston v. Shook and Fletcher Insulation Co., 764 F.2d 1480, 1483 (11th Cir. 1985) (referencing Starling v. Seaboard Coast Line R.R. Co. et al., 533 F. Supp. 183, 191 (S. D. Ga. 1982))

[99] Hall v. E.I. Du Pont De Nemours & Co., 345 F. Supp. 353, 379 (E.D.N.Y. 1972).

[100] *Id.* at 358.

[101] *Id*.

[102] Mark A. Behrens & Christopher E. Appel, *The Need for Rational Boundaries in Civil Conspiracy Claims*, 31 N. ILL. U. L. REV. 37, 57 (2010).

[103] *Id*. at 68. For courts rejecting the application of enterprise liability to asbestos see generally Case v. Fibreboard Corp., 743 P.2d 1062, 1067 (Okla. 1987); Gaulding v. Celotex Corp., 772 S.W.2d 66, 70 (Tex. 1989); Celotex Corp. v. Copeland, 471 So.2d 533, 535 (Fla. 1985); Thompson v. Johns-Manville Sales Corp., 714 F.2d 581, 583 (5th Cir. 1983); Univ. Sys. Of N.H. v. U.S. Gypsum Co., 756 F.Supp. 640, n.16 at 657; Marshall v. Celotex Corp., 651 F. Supp. 389, 395 (E.D. Mich. 1987).

mostly rejected plaintiffs' attempts to use "alternative liability"[104] as a basis for recovery in asbestos cases.[105]

Despite major setbacks in latent-disease cases, defendant indeterminacy has not deterred plaintiffs from pursuing litigation. Rather, plaintiffs and their lawyers have sought new answers and pathways to trial litigation, making adjudication of these cases more complex. This has led to an inefficient and overwhelmed system as a whole.[106]

Nevertheless, plaintiffs may avoid complex litigation issues by seeking an administrative scheme to receive compensation for asbestos injuries, similar to the so-called "black lung"[107] legislation.[108] The Supreme Court of the United States has also called for national legislation in the face of asbestos litigation issues.[109] Moreover, lawmakers in the United States made mention of the black lung scheme as being one that could benefit the asbestos litigation crisis.[110]

However, to this point, no such national legislation has been passed. And, despite the refusal of courts to apply plaintiff-friendly doctrines such as market share liability and enterprise liability, plaintiffs have not relented. Instead, they have focused on their various exposures to asbestos and, using expert testimony, have attempted to sway courts into creating very low thresholds for causation in asbestos-related, latent-disease cases. In sum, the battle between exposure-related causation theories demonstrates yet another

---

[104] Summers v. Tice, 33 Cal.2d 80, 199 P.2d 1 (1948) (introducing alternative liability doctrine).

[105] *See*, *e.g.*, Black v. Abex Corp., 603 N.W.2d 182, 191 (N.D. 1999); Nutt v. A.C. & S. Co., 517 A.2d 690, 694 (Del. Super. Ct. 1986); U.S. Gypsum Co., 756 F. Supp. at 654–55; *Case*, 743 P.2d at 1067; Rutherford v. Owens-Ill., Inc., 941 P.2d 1203, 1220–21 (Cal. 1997); *Gaulding*, 772 S.W.2d at 69; *Copeland*, 471 So.2d at 535.

[106] *See* Schwartz, *supra* note 2, at 2.

[107] *See generally Black Lung*, UNIV. OF LOUISVILLE SCHOOL OF MED.(2018) ("Black lung, or coal workers' pneumoconiosis, is the name given lung diseases caused by inhaling coal-mine dust. Only the smallest dust particles make it past the nose, mouth and throat to the alveoli deep in the lungs."), https://louisville.edu/medicine/departments/medicine/divisions/pulmonary/clinical-services/pulmonary/ild/black-lung (last visited Jan. 16, 2020).

[108] The "black lung" legislation was an act passed to ensure compensation of coal miners who developed "black lung" sickness during work in their occupation. *See* Allen R. Prunty & Mark E. Solomons, *The Federal Black Lung Program: Its Evolution And Current Issues*, 91 W. VA. L. REV. 665, 667 (1989).

[109] Ortiz v. Fibreboard Corp., 527 U.S. 815, 821 (1999).

[110] Stengel, *supra* note 2, at 223 n.4.

sticking point in addressing the glut of asbestos cases in the American judicial system.

b. Difficulties With Theories of Causation Exacerbated Asbestos Litigation Crisis

Since *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), courts across the United States have taken on the duty of acting as a gatekeeper to junk science presented by experts-for-hire.[111] Because of this new standard,[112] courts have been thrust into the duty of playing "amateur scientists."[113] This role has extended prominently into asbestos litigation, as claimants and defendants alike battle over which exposure theory is proper to establish causation. The two main theories adopted by the courts are the "any-exposure" theory[114] and the *Lohrmann*[115] "frequency-regularity-proximity" test.[116]

As asbestos litigation has carried on, courts have developed entirely new sets of rules to attempt to efficiently manage their asbestos dockets; almost all of these rule changes have consistently favored plaintiffs.[117] One of these plaintiff-friendly developments was the adoption of the any-exposure theory, otherwise known as the "any fiber" theory."[118] This theory asserts that asbestos-related diseases are a result of the cumulative build-up of asbestos fibers inhaled by an individual; thus, no matter how trivial one's exposure might have been to a particular asbestos-containing product, they

---

[111] *See* Sofia Adrogue, *The Post-Daubert Court-"Amateur Scientist" Gatekeeper or Executioner?*, 35-APR HOUS. LAW. 10 (Mar.–Apr. 1998) ("The Ninth Circuit on remand in *Daubert II*, stated that 'federal judges ruling on the admissibility of expert scientific testimony face a far more complex and daunting task in a post-Daubert world than before.'").

[112] *Id.* (In *Daubert*, the United States Supreme Court rejected the previously acceptable *Frye* test which rendered expert scientific testimony admissible if the expert used generally accepted scientific methods in reaching the conclusion.) (referencing Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 601 (1993)).

[113] *Daubert*, 509 U.S. at 601 (Rehnquist, J., concurring in part and dissenting in part).

[114] Mark A. Behrens & William L. Anderson, *The "Any Exposure" Theory: An Unsound Basis for Asbestos Causation and Expert Testimony*, 37 SW. U. L. REV. 479, 486 (2008).

[115] Lohrmann v. Pittsburgh Corning Corp., 782 F.2d 1156, 1163 (4th Cir. 1986).

[116] Charles T. Greene, *Determining Liability in Asbestos Cases: The Battle to Assign Liability Decades After Exposure*, 31 AM. J. TRIAL ADVOC. 571, 573 (2008).

[117] *See id.* at 580; Behrens & Anderson, *supra* note 114, at 479–80 (worth noting is that, because the litigation became so "malleable and lucrative," plaintiffs' attorneys have spent several years searching for the "next asbestos.").

[118] Behrens & Anderson, *supra* note 114, at 479–80.

should be able to hold the manufacturer of that product liable for their disease.[119] This theory blew the doors of asbestos litigation wide open. Plaintiffs were able to sue countless defendants based on each individual claim since, due to the widespread nature of asbestos-containing products, each plaintiff had come in contact with several manufacturers' asbestos products.[120]

Courts have had mixed responses to the any-exposure theory, though initially the theory found limited success.[121] The court in *Celotex Corp. v. Tate*[122] is a good example of a court that embraced this theory. In *Tate*, a plaintiff unloaded bags of asbestos from boxcars and poured the asbestos into mixers.[123] The defendant argued that the plaintiff needed to establish that it was, in fact, its product (to the exclusion of others) that caused the plaintiff's injury. The Texas appellate court disagreed, holding that "when a defendant has in fact caused harm to the plaintiff, he may not escape liability merely because the harm he has inflicted has combined with similar harm inflicted by other wrongdoers."[124] Thus, courts adopting this theory shifted the burden to defendants to prove, much like the burden in alternative liability, that it was not their product that caused the harm.[125]

Another prominent standard, the *Lohrmann* standard, has received more widespread adoption in asbestos cases. "Courts in every circuit but the D.C. Circuit, and the First, Second, and Fifth Circuits have adopted the *Lohrmann* test."[126] In *Lohrmann*, the plaintiff had been an employee for a shipyard for nearly forty years.[127] Once the shipyard worker had been diagnosed with both asbestosis and chronic pulmonary disease, he sought recovery based upon negligence and strict liability.[128] The real issue, however, was whether the plaintiff needed to show by way of "substantial evidence"

---

[119] *Id.*

[120] *See id.*

[121] *Id.* at 480–82.

[122] Celotex Corp. v. Tate, 797 S.W.2d 197, 204 (Tex. App.—Corpus Christi 1990, writ dism'd by agr.).

[123] *Id.* at 200.

[124] Greene, *supra* note 116, at 585 (quoting *Tate*, 797 S.W.2d at 203).

[125] *Id.* at 585–86.

[126] Slaughter v. S. Talc Co., 949 F.2d 167, 171 n.3 (5th Cir. 1991) (also noting that "Michigan, Massachusetts, New Jersey, Illinois, Pennsylvania, Maryland, Nebraska, and Oklahoma" had adopted the test as of that case).

[127] Greene, *supra* note 116, at 573.

[128] *Id*.

that the defendant's product was a factor in causing his injuries.[129] The shipyard worker asserted that all he needed to do was present evidence that the company's asbestos-containing product was present at the workplace while the plaintiff was present. The court ultimately disagreed and instead applied the frequency-regularity-proximity rule.[130] The frequency-regularity-proximity rule applies a much higher burden for plaintiffs to meet. Yet, perhaps ironically, that standard has led to more confusion, not less, about when a plaintiff can and cannot bring a claim.[131] The any-exposure theory allows a plaintiff to bring a claim if he's been exposed to the product at all; the *Lohrmann* test requires, vaguely, more.

Between the two standards, the *Lohrmann* standard is more widely accepted among jurisdictions.[132] Twenty-seven states have explicitly adopted the test, while others, like Texas, have adopted an even more stringent standard.[133] Texas's standard, adopted in *Borg-Warner Corp. v. Flores*,[134] requires more than simple frequency, regularity, and proximity.[135] It additionally requires that the plaintiff prove that the product at issue was a "substantial factor" in causing the harm.[136]

This step is perhaps a step that many legal observers have been waiting to see adopted nationwide. Much has been written about genuine plaintiffs at the beginning of asbestos litigation's rise. However, also heavily

---

[129] *Id*. at 574.

[130] *Id*. (The *Lohrmann* standard states that "there must be evidence of exposure to a specific product on a regular basis over some extended period of time in proximity to where the plaintiff actually worked." The court noted that "[i]n effect, this is a de minimis rule since a plaintiff must prove more than a casual or minimum contact with the product.") (quoting Lohrmann v. Pittsburgh Corning Corp., 782 F.2d 1156, 1162–63 (4th Cir. 1986)).

[131] DiMasi, Brian M., *The Threshold Level of Proof of Asbestos Causation: The "Frequency, Regularity and Proximity test" and a Modified Summers v. Tice Theory of Burden-Shifting*, 24 CAP. U. L. REV. 735, 752–53 (1995) ("Furthermore, the *Lohrmann* test, which was synthesized by the *Lohrmann* district court to aid in the determination of 'substantial factor' causation, injects confusion and complexity into the weighing of evidence of asbestos exposure, effectively denying asbestos victims the opportunity to present their cases to a jury.").

[132] Jason Litt et al., *Returning to Rutherford: A Call to rejoin California Courts to Rejoin the Legal Mainstream and Require Causation be Proved in Asbestos Cases Under Traditional Torts Principles,* 45 Sw. L. Rev. 989, 1011 (2016).

[133] *Id*.

[134] Borg-Warner Corp. v. Flores, 232 S.W.3d 765 (Tex. 2007).

[135] *Id.* at 769.

[136] Greene, *supra* note 116, at 576–78.

noted has been the effect, on dockets everywhere, of non-sick claimants.[137] Commentators assert that "Today, the vast majority of new asbestos claimants—up to [90%]—are 'people who have been exposed to asbestos, and who (usually) have some marker of exposure . . . but who are not impaired by an asbestos-related disease and likely never will be.'"[138] Indeed, the differing standards of causation, along with the unclear standards surrounding who can and cannot be sued by claimants, has led to the wild-west of litigation within the asbestos context.

Whatever courts' responses have been to the two issues explored above, they seemingly only further complicate the issue. Asbestos litigation ran rampant and continues to clog through the United States judiciary today. These two problems, defendant indeterminacy and establishing causation, will also be pivotal problems in 3D-printing litigation. The next part of this Article will address why these two issues are likely to plague 3D-printing litigation and will then make suggestions as to what steps manufacturers and courts should be taking to (a) avoid the litigation from the outset and (b) clarify the law to provide for more efficient judicial processes.

IV. AVOIDING ASBESTOS CONSUMER SAFETY ISSUES AND LITIGATION INEFFICIENCIES IN THE 3D-PRINTING CONTEXT

The American judiciary, when faced with the widespread problem of asbestos litigation, has done little to clarify the law and make the adjudication of such cases more efficient. Indeed, in the entire context of latent-disease jurisprudence, courts have consistently found themselves bogged down by problems identifying rightful defendants and establishing causation in a manner fair to both parties.[139] As a result, plaintiffs and defendants alike will want to take preventative steps and vie for favorable theories and doctrines in the wake of 3D printing's ascension to popularity. "As 3D printing develops, the law will also have to develop in order to continue to maintain its relevance."[140]

The issue in identifying who caused the resulting harm will be a question that could become far more complicated in 3D-printing litigation than in the asbestos context. In asbestos litigation, claimants could often

---

[137] Behrens & Goldberg, *supra* note 52, at 478–79.

[138] *Id.*

[139] *See generally* Gifford, *supra* note 13.

[140] Beck & Jacobson, *supra* note 55, at 147.

point to particular products, or genres of products, that caused their harm.[141] However, many asbestos products were fungible and therefore recreated by various manufacturers—plaintiffs often could not meet the burden of identifying a liable manufacturer.[142] Imagine that same problem when almost anyone and everyone, across all kinds of professions and in homes, hospitals, factories, and otherwise, are using 3D printers.[143] This search for a party from which to recover for one's injuries becomes theoretically more difficult than finding a needle in a haystack.

Further complicating the issue is that this new form of latent-disease litigation will focus not on the actual products created by the manufacturer, but rather on the means of creation used by the manufacturer. It is exposure to the emissions from 3D printers—created and emitted during the creation process—that is dangerous to human beings.[144] So, when everyone—from one's neighbor to one's doctor and employer—is using 3D printers, how exactly is a claimant to identify the manufacturer liable for his or her harm? This is far more complicated than trying to establish a list of possible parties responsible for creating the asbestos-containing insulation one was exposed to. Plaintiffs will now need to identify whose act(s) of creation contributed to their disease or condition.

Additionally, courts will likely be faced with the question of whether to blame the 3D-printer manufacturers or the manufacturers of the reagents that release carcinogens when run through a 3D printer. As discussed above, there are differences in the emissions of various materials used in 3D printing.[145] Thus, our issue is further complicated since courts could potentially point the finger at two groups of manufacturers: manufacturers of 3D printers and manufacturers who produce 3D-printing reagents that are carcinogenic or otherwise dangerous to humans. This kind of issue is just the tip of the iceberg for claimants and defendants facing the preeminent industrial 3D-printing regime.[146]

---

[141] *See* Gifford, *supra* note 13, at 653–654.

[142] *Id.*

[143] *See generally* Beck & Jacobson, *supra* note 55, at 144–45 ("3D printing is already in the process of becoming a significant industry with tremendous innovative potential for many applications, from dental and medical, to automotive, aerospace/aviation, toys, military, fashion, food, eyewear, and construction.).

[144] *See generally* Joob & Wiwanitkit, *supra* note 79.

[145] *See generally* Stefaniak et al., *supra* note 73.

[146] Beck & Jacobson, *supra* note 55 at 147–48 ("One of the biggest legal areas where 3D printing will have an impact is tort liability. The legal implications will include what is

The logical first step in approaching these problems is to prevent, as much as possible, the emissions from causing harm in the first place. Many 3D printers can be sold with enclosures or can be safely operated in a self-made enclosure appropriate for the product.[147] Furthermore, it may be appropriate to use creation processes, where possible, that operate at lower temperatures. Doing so can cut down on the amount of emissions created by the printer and, thereby, further lower people's exposure to its harmful chemicals.[148] Other obvious and important precautions to take have been set out by the National Institute for Occupational Safety and Health (NIOSH) and range from following the printer-manufacturer's controls to turning off the printer nozzle during jams.[149] While some of these preliminary steps are obvious, they are still critical to note. Also important, though not explored in this Article, are any future Occupational Safety and Health Administration (OSHA) guidelines and regulations put in place for 3D printers in the workplace. This Article does not discuss in-depth OSHA or other possible

---

exactly a 'product,' who is the 'manufacturer,' what is the 'marketplace,' and who should be potentially liable for a defective 3D-printed product (once 'product' is defined). These legal implications are only heightened for more complex and technical products such as drugs and medical devices. Although it is unclear, at this point in the absence of precedent, exactly how the law will change, what is certain is that the law will need to adapt or change as 3D printing becomes commonplace.").

[147] This is a logical step because "[h]eating of certain thermoplastic filament can generate toxic vapors and vapors with high volatile organic compounds (VOCs). Most 3D printers do not come with an enclosure, exhaust ventilation or any filters." *See 3D Printer Safety*, UNIV. OF VT., https://www.uvm.edu/riskmanagement/3d-printer-safety ("To reduce the potential for nano particles to aerosolize or be inhaled by users, it is best to purchase 3D printers with an enclosure or have an enclosure made.") (last visited Jan. 16, 2020).

[148] *Id.* ("Nanoparticles (ultrafine particles less than 1/10,000 of a millimeter) are one of the by-products emitted during the 3D printing process. Recent studies have shown that 3D printing using a low-temperature polylactic acid (PLA) feedstock can release 20 billion particles per minute, while a higher temperature acrylonitrile butadiene styrene (ABS) feedstock can release 200 billion.").

[149] *Control Measures Critical for 3D Printers*, 1 NIOSH RESEARCH ROUNDS 12 (June 2016), https://www.cdc.gov/niosh/research-rounds/resroundsv1n12.html#a ("To reduce emissions, the investigators recommend five specific steps: (1) Always use the manufacturer's supplied controls (full enclosure appears more effective at controlling emissions than a cover). (2) Use the printer in a well-ventilated place, and directly ventilate the printer. (3) Maintain a distance from the printer to minimize breathing in emitted particles, and choose a low emitting printer and filament when possible. (4) Turn off the printer if the printer nozzle jams, and allow it to ventilate before removing the cover. (5) Use engineering measures first, such as manufacturer-supplied equipment and proper ventilation, then use materials with lower emissions. Finally, wear protective equipment, such as respirators.").

regulations because this Article is more concerned with clarifying litigation issues not related to compliance with these kinds of regulations.

The next logical step, again a preventative one, will be to try to use, where possible, materials that are less dangerous to humans. It is well documented, and discussed in-depth above, that different materials can have various different potentials for harm.[150] Thus, it is important that innovators in this space continue to identify and develop 3D-printing reagents that emit particles that are not known or suspected carcinogens. Should courts decide that the proper parties for suit are the manufacturers of these reagents, this step may be paramount. Outside of these common-sense measures, however, plaintiffs and defendants are likely to disagree on what standards or doctrines courts ought to apply.

Plaintiffs, for instance, are likely to encourage courts to adopt broader theories of liability such as the previously discussed market share liability theory.[151] Using this theory, and others like it, plaintiffs would be given wide discretion as to which manufacturers they elect to sue, as many of these doctrines provide for joint and several liability.[152] This freedom would assist plaintiffs, and courts, in circumventing the problems in attempting to adequately identify each individually-liable party. However, plaintiffs will face almost universal rejection of such doctrines by the American judiciary.[153] Plaintiffs will need to provide compelling reasons for the adoption of these theories in the 3D-printing, latent-disease context.

---

[150] *Id.* ("The emissions also varied by filament type and color. Filaments made from natural materials like corn emitted smaller particles than plastic filaments did. . . . Calculations showed that the risk of the particles lodging in the lungs was 3 times higher for the small particles made from natural substances compared with the larger plastic particles. Color also affected particle size, with natural corn-based filaments in the color true red emitting the smallest particles, on average. In contrast, blue plastic filaments emitted the largest particles"); *see also* Joob & Wiwanitkit, *supra* note 79.

[151] *See* Gifford, *supra* note 13 at 654–56 ("Despite the traditional requirement that a claimant identify the specific product manufacturer whose product caused her harm, manufacturers of mass products may be held liable without proof of specific identification on legal theories including civil conspiracy or concert of action, alternative liability, enterprise or industry-wide liability, and market share liability.").

[152] *Id.* at 655 ("Even if courts impose liability on mass products manufacturers collectively, with the exception of market share liability, such liability is joint and several.").

[153] *Id*. at 655–56 ("Each of these theories for holding manufacturers of mass products liable, however, has been applied only in cases with specific (and generally unusual) circumstances. . . . Market share liability has inspired considerable academic attention, despite its

Furthermore, plaintiffs are likely to advocate for a less restrictive test for causation than the *Lohrmann* standard.[154] The frequency-regularity-proximity test set out by the court in *Lohrmann*[155] will be too cumbersome, plaintiffs will argue, in determining which of several commonly encountered 3D printers caused each plaintiffs' injuries. In rejecting *Lohrmann*, plaintiffs are likely to argue, as is asserted in the *Lohrmann* case itself, that an any-exposure theory will be proper for establishing liability.[156] Much like the court in *Lohrmann*, and the many courts that have since adopted the *Lohrmann* standard, plaintiffs are likely to face a high bar in asking courts to move away from that standard.[157]

A final suggestion that may be agreeable to plaintiffs would be an adoption of a similar regime to the black lung legislation.[158] However, an application of this theory is likely to require that 3D-printer emissions become a known cause of a unique disease or form of cancer. Even in the latter situation, Congress has not adopted similar legislation in response to asbestos's known causation of mesothelioma.[159]

By contrast, defendants are likely to want courts to move away from broad theories like market share liability and adhere to the *Lohrmann* standard, or perhaps even more restrictive standards, in assessing liability. These blanket suggestions may also prove unreliable, as asbestos litigation has clogged our court system even with the judiciary's move away from broader liability theories and, simultaneously, towards the narrow *Lohrmann* causation theory. The first issue courts will need to decide, however, is which party or parties to identify as defendants.

---

virtually universal subsequent rejection by the courts in cases other than those against DES manufacturers.").

[154] *See generally* Greene, *supra* note 116.

[155] Lohrmann v. Pittsburgh Corning Corp., 782 F.2d 1156, 1156 (4th Cir. 1986).

[156] Greene, *supra* note 116, at 574 ("The plaintiffs asserted that the court should 'adopt a rule that if the plaintiff can present any evidence that a company's asbestos-containing product was at the workplace while the plaintiff was at the workplace, a jury question [had] been established as to whether that product contributed as a proximate cause to the plaintiff's disease'").

[157] The court in *Lohrmann* called it's new standard a "de minimis rule" that required plaintiffs to "prove more than a casual or minimum contact with the product." *Lohrmann*, 782 F.2d at 1162.

[158] *See generally Black Lung*, *supra* note 107; Prunty & Solomons, *supra* note 108, at 667; Ortiz v. Fibreboard Corp., 527 U.S. 815, 821 (1999).

[159] *See* Prunty & Solomons, *supra* note 108, at 666–68.

Because 3D printers will likely pervade every important space in humans' lives[160] it will be impossible to distinguish which printers are the primary cause of any individual's diseases. Courts cannot simply ignore these likely widespread claims because it is difficult to identify specific defendants. As such, liability is likely to be thrust upon one of two parties, or some combination thereof: 3D-printer manufacturers and/or manufacturers of 3D-printing reagents. Parties in this position should consider several recommendations for courts to adopt.

First, 3D-printer manufacturers should assert sole liability upon the manufacturers of the dangerous reagents. It would be an extreme undertaking for courts to evaluate every 3D printer that each individual plaintiff was exposed to and then identify which printer caused the plaintiff's harm. Furthermore, where claimants may possibly encounter any number of different 3D printers, many of those printers will be using the same reagents as their construction materials.[161] Thus, where there will be fluctuation in 3D printers, there will be less uncertainty as to what reagents were being used and, thus, what parties may be liable.

Fungibility will likely be the primary issue with 3D printers. Fungibility creates issues in assessing causation and liability in cases involving multiple defendants. If 3D printers are everywhere, how can any claimant identify a defendant with specificity? While courts have notably shown a reluctance in applying theories such as market share liability,[162] such a theory may be the only rational choice. A clear certainty in all of this is that there will be plaintiffs who have been harmed by 3D-printer emissions. Courts cannot simply shut the courtroom doors to potentially millions of plaintiffs under the premise that 3D printers are just too ubiquitous to assess liability. Additionally, by applying market share liability, courts can encourage manufacturers of reagents to continuously research and develop safer materials while simultaneously encouraging employers and others using this technology to ensure they are using it in the safest way possible.

If courts do elect to hold 3D-printer manufacturers themselves liable, those manufacturers will then want courts to adopt the *Lohrmann*

---

[160] Nora Freeman Engstrom, *3-D Printing And Product Liability: Identifying The Obstacles*, 162 U. PA. L. REV. ONLINE 35, 35 (2013) ("Brook Drumm, the founder of one 3-D printing company, for example, envisions 'a printer in every home.'").

[161] *See generally* Stefaniak et al., *supra* note 73.

[162] *See* cases cited *supra* note 97.

standard in establishing causation.[163] This too could be a rational pairing for courts. By applying something akin to the frequency-regularity-proximity test to 3D printers, plaintiffs will be required to identify a certain manufacturer and the printer that they were exposed to at a higher rate than others. However, such a standard will likely prove too burdensome for plaintiffs, due to the aforementioned problem of ubiquity. This further demonstrates why the burden should lie with reagent manufacturers. We can be certain, regardless of which printer is being used, that consumers will be consistently exposed to the emissions from these same materials.

Regardless of the decision on which manufacturers to properly hold liable, perhaps the best answer for the courts would be to adopt some middle-ground between both the desires of the plaintiffs and the defendants to create a more efficient, predictable standard. By applying the *Lohrmann* standard, courts can ensure that plaintiffs identify 3D printers that they more than casually or minimally experience on a daily basis.[164] This will put a defendant-friendly restriction on plaintiffs, while maintaining the narrow *Lohrmann* standard.

However, as discussed, it is likely that plaintiffs will encounter several printers on a more than casual basis.[165] As such, there may be several manufacturers potentially liable. This is a situation in which defendants may be amenable to a market share liability theory, since that theory does not include joint and several liability.[166] A market share liability standard may ultimately be a more economically advantageous choice than a standard that leaves major manufacturers of 3D printers on their own to bear the costs for diseases they didn't uniquely cause.

Thus, perhaps by combining a restrictive and narrow causation theory, such as the *Lohrmann* standard, and pairing it with a broad theory of liability such as market share liability, courts may be able to strike a balance between identifying the limited possible causes of plaintiffs' latent diseases and holding more parties responsible for their contributions instead of leaving one manufacturer "caught holding the bag." In so doing, courts can operate more efficiently, as calculation of damages will be far simpler, and the

---

[163] *See generally* Greene, *supra* note 116.

[164] *See generally* Lohrmann v. Pittsburgh Corning Corp., 782 F.2d 1156, 1162 (4th Cir. 1986).

[165] *See* Engstrom, *supra* note 159, at 35─36.

[166] *See* Gifford, *supra* note 13, at 655.

motivation to settle will increase once litigants pass the initial phases of trial.

Finally, as noted above, Congress could pass legislation akin to the black lung legislation that was used to compensate injured miners.[167] This solution would likely be agreeable to both plaintiffs and defendants alike. However, such legislation will likely require 3D printers to be uniquely identified as the cause for a specific kind of disease or cancer. While not altogether unlikely, this Article cannot purport to predict such an outcome. If it were to arise, though, similar legislation would be appropriate, agreeable, and perhaps the best choice to avoid any massive influx of nationwide litigation.

V. CONCLUSION

Worth briefly mentioning is that the issues discussed at length in this Article, i.e. the latent-disease litigation implications of the rise of 3D printing, are only the tip of the iceberg.[168]

3D printing will likely require pivotal changes in how courts approach tort liability.[169] Because anyone can share their creations, including schematics for those creations, online, "anyone can manufacture a product."[170] As such, it becomes extremely difficult to determine who is liable. There are several parties who could bear liability, including the manufacturer, the creator of the schematic who shared it online, and the 3D-printer manufacturer itself, among others.[171] This, in turn, will present many other issues such as establishing jurisdiction, identifying the party at fault, or identifying a liable party capable of paying the judgment.[172]

3D printers are likely to cause many problems in the realm of intellectual property.[173] In the realm of trademarks alone, it will be tremendously hard for trademark owners to track users who are printing similar products and using them in public spaces without the rights to do so.[174] Copyrights may also prove to be difficult since CAD files, the usual mode of storage

---

[167] *See* Prunty & Solomons, *supra* note 108, at 667.

[168] *See supra* note 62 and accompanying text.

[169] *See* Beck & Jacobson, *supra* note 55, at 158–59.

[170] *Id.* at 158.

[171] *Id.* at 158–61.

[172] *Id.* at 160.

[173] *See* Osborn, *supra* note 58, at 582.

[174] *Id*. at 583–84.

for 3D-printer schematics, are likely utilitarian articles for which copyright law provides no protections.[175]

Thus, while the thrust of this Article focuses on the capability of 3D printers to become the subject of the next asbestos-like, latent-disease litigation, it is clear that 3D printing is poised to present numerous legal problems. From 3D-printed coffee cups to 3D-printed guns,[176] Congress and courts alike are certain to face numerous novel and unique problems as 3D printing continues to take the world by storm. However these groups choose to respond, it is critical that they ensure we do not create another court-clogging, inefficient, legal regime like the one that burdens asbestos litigation. In that scheme, both plaintiffs and defendants suffer from the mass uncertainty and inefficiency present in the system.

---

[175] *Id*. at 589.

[176] Marrian Zhou, *3D-Printed Gun Controversy: Everything You Need to Know*, CNET (Sept. 25, 2018), https://www.cnet.com/news/the-3d-printed-gun-controversy-everything-you-need-to-know/.