JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 5 Part 1 • Spring 2021

FACIAL RECOGNITION TECHNOLOGY: CAN WE TAME THE WILD West?

AND

PUBLIC POLICY AND THE INSURABILITY OF CYBER RISK

JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 5 Part 2 • Fall 2021

TABLE OF CONTENTS

FACIAL RECOGNITION TECHNOLOGY: CAN WE TAME THE WILD WEST?

Angela M. Nieves*

TABLE OF CONTENTS

* Juris Doctor Candidate, St. Thomas University School of Law; ST. THOMAS LAW REVIEW, Managing Editor 2020; Bachelor of Arts in Liberal Studies, Florida International University, 2008.

I. INTRODUCTION: THE PROBLEM WITH FACIAL RECOGNITION TECHNOLOGY

A. Background

Facial recognition technology ("FRT") is a biometric resource that identifies individuals by analyzing physiological or behavioral characteristics and matching them to a database of named persons.[1] It has come a long way from its beginnings in research labs in the 1960s and 70s.[2] The use of cameras for surveillance and identification can be traced back several decades, when businesses and city authorities would install closed-circuit television (CCTV) cameras to film small areas of interest.[3] To make an identification later, officials would pore over tapes of recorded footage in search of helpful images and details and then compare these against the database of information in their possession, a process which was obviously time-consuming and labor-intensive.[4] Today, advances in science mean law enforcement agencies can have even real-time digital matches in just seconds, and the proliferation of cameras makes mass surveillance a possibility.[5]

---

[1] *See* Rosie Brinckerhoff, *Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever*, 70 FED. COMM. L.J. 105, 112 (2018).

[2] *See* Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy.*, 23 B.U. J. SCI. & TECH. L. 88, 93 (2017); *see also* Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/ (describing the advancements made in early facial recognition technology).

[3] *See* Michael Kwet, *The Rise of Smart Camera Networks, and Why We Should Ban Them*, INTERCEPT (Jan. 27, 2020 12:53 PM), https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/ (discussing the early surveillance uses of cameras).

[4] *See* HERMAN KRUEGLE, CCTV SURVEILLANCE: VIDEO PRACTICES AND TECHNOLOGY 276 (Elsevier ed., 2011) (explaining that the operation of real-time video recording systems and later VHS recording systems was cumbersome and inefficient).

[5] *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech. & the Law. Comm. on the Judiciary*, 112th Cong. 19 (2012) [hereinafter *Privacy and Civil Liberties Hearing*] (statement of Larry Amerson, Sheriff, on behalf of the National Sheriff's Association) (detailing how results from facial

The technology is not limited to identification through surveillance, however. Social media networks and digital providers employ the technology on their websites and mobile applications to enhance consumer experience as well as engage new users.[6] Both the public and private sectors use FRT for a growing list of business and security uses.[7] For example, retail stores can identify repeat shoplifters,[8] transportation agencies can positively verify passengers prior to any boarding,[9] companies can have their employees clock in with a face scan,[10] and cars can alert drowsy or distracted drivers.[11] In countries like Russia and Sweden, everyday citizens can use mobile phone apps to identify strangers on the street.[12] It is an inarguable fact that the ever-evolving science of facial recognition is a powerful tool in the hands of its user. But how exactly this technology is used, and how this use affects individuals and society as a whole, are topics that are hotly debated by FRT providers, consumers, legislators, academics, and rights advocacy groups.[13]

Many questions surround the appropriateness, legality, and even morality of facial recognition technology's ever-expanding capabilities, and its ever-growing prevalence in our modern society.[14] The technology has advanced at an astonishing pace in recent years, leading to its unchecked use in ways

---

recognition can be obtained in seconds); *see also* Thomas Ricker, *The US, Like China, Has About One Surveillance Camera for Every Four People, Says Report*, VERGE (Dec. 9, 2019 10:45 AM), https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens (explaining that the U.S. is nearly on par with China in terms of number of surveillance cameras).

[6] CHRISTOPHER ANGLIM, ET AL. PRIVACY RIGHTS IN THE DIGITAL AGE 192 (Grey House Publishing ed., 2016).

[7] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY REPORT 32 (2015) [hereinafter *GAO Report*] (noting that the use of biometrics in the business and security screening sectors was growing).

[8] Brinckerhoff, *supra* note 1, at 113.

[9] *Facial Recognition Technology: Part II: Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 8 (2019) [hereinafter *Transparency Hearings*] (statement of Austin Gould, Assistant Administrator, Requirements and Capabilities Analysis, Transportation Security Administration).

[10] Khari Johnson, *Congress Moves Toward Facial Recognition Regulation*, VENTUREBEAT (Jan. 15, 2020 11:27 AM), https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation/.

[11] Mark Phelan, *2020 Subaru Models Will Greet You, Help You Keep Your Eyes on the Road*, DETROIT FREE PRESS (Aug. 3, 2019 7:44 PM), https://www.freep.com/story/money/cars/mark-phelan/2019/08/03/subaru-driverfocus-outback-forester-legacy/1903279001/.

[12] Brinckerhoff, *supra* note 1, at 113.

[13] *See generally Privacy and Civil Liberties Hearing, supra* note 5.

[14] *See* Seema Mohapatra, *Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation*, 43 PEPP. L. REV. 1017, 1024 (2016) (explaining that different privacy and ethical concerns are raised with the use of FRT in medical, commercial, and security applications).

that alarm everyone from legislators to watchdog groups to even developers of FRT themselves,[15] who observe that it is being used in ways that potentially violate fundamental rights.[16] Due process advocates contend that FRT allows the government to monitor our every move which violates our right to privacy.[17] FRT developers and consumers also collect and use millions of photos obtained from civilians without their knowledge or consent, constituting a separate violation of privacy.[18] Civil liberties groups contend that awareness that the government is watching us and using FRT to identify us chills associational and expressive freedoms.[19] Civil rights advocates meanwhile are drawing attention to the fact that FRT seems to disproportionately affect minorities and certain socioeconomic groups.[20]

In spite of these and other growing concerns over the years, the federal government has failed to enact laws that explicitly regulate the use of FRT.[21]

---

[15] *See* Peter Trepp, *How Face Recognition Evolved Using Artificial Intelligence*, FACEFIRST (Jan. 07, 2020), https://www.facefirst.com/blog/how-face-recognition-evolved-using-artificial-intelligence/ (noting the number of FRT milestones since 2010 to highlight the speed with which it has developed); *see also* Shirin Ghaffary, *How To Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation (noting legislators' push for limiting FRT use by law enforcement, and Microsoft's and IBM's calls for government regulation of the FRT industry); *see also* Mike Masnick, *Facial Recognition Company Says It Won't Sell to Law Enforcement, Knowing It'll Be Abused*, TECHDIRTY (June 29, 2018 1:30 PM), https://www.techdirt.com/articles/20180627/17283340123/facial-recognition-company-says-it-wont-sell-to-law-enforcement-knowing-itll-be-abused.shtml (describing FRT developer Kairos' refusal to sell the technology to law enforcement because they would likely abuse and misuse it).

[16] *See* Nakar & Greenbaum, *supra* note 2, at 93 ("Perhaps most disconcerting about all of this is that we often don't know when FRT is employed, either by the government or by private actors. Moreover, we don't know, and might never know how that data is processed, correlated and used to discern new and potentially damaging information about us. Living with all of these unknowns can create substantial and pervasive harms, including, intentional or unintentional censorship, control and inhibition of our actions, and the emotional harm of constant monitoring.").

[17] *See infra* Section II.B.ii.

[18] *Id.*

[19] Nakar & Greenbaum, *supra* note 3, at 115.

[20] *See Facial Recognition Technology: (Part I) Its Impact on Our Civil Rights and Liberties: Before the H. Comm. on Oversight & Reform*, 116th Cong. 21 (2019) [hereinafter *Impact Hearing*] (statement of Andrew G. Ferguson, Professor of Law, Univ. of the D.C., David A. Clarke School of Law); *see also* Olivia Solon, *Facial Recognition Database Used by FBI is Out of Control, House Committee Hears*, GUARDIAN (Mar. 27, 2017 6:00 AM), https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports ("Inaccurate matching disproportionately affects people of color").

[21] *See GAO Report, supra* note 7, at 28 ("[W]e did not identify any federal laws that expressly regulate commercial uses of facial recognition technology in particular."); *see also*

Thus, the proper gathering, storage, and use of biometric records–such as photos of faces–have been left to the states to determine.[22] Where states have not acted, developers and users of FRT find themselves free to manage the process, and reports on secret deals and questionable activities have led to increasing apprehension about their stewardship of the biometric data collected.[23] FRT developers are even racing to adapt their systems to facial coverings that have become ubiquitous in the COVID-19 pandemic, without any real consensus or requirements from consumers or regulators.[24]

With almost no U.S. laws governing police or private use of FRT, and no systems to ensure accuracy and bias-free results, some are calling this the wild west of biometrics.[25] This article examines the ways FRT is used in the United States and its impact, current and potential, on our society. Part II sets out the differing claims about its value and its drawbacks, as seen through the eyes of the major stakeholders: private service providers, consumers such as police departments and retail businesses, and rights advocates. Part III discusses past legal responses to address those claims, and the factors that helped shape those responses. The analysis in Part IV attempts to draw from

---

Brinckerhoff, *supra* note 1, at 107 (explaining that in the US there is no one comprehensive federal law regulating privacy and the gathering, use, and storage of personal information).

[22] *GAO Report, supra* note 7, at 32.

[23] *See Impact Hearing*, *supra* note 21, at 6- 7 (statement of Neema Singh Guliani, Senior Legis. Counsel, ACLU) (stating that the FBI and other agencies have been expanding the use of FRT, and mostly secretly); *see also* NANCY YUE LIU, BIO-PRIVACY: PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS, 73 (Routledge ed., 2012) (discussing the public's distrust of companies and government agencies handling their facial image data).

[24] *See* Mara Hvistendahl and Sam Biddle, *Homeland Security Worries Covid-19 Masks Are Breaking Facial Recognition, Leaked Document Shows*, THE INTERCEPT (July 16, 2020 2:10 PM), https://theintercept.com/2020/07/16/face-masks-facial-recognition-dhs-blueleaks (noting that FRT developers are "scrambl[ing] to adapt their systems to facial coverings"); *see also* Wudan Yan, *Face-Mask Recognition Has Arrived—For Better or Worse*, NAT'L GEOGRAPHIC (Sept. 11, 2020), https://www.nationalgeographic.com/science/2020/09/face-mask-recognition-has-arrived-for-coronavirus-better-or-worse-cvd (noting concern among experts about the lack of rules and federal guidelines with regard to data collection and use); *see also* Susan Miller, *Facial Recognition Adapts to a Mask-Wearing Public*, GCN (June 3, 2020), https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx (citing FRT developer NEC's advice to customers like the U.S. Customs and Border Patrol to "make their own decisions about the [updated] technology for now").

[25] *See* Ephrat Livni, *Facial-Recognition Technology Will Make Life a Perpetual Police Lineup For All*, QUARTZ (Mar. 26, 2017), https://qz.com/940979/facial-recognition-technology-will-make-life-a-perpetual-police-lineup-for-all (quoting Clare Garvie's comparison of the regulation and standard-free panorama to "a wild west"); *see also* DJ Pangburn, *Due To Weak Oversight, We Don't Really Know How Tech Companies Are Using Facial Recognition Data*, FAST COMPANY (July 5, 2019), https://www.fastcompany.com/90372734/due-to-weak-oversight-we-dont-really-know-how-tech-companies-are-using-facial-recognition-data ("It's every company for itself, it's the Wild West—there are no rules, there aren't any industry best practices").

current FRT trends a prediction of its practical and legal future in the U.S. Part V will evaluate the effectiveness of past responses and possible alternatives. In addition, it will propose solutions for this important struggle to balance the usefulness of FRT with individual rights, a difficult dilemma that America needs to solve sooner rather than later.[26]

B. A Leap in Biometric Data

Understanding the debates surrounding the use of FRT and its implications on individual rights requires at minimum a high-level explanation of biometrics and what facial recognition is. A person's biometric data are generally biological or behavioral features that are unique and verifiable, like fingerprints or voiceprints, which are used for identification purposes.[27] In FRT, the biometric is our facial image, which the technology uses to generate a digital file, or faceprint, after it has mapped out unique features that can be compared against other faceprints.[28] FRT analyzes and measures a person's features or behavioral characteristics in four steps.[29] It first detects a face in an image, and then analyzing the person's physical characteristics, uses an algorithm to create the faceprint.[30] Another algorithm then either verifies identity by accepting or denying the identity claimed, or it identifies the person by matching them to a database of known people.[31] The success of the technology is dependent upon the size of the database it has to draw upon; FRT thus requires an extensive number of faceprints for accurate results.[32]

---

[26] *See* AMOS N. GUIORA, CYBERSECURITY: GEOPOLITICS, L. & POL'Y, 77 (Routledge ed., 2017) (explaining that democratic societies like the U.S. must balance things like national security and the rights of individuals if they are to retain their character and purpose).

[27] Jeffrey Rosenthal & David Oberly, *Biometric Privacy In 2020: The Current Legal Landscape*, LAW360 (Feb. 3, 2020, 5:59 PM), https://www.law360.com/articles/1239794/biometric-privacy-in-2020-the-current legal-landscape [hereinafter Rosenthal & Oberly, *Legal Landscape*].

[28] Kimberly L. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 427 (2014).

[29] ANGLIM, *supra* note 6, at 190.

[30] *GAO Report, supra* note 8, at 3.

[31] ANGLIM, *supra* note 6, at 190.

[32] *See* Adrienne Lafrance, *The Ultimate Facial-Recognition Algorithm*, ATLANTIC (June 28, 2016), https://www.theatlantic.com/technology/archive/2016/06/machine-face/488969 (explaining that large datasets are needed to properly test the accuracy of FRT).

II. CONFLICTING CLAIMS AND PERSPECTIVES

A. Facial Recognition Technology Supporters

1. Creators and Vendors

The current technology has been created and developed by tech giants such as Amazon and Google, as well as lesser known companies who have worked hard to make it as ubiquitous as global positioning system (GPS) tracking.[33] Nowadays, facial recognition is commonly used to log in to a computer, authenticate a credit card transaction, or identify loved ones in photo management software.[34] FRT innovators minimize privacy concerns, preferring instead to tout the growing list of benefits that go beyond the convenience or "cool" factors.[35] For example, FRT is used to search through criminal mug shots to generate potential suspects, saving law enforcement agencies precious time and manpower.[36] FRT has also been used to locate missing persons as well as to identify unknown individuals.[37] In recent years, scientists have been able to use FRT to help diagnose around ninety rare genetic conditions using ordinary family photos.[38] FRT companies continue to push for more uses and better results, generally expressing a more nuanced view on the privacy rights of the people whose photos they use in the name of those technological advancements.[39]

FRT developers are also quick to point out that Americans have demonstrated a willingness to share private details about themselves,

---

[33] *See GAO Report, supra* note 7, at 6 (acknowledging that FRT is widely used commercially but the full extent of FRT is unknown); *see also* Trepp, *supra* note 15 (describing FRT as a feature as common in consumer products like GPS).

[34] *See* Rosenthal & Oberly, *Legal Landscape*, *supra* note 27 (describing common uses of biometric data).

[35] *See* Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT ON THE ISSUES (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ (stating that FRT has created "many new and positive benefits for people around the world.").

[36] See *Transparency Hearings*, *supra* note 9, at 3 (statement of Kimberly J. Del Greco, Deputy Assistant Director, Crim. Justice Information Services, Federal Bureau of Investigation) (explaining the general process of the FBI's FRT in assisting investigations).

[37] *See* Smith, *supra* note 35 (describing how FRT identified thousands of missing children in India in just four days, and how historians used FRT to identify previously unknown Civil War soldiers).

[38] Mohapatra, *supra* note 14, at 1022.

[39] *See* ANGLIM, *supra* note 6, at 190 (explaining how FRT is become more accurate every day); *see also Transparency Hearings*, *supra* note 9, at 4 (statement of Kimberly J. Del Greco) (describing the improved accuracy rate of the FBI's facial recognition program).

including their images, on a growing number of online sites.[40] Consumers almost immediately embraced facial recognition as a convenient means for accessing smartphones and tagging pictures, and as other industries incorporate FRT into their products, consumer demand for the technology has risen.[41] In response, tech giants Amazon, Apple, Facebook, Google, and Microsoft have each filed facial recognition patent applications.[42] Additionally, developers argue that Americans do not see FRT as exceedingly invading their privacy for two principal reasons. First, the data is collected in public, where people tend to expect less privacy and anonymity.[43] Second, most people feel collecting a photo of a person is not as intrusive as other biometrics such as fingerprints.[44] Thus, FRT providers argue most people are willing to endure some loss of privacy in exchange for the technology's benefits, which include convenience, security, but also the tremendous economic growth it has brought about.[45] Thanks to its multi-purpose nature, analysts predict the facial recognition market will reach over $12 billion by 2025.[46]

2. Consumers of Facial Recognition Technology

Businesses in the private sector have steadily become supporters of FRT, finding commercial potential in innovative, industry-specific applications of the technology.[47] Retail stores and shopping malls, for instance, employ the

---

[40] *See* ANGLIM, *supra* note 6, at 190 (Grey House Publishing ed., 2016) (describing how individuals create a FRT repository by uploading billions of photographs to the internet).
[41] *See* Nakar & Greenbaum, *supra* note 2, at 93 (explaining that facial recognition systems will become more pervasive thanks to strong consumer demand).
[42] Natasha Singer, *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, N.Y. TIMES (July 9, 2018), https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html.
[43] YUE LIU, *supra* note 23, at 171.
[44] *Id.* at 30.
[45] *See* GUIORA, *supra* note 26, at 28 (discussing a willingness to tolerate impositions on privacy in the name of protection); *see also* ANGLIM, *supra* note 6, at 191 (asserting various trade-offs that FRT provides).
[46] *See* Nakar & Greenbaum, *supra* note 2, at 96 ("FRT is already implemented in many areas such as security, commerce, social media, personal use, and even for religious purposes."); *Facial Recognition Market to Hit $12 Billion by 2025 - Global Insights on Top Trends, Key Technologies, Competitive Landscape, New Investments, Strategic Initiatives, and Business Opportunities: Adroit Market Research*, GLOBENEWSWIRE (last visited Apr. 21, 2020), https://www.globenewswire.com/news-release/2020/01/27/1975200/0/en/Facial-Recognition-Market-to-hit-12-billion-by-2025-Global-Insights-on-Top-Trends-Key-Technologies-Competitive-Landscape-New-Investments-Strategic-Initiatives-and-Business-Opportun.html [hereinafter *Facial Recognition Market to Hit $12 Billion*].
[47] *See* Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, INTELLIGENCER (Oct. 20, 2018), https://nymag.com/intelligencer/2018/10/retailers-

technology, using security cameras as well as cameras in digital signs and kiosks, to track shoppers' habits and gauge their attention to ads.[48] Retailers and advertisers can then adjust advertisements accordingly in real time, which can potentially lead to more sales.[49] Restaurants are using FRT to enhance customers' ordering experience, allowing them to use self-service kiosks to quickly and easily reorder their favorite meals.[50] Simplifying this process often means more orders for the restaurant and the ability to shift labor to other areas of need.[51]

A growing number of business establishments are also using FRT to enhance service for repeat customers or deny service to *personae non gratae*.[52] Hotels are beginning to use facial recognition to welcome returning guests with personalized greetings and speedy check ins.[53] Cruise lines use FRT to facilitate faster embarkation and debarkation of passengers, as well as to help them access photos of themselves taken throughout their cruise.[54] In the hospitality industry, these kinds of measures, which provide for a more personalized and frictionless customer experience, are key to attracting and retaining loyal customers,[55] a principal source of revenue. The private sector additionally uses FRT for risk management: stores large and small use it to

---

are-using-facial-recognition-technology-too.html (describing various uses of FRT in retail stores).

[48] Tabor, *supra* 47; *see also* Debra Cassens Weiss, *Macy's Uses Facial Recognition Software to Identify Customers on Security Cameras, Lawsuit Claims*, ABA JOURNAL (Aug. 12, 2020 3:36 PM), https://www.abajournal.com/news/article/suit-claims-macys-uses-facial-recognition-software-to-identify-customers-on-security-cameras (detailing a lawsuit filed in Illinois against Macy's alleging the retailer used FRT to identify unknowing customers for improved marketing and security).

[49] *GAO Report, supra* note 7, at 9.

[50] *When Restaurant Tech Sees Your Face and Identifies Your Taste*, PYMNTS (Nov. 5, 2019), https://www.pymnts.com/restaurant-innovation/2019/malibu-poke-facial-recognition-technology-self-service-kiosks/.

[51] *Id.*

[52] *See* Brinckerhoff, *supra* note 1, at 114 (describing how FRT can be used to identify repeat customers as well as previous shoplifters).

[53] *E.g.*, Frank Wolfe, *Facial-Recognition Tech Creates Service, Security Options*, HOTEL MANAGEMENT (Oct. 10, 2019 11:11AM), https://www.hotelmanagement.net/tech/facial-recognition-tech-creates-service-security-options; *Facial Recognition in Retail & Hospitality*: Cases, Benefits, Laws, INTELLECTSOFT (Apr. 17, 2019) https://www.intellectsoft.net/blog/facial-recognition-in-retail-and-hospitality/.

[54] *Facial Recognition Technology*, CARNIVAL.COM, https://help.carnival.com/app/answers/detail/a_id/6019/~/facial-recognition-technology (last visited Apr. 21, 2020).

[55] *See 3 Ways Facial Recognition Tech Can Generate Revenue for Hotels*, HOSPITALITY TECHNOLOGY (Aug. 8, 2018), https://hospitalitytech.com/3-ways-facial-recognition-tech-can-generate-revenue-hotels (discussing three advantages to using FRT in the hospitality industry: creating enhanced customer experiences, augmenting a hotel's customer database, and increased security).

alert to previously identified shoplifters, and casinos use it to keep card counters out.[56] Moreover, the technology has been used in locations such as amusement parks and stadiums to ensure the safety of attendees; FRT has helped reunite lost children with their parents,[57] scan selfie-kiosks at concerts for known stalkers,[58] and detect persons banned from being on public school grounds.[59] With FRT developers providing the private sector with products that both generate revenue and limit risk, the technology is likely to continue enjoying support from those private organizations.[60]

Security being a top priority across all industries, FRT creators have marketed the technology to consumers in the public sector as well.[61] Law enforcement authorities have joined the growing group of agencies who purport to use FRT as an investigative tool.[62] The technology can be used when fingerprint identification fails, or when a suspect is uncooperative in identifying himself.[63] Recent studies have even demonstrated FRT algorithms are better than humans at identifying individuals from images captured under different lighting conditions.[64] Recognizing how FRT can enhance crime-solving and counter-terrorism capabilities, federal agencies like the Federal Bureau of Investigation ("FBI") have collaborated with over two dozen states to share databases and increase the likelihood of identification.[65] FRT supporters point to success stories, such as the positive

---

[56] Nakar & Greenbaum, *supra* note 2, at 99.

[57] *See* Singer, *supra* note 42 (relating Amazon's claim that its FRT is used at parks to find lost children).

[58] *See* Lane Brown, *There Will Be No Turning Back on Facial Recognition*, INTELLIGENCER (Nov. 12, 2019), https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html (explaining how FRT was used at several Taylor Swift concerts to check for known stalkers of the artist).

[59] Tom Simonite & Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, WIRED (Oct. 17, 2019 6:00 AM), https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.

[60] *See GAO Report, supra* note 7, at 7–10 (citing several different commercial uses for FRT).

[61] *See* Singer, *supra* note 42 (citing Amazon's marketing of its FRT to police departments); *see also GAO Report, supra* note 7, at 8–9 (listing the different commercial and security uses of FRT in the private sector).

[62] *See Transparency Hearings*, *supra* note 9, at 4 (statement of Kimberly J. Del Greco).

[63] *Id.* at 3 (statement of Kimberly J. Del Greco); *see also* Cade Metz & Natasha Singer, *Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities*, N.Y. TIMES (June 29, 2018), https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html (describing the use of FRT to identify the suspect in the Capital Gazette killings).

[64] *See* RACHEL B. JEFFERSON, BIOMETRICS, PRIVACY, PROGRESS, AND GOVERNMENT, 31 (Nova Science Publishers ed., 2010).

[65] *See Privacy and Civil Liberties Hearing, supra* note 6, at 19 (statement of Larry Amerson) (extolling the ways FRT helps authorities fight terrorism and protect society at large); *see also* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CTR. ON PRIVACY & TECH. (Oct. 18,

identification of imposters attempting to enter the U.S.,[66] and the capture of a pedophile who had eluded law enforcement for 20 years.[67] Government agencies such as the Transportation Security Administration ("TSA") and the U.S. Customs and Border Protection ("CBP") are using FRT at checkpoints across the nation, which they claim increases security effectiveness and enhances travelers' experience.[68] But the most common use of FRT by law enforcement is also the most controversial one: surveillance.

Given its origins in defense and law enforcement, it is unsurprising that surveillance is where facial recognition would truly surpass all other technologies.[69] The United States has approximately seventy million surveillance cameras installed, which is roughly one camera per four people, rivalling China's per person camera penetration rate.[70] Taken together with the fact that law enforcement facial recognition networks contain the images of over 117 million American adults and that the technology is continually improving in accuracy, authorities wield a powerful weapon that can be used to identify anyone practically anywhere, as well as monitor their every movement.[71] Agencies that use FRT for surveillance claim the goal is to ensure the security of the public, which is accomplished by running captured images against their databases in search for persons on a "hot list."[72] However, there are no laws establishing guidelines on the process, much less limits on its use.[73]

In 2015, police in Baltimore used FRT in conjunction with a social media platform to identify participants at a protest over the police shooting of

---

2016), https://www.perpetuallineup.org/ (explaining that FBI and law enforcement face recognition systems are increasingly accessing state driver license and ID photo databases).

[66] *See* TRANSPORTATION SECURITY ADMINISTRATION AND U.S. CUSTOMS AND BORDER PROTECTION: DEPLOYMENT OF BIOMETRIC TECHNOLOGIES REPORT TO CONGRESS, U.S. DEPT. OF HOMELAND SECURITY 17 (Aug. 30, 2019) [hereinafter TSA BIOMETRIC REPORT] (noting that as of April 2019, CBP had identified 130 imposters attempting to cross U.S. borders); *see also* Tajha Chappellet-Lanier, *CBP's Airport Facial Recognition Technology Catches Its First 'Imposter'*, FEDSCOOP (Aug. 24, 2018), https://www.fedscoop.com/cbp-facial-recognition-success/ (detailing the capture of a Congolese man attempting to use a French passport to clear an airport checkpoint).

[67] *See Transparency Hearings*, *supra* note 10, at 12 (testimony of Kimberly J. Del Greco).

[68] *Id.* at 12 (2019) (statement of Austin Gould).

[69] *See* Trepp, *supra* note 16 (explaining that FRT's roots are "firmly planted in the defense and law enforcement sectors.").

[70] *See* Ricker, *supra* note 6.

[71] *See* Garvie, Bedoya, & Frankle, *supra* note 66 (noting that over 117 million American adults are in law enforcement face recognition networks); *see also* L. Brown, *supra* note 59 (citing NIST test results in 2018 that were twenty times better than those in 2014).

[72] Garvie, Bedoya, & Frankle, *supra* note 66.

[73] *See Impact Hearing*, *supra* note 21, at 11 (statement of Cedric Alexander, former President, National Organization of Black Law Enforcement Executives).

Freddie Gray.[74] Officers were able to discover protesters with outstanding warrants and arrest them on the spot, during the exercise of their First Amendment right to assemble.[75] And while many would assume the police would infringe on fundamental rights only in the name of capturing the most dangerous of criminals, some police departments have taken to using facial recognition to apprehend even non-violent suspects.[76] With private business and home camera owners increasingly willing to plug their units into police networks to help the fight against crime, law enforcement agencies could soon have a vast network of cameras at their disposal, giving them complete surveillance of public spaces, [77] and without any laws, regulations, or checks systems.[78]

B. Rights Advocates

1. Consent is Key

In an era where consent is generally required, oftentimes even for the most banal of activities, opponents of FRT note that this technology has proliferated without express or sometimes even implied consent from the individuals whose photos developers use.[79] The vast majority of Americans are unaware that their photos have been taken, stored, used, and even sold by developers as the technology continues to evolve.[80] The data can also be

---

[74] *Id*. at 54 (statement by Rep. Elijah Cummings, Chairman of the Committee).
[75] *Id*.
[76] *See* Nakar & Greenbaum, *supra* note 3, at 97 (describing use of FRT to apprehend non-violent offenders).
[77] *See* Kwet, *supra* note 4 (describing the pervasiveness of cameras in public spaces).
[78] *See Impact Hearing*, *supra* note 21, at 11 (statement of Cedric Alexander).
[79] *See* Nakar & Greenbaum, *supra* note 3, at 96 (addressing concerns over consent and FRT).
[80] *See* Lauren Berg, *AI Biz Kept 'Face Database' Of OKCupid Profile Pics, Suit Says*, LAW360 (Feb. 14, 2020, 8:59 PM), https://www.law360.com/cybersecurity-privacy/articles/1244342/ai-biz-kept-face-database-of-okcupid-profile-pics-suit-says?nl_pk=9a283bed-c005-42eb-aa84-e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy ("Clarifai Inc., an artificial intelligence company . . . secretly harvested the profile pictures of tens of thousands of users on the dating site OKCupid . . ."); *see also* Delia Paunescu, *The Government Keeps Its Use of Facial Recognition Tech Secret. The ACLU is Suing.*, VOX (Nov. 7, 2019 5:00 PM) https://www.vox.com/recode/2019/11/7/20953655/facial-recognition-technology-government-fbi-aclu-lawsuit-reset-podcast ("[B]ig tech companies like Amazon and Microsoft have been selling facial recognition tech to various companies for business purposes while Amazon is also selling its facial recognition capabilities directly to law enforcement agencies, despite the fact that most citizens have never consented to their faces being used for these purposes."); *see also* Solon, *supra* note 21 ("Approximately half of adult Americans' photographs are stored in facial recognition databases that can be accessed by the FBI, without their knowledge or consent . . .").

accessed by any government agency for any reason.[81] No doubt most people would be shocked to learn that the FBI has three facial recognition programs and access to over 640 million photos: only 36 million are criminal mug shots, the rest are civil in nature, passport and driver license photos of everyday law-abiding citizens.[82] Because the makers of FRT and their customers are not required to obtain consent from anyone or report any details on how the technology is being used, Americans are purposely kept in the dark as to when and how FRT is employed, and what happens to their data over time.[83] Furthermore, this lack of transparency allows FRT users to cover up data breaches and escape higher accountability for the mishandling of data, despite public scrutiny.[84] If facial recognition is here to stay, critics argue, the public must be notified when and how their data is being used, stored, and shared, and affirmative consent must be obtained beforehand.[85]

2. Due Process: Privacy Rights in Play

The right to privacy has been recognized as a fundamental human right

---

[81] *See* Josiah Wolfson, *The Expanding Scope of Human Rights in a Technological World--Using the Inter-American Court of Human Rights to Establish a Minimum Data Protection Standard across Latin America*, 48 U. MIAMI INTER-AM. L. REV. 188, 193 (2017) (explaining that an individual's private data may be: "(1) sold to private companies; (2) processed anywhere in the world; (3) accessed by a government agency without just cause; (4) stored for an indefinite period of time; and (5) used for an unintended purpose.").

[82] *See Transparency Hearings*, *supra* note 10, at 35, 47 (testimony of Dr. Gretta L. Goodwin, Director, Justice and Law Enforcement Issues, Homeland Security and Justice Team, U.S. Government Accountability Office).

[83] *See* Nakar & Greenbaum, *supra* note 3, at 93 (stating "we often don't know when FRT is employed, either by the government or by private actors"); *see also* Celeste Bott, *Surveillance Co. Clearview AI Hit With Biometric Privacy Suit,* LAW360 (Feb. 6, 2020 3:56 PM), https://www.law360.com/articles/1241502/surveillance-co-clearview-ai-hit-with-biometric-privacy-suit (describing a FRT company's covert harvesting of Illinois residents' photos and biometric data for profit).

[84] *See* John Fingas, *FTC Fines TikTok $5.7 Million Over Child Privacy Violations*, ENGADGET (Feb. 27, 2019), https://www.engadget.com/2019/02/27/ftc-fines-tiktok-over-child-privacy/ (citing social media company TikTok's $5.7 million penalty for collecting data from minors without appropriate consent, and making the profiles public despite "thousands of complaints"); *see also* Craig Giles & Zahra Deera, *TikTok Investigation Should Prompt More Data Transparency*, LAW360 (Feb. 21, 2020 4:27 PM), https://www.law360.com/cybersecurity-privacy/articles/1245489/tiktok-investigation-should-prompt-more-data-transparency?nl_pk=9a283bed-c005-42eb-aa84-e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy (describing criticism of social media companies' secrecy of or failure in the handling of user data).

[85] *See Impact Hearing*, *supra* note 21, at 22, 30 (testimony of Joy Buolamwini, Founder, Algorithmic Justice League).

worldwide, and in the U.S. it is a protected right under the Fourth Amendment to the Constitution.[86] The illegal sharing of a person's sensitive information constitutes an invasion of privacy, a violation that becomes prevalent in times of war and terrorism, or under certain types of government.[87] During World War II for example, Nazi Germany partnered with International Business Machines (IBM) to create a system for collecting and synthesizing the data of the Jewish population in order to facilitate the Nazi master plan.[88] Today, civil liberties groups draw parallels to the collaborations between corporations like Amazon and government entities like police departments and Immigration and Customs Enforcement ("ICE").[89] It was recently revealed, for example, that unbeknownst to state residents, ICE uses FRT to check millions of driver license photos to find and deport undocumented immigrants, despite many of them having legally obtained those licenses in states like Washington, Utah, and Vermont.[90] In New York City, meanwhile, close to 3,000 arrests have been made using FRT, but most of the accused were not informed that FRT was used to identify them.[91] These and other examples of the intrusive nature of facial recognition and the serious consequences it can yield cause activists and academics alike to warn organizations that if they continue to ignore ethical concerns in their dealings, they run the risk of repeating the sins of IBM in the Nazi era.[92]

Rights activists also point out another disturbing trend that impinges on our right to privacy: beyond recorded and real-time surveillance, FRT is capable of identifying patterns, which pieced together become new

---

[86] U.S. CONST. amend. IV ("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."); *see also* G.A. Res. 217A (III), Art. 12, U.N. Doc. A/810 (1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . .").

[87] Alvar Freude and Trixy Freude, *Echoes of History: Understanding German Data Protection*, BERTELSMANN FOUNDATION (Oct. 1, 2016), https://www.bfna.org/politics-society/echoes-of-history-4tdtdjes5l/ .

[88] Wolfson, *supra* note 82, at 190.

[89] Anthony Cuthbertson, *Amazon Workers' 'Refuse' To Build Tech For US Immigration, Warning Jeff Bezos of IBM's Nazi Legacy,* INDEPENDENT (June 22, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-workers-immigration-jeff-bezos-ibm-nazi-protest-a8411601.html.

[90] Bill Chappell, *ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019 4:23 PM), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa.

[91] *Impact Hearing*, *supra* note 21, at 34 (testimony of Clare Garvie, Senior Associate, Center on Privacy & Technology, Georgetown University Law Center).

[92] Cuthbertson, *supra* note 90.

information that can be used to predict a person's movements.[93] By stringing together data collected over time from different cameras at different locations, FRT can predict where you will go next and what you will do, a kind of predictive analytics that can be used –and abused– by private businesses and law enforcement alike.[94] Rights advocates warn that the government in particular has access to multiple points of data (i.e. surveillance footage, phone call and email records, financial transactions, crime statistics) that make this kind of predictive analytics possible.[95] However, the Supreme Court in *Carpenter v. United States* recently held that using cell phone records to determine a suspect's locations over an extended timeframe amounted to a warrantless search under the Fourth Amendment and thus violated his right to privacy because such data could potentially reveal intimate details of his life that go beyond being spotted in public thoroughfares.[96] Thus, were FRT to be used to secretly gather data on a person's movements over an extended period of time, the Court could find that it too constitutes a violation of privacy rights.[97]

3. First Amendment Rights at Risk

Under the First Amendment to the Constitution, Americans have a right to freely express themselves and assemble peacefully.[98] Decades of jurisprudence have led to our conviction that government actions that tend to have a chilling effect on the open exchange of ideas or the free association of persons are an unconstitutional burden on our First Amendment rights.[99]

---

[93] *See* K. Brown, *supra* note 29, at 466 (explaining that FRT "identif[ies] patterns within such data which reveal new information that does not exist anywhere in isolation").

[94] *See* Nakar & Greenbaum, *supra* note 3, at 93 (citing the fact that although we know FRT can be used to glean new information, FRT users do not disclose "how that data is processed, correlated and used to discern new and potentially damaging information about us"); *see also* Smith, *supra* note 36 (explaining how biometric data could potentially be exploited by business).

[95] K. Brown, *supra* note 29, at 426–27.

[96] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (finding that the data on the suspect's locations over a four-month period constituted a warrantless search that violated his Fourth Amendment right to privacy).

[97] *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A. (last visited Apr. 21, 2020) https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

[98] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . or the right of the people peaceably to assemble . . . ").

[99] *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166–67 (2002) (holding that a permit requirement for door-to-door solicitation placed an undue burden on the freedom of expression because it would inhibit some speech by persons wishing to remain anonymous, as well as outright ban spontaneous speech); *see also* Lamont

Courts have additionally upheld an individual's right to anonymous speech and association.[100] Opponents of FRT point out that the technology is often sold –secretly– to government agencies without the proper training or understanding of its unintended consequences.[101] As a result, FRT users are often either unaware or unconcerned that facial recognition can undermine free expression, free association, privacy, and anonymity, especially when used to target people at political events, protests, religious meetings, and other types of public gatherings where anonymity and the freedom to assemble are expected.[102]

In 2015, the United States Government Accountability Office ("GAO") issued a report warning that widespread and unregulated use of FRT could give businesses, government agencies, and even individuals the ability to identify (or misidentify) and track almost anyone in public without their knowledge or consent.[103] Just a few years later, there are multiple instances of the prophecy fulfilled: FRT company Clearview AI is facing a class action suit over its secret extraction and subsequent sale of individuals' photographs and biometric data;[104] cities like Chicago and Detroit have sophisticated surveillance networks running real-time facial recognition through hundreds of public and private cameras at parks, schools, churches, apartment buildings, and immigration centers;[105] and police investigators are manually editing low-quality and distorted photos in hopes of creating more matches and thus more arrests.[106]

There are many activities that require varying degrees of anonymity for people to freely participate and exercise their First Amendment rights. Political rallies, street protests, and houses of worship usually offer a measure

---

v. Postmaster Gen., 381 U.S. 301, 302, 307 (1965) (finding unconstitutional a statute preventing the U.S. Postal Service from delivering "communist political propaganda" to addressees unless they request to receive it, because it serves as a deterrent due to the sensitive nature of the material).

[100] *See* Talley v. California, 362 U.S. 60, 64 (1960) (holding that an ordinance barring the anonymous distribution of handbills restricts the freedom of expression and is thus unconstitutional); *see also* NAACP v. Alabama, 357 U.S. 449, 466 (1958) (finding Alabama's ban on the activities of NAACP lawyers and its demand to see the group's membership lists a violation of the members' rights to pursue their interests privately and to associate freely with others).

[101] *See Impact Hearing*, *supra* note 21, at 27 (testimony by Dr. Cedric Alexander).

[102] *See* Solon, *supra* note 21.

[103] *See GAO Report, supra* note 8, at 13, 17.

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

[105] See *Impact Hearing*, *supra* note 21, at 1–2 (statement of Rep. Rashida Tlaib).

[106] *See* Drew Harwell, *Police Have Used Celebrity Look-Alikes, Distorted Images to Boost Facial-Recognition Results, Research Finds*, WASH. POST (May 16, 2019 6:12 PM), https://www.washingtonpost.com/technology/2019/05/16/police-have-used-celebrity-lookalikes-distorted-images-boost-facial-recognition-results-research-finds/ [hereinafter Harwell, *Police Have Used Celebrity Look-Alikes*].

of inconspicuousness for participants to feel comfortable.[107] Other activities may require total anonymity for participation to occur, such as visiting a medical center, or meeting with a media outlet when the individual is a whistleblower.[108] As surveillance networks grow and more and more persons become aware that they may be identified in public settings, some may instinctively, or purposefully, begin to avoid visiting or gathering in certain locations and events, which civil liberties groups contend is the chilling effect that makes this use of FRT a violation of their rights.[109] Moreover, the public is increasingly understanding that FRT users amass astonishing amounts of data considered private or sensitive, with no legal requirements to disclose their use of it or to dispose of it in any way.[110] This too can contribute to self-censorship and inhibition.

4. Civil Rights: The Disparate Effects of Facial Recognition

Of particular concern to rights advocates is the disproportionate effect FRT has on communities of color and poor communities, especially since law enforcement has a verifiable history of targeting activists and marginalized communities for surveillance.[111] First, various studies have shown that the technology is still considerably less accurate on certain groups, such as women and people of color.[112] African Americans, Asians, and Native Americans are up to one hundred times more likely to be misidentified by FRT as compared to white men, a potentially devastating discrepancy considering police investigators mostly use FRT to identify criminal suspects.[113] Studies conducted by the National Institute of Standards and

---

[107] *See* Jake Laperruque, *Unmasking the Realities of Facial Recognition*, POGO (Dec. 5, 2018), https://www.pogo.org/analysis/2018/2/unmasking-the-realities-of-facial-recognition.
[108] *Id.*
[109] *See GAO Report, supra* note 8, at 14; *see also* Nakar & Greenbaum, *supra* note 3, at 115 ("Awareness that the Government may be watching chills associational and expressive freedoms."); K. Brown, *supra* note 29, at 434–35 ("People involuntarily experience 'selfcensorship and inhibition' in response to the feeling of being watched.").
[110] *See* ANGLIM, *supra* note 7, at 191 (describing how privacy groups and government agencies are publicly expressing the concerns over personal data gathering, sharing, and use without consumer consent); *see also* K. Brown, *supra* note 29, at 464 ("Currently, there are no laws requiring private entities to provide individuals with notice that they are collecting personal data using FRT, how long that data will be stored, whether and how it will be shared, or how it will be used."); Wolfson, *supra* note 82, at 192 (noting that media sources worldwide are repeatedly informing the public of how their data is being processed and the associated dangers).
[111] *See* Kwet, *supra* note 4 (noting that law enforcement agencies have targeted marginalized communities for surveillance).
[112] *See Impact Hearing*, *supra* note 21, at 10 (statement of Neema Singh Guliani).
[113] *See* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition*

Technology ("NIST"), which develops standards for new technology, also continue to show higher error rates in determining a person's gender, age, or race,[114] despite developers' acknowledgment of the problem and assertions that steps are being taken to correct it.[115]

Another concern is that FRT disproportionately harms minority and marginalized communities.[116] This occurs because these communities tend to be over-policed, resulting in disproportionately high arrest rates.[117] This in turn leads to African Americans being over-represented in mug shots and disproportionately subjected to facial recognition searches by the police.[118] Despite these disparities, there is still no independent testing nor standardized internal testing for the aforementioned error rates.[119] In addition, the use of FRT in certain processes, such as jury selection at a trial, can negatively impact individuals by yielding results based on potentially discriminatory assumptions of demographic groups.[120] For example, facial recognition programs analyze and interpret facial expressions while at the same time scraping data about the potential jurors from public records and social media platforms.[121] Some programs then cross reference that data with assumptions about specific groups of people, such as Asian and Latin Americans having leadership skills– precisely the kinds of propensity notions lawyers are not

---

Systems, Casts Doubt On Their Expanding Use, WASH. POST (Dec. 19, 2019 6:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ [hereinafter Harwell, *Federal Study*].

[114] *See* Harwell, *Federal Study*, *supra* note 114.

[115] *See* ANGLIM, *supra* note 7, at 190 (noting that FRT error rates continue to decline even as the technology improves); *see also* Smith, *supra* note 36 (acknowledging the demographic differentials in FRT).

[116] See *Impact Hearing*, *supra* note 21, at 10 (statement of Neema Singh Guliani).

[117] *See Transparency Hearings*, *supra* note 10, at 32 (statement of Rep. Eleanor Holmes Norton).

[118] *See* Solon, *supra* note 21 (noting the disproportionality of African Americans who are subjected to police facial recognition); *see also Transparency Hearings*, *supra* note 10, at 32 (statement of Rep. Eleanor Holmes Norton - describing the excessive policing of minority communities and that it leads to a higher number of mug shots of African Americans).

[119] *See* Garvie, Bedoya, & Frankle, *supra* note 66; *see also* Solon, *supra* note 21 (relating that the Government Accountability Office has noted concern over the FBI's assessment of its FRT accuracy, and its lack of testing for false positives or racial bias).

[120] *See* Todd Feathers, *This Company Is Using Racially-Biased Algorithms to Select Jurors*, VICE (Mar. 3, 2020, 1:00 PM), https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en_us/article/epgmbw/this-company-is-using-racially-biased-algorithms-to-select-jurors.

[121] *See* Gabrielle Orum Hernández, *Facial Recognition Technology Used in Jury Consulting*, LAW.COM (Apr. 17, 2017 4:41 PM), https://www.law.com/sites/almstaff/2017/04/17/facial-recognition-technology-used-in-jury-consulting/ (describing facial recognition programs created to aid in the jury selection process).

allowed to weigh in *voir dire*.[122] Because the program considers race or gender-based propensity arguments to reach conclusions on the most favorable jurors, some rights advocates explain this could essentially be "tech-washing [people's] racialized assumption of individuals," but without transparency from the developer it cannot be known for sure.[123] And limiting the potential for harm, they contend, should not be left "to the good will of the agencies that procure [FRT], the corporations that develop [it], nor their secretive ethics departments . . . ."[124]

5. The Potential for Abuse

Equally troubling for rights advocates is the potential for abuse. The FRT industry lacks the transparency, guidelines, and safeguards necessary to ensure it is not misused in error, or exploited in malice.[125] There are no reporting requirements FRT providers or government entities must comply with that would inform the public when and how the technology is being used, nor is there any guidance or oversight on its use.[126] The public is forced to simply trust the FRT handlers with their biometric data.[127] However, the growing number of scandals involving mismanagement of private data, combined with reports detailing the questionable ways the technology is being employed, highlight the risk of misuse by good and bad actors alike.[128]

---

[122]U.S. Patent Application No. 20,190,130,778, col. 2 sec. 0074–75 (available at http://www.freepatentsonline.com/20190130778.pdf). The patent is for Momus Analytics, a jury selection software that uses biometric data including FRT to aid lawyers in discerning which jurors could be most influential during deliberations. Momus uses some race-based propensity arguments, such as leadership being a likely trait for people of Asian, Central American, or South American descent, while people who describe their race as "other" are less likely to be leaders.; *see also* Feathers, *supra* note 121 (noting the existence of certain stereotypes such as the notion that Black jurors are more sympathetic than white ones, and how it can lead to underrepresentation in jury panels).

[123] *See* Feathers, *supra* note 121 (quoting Gonzaga University professor Drew Simshaw, who studies artificial intelligence and legal technology: "[W]e don't know if the data that's being used is relying on data that reflects inequality, prejudice, and discrimination in society. The proprietary nature of the services, the lack of transparency, and this black box issue present challenges.").

[124] *See* Cuthbertson, *supra* note 90.

[125]*Impact Hearing*, *supra* note 20, at 9 (giving the statement of Neema Singh Guliani).

[126] *See* Pangburn, *supra* note 26 (noting the lax regulations, weak government oversight, and lack of clear rules or guidelines with regard to FRT).

[127] *See* YUE LIU, *supra* note 23, at 74 (detailing how businesses and government agencies do not offer any way for people to verify their data is being used in the manner they claim).

[128] *See* Giles & Deera, *supra* note 84 (listing the scandals surrounding the mishandling of user data by TikTok, Google, and Facebook); *see also* Harwell, *Police Have Used Celebrity Look-Alikes*, *supra* note 106 (noting some unethical uses of FRT to apprehend criminal suspects, such as using altered photos, composite sketches, and celebrity shots when the

In Florida, for example, the Pinellas County Sheriff's Office runs a program it makes available to all Florida law enforcement agencies which allows them to search through thirty-three million driver-license and police photos.[129] There are no requirements of reasonable suspicion to run a search, and no requirement to disclose the use of FRT[130] in *Brady* evidence.[131] Meanwhile, apartment complexes are starting to use FRT to grant access to individuals as well as to "enhance security,"[132] which many residents find invasive and impractical given the issues with the technology and the way it is being used.[133] The use of FRT for these purposes gives the user a powerful control tool that, when used improperly, can restrict an individual's freedom and self-development.[134]

III. PAST LEGAL RESPONSES AND CONDITIONING FACTORS

A. GDPR: The Response Abroad

In the 1990s, the emerging digital revolution took the world by storm, and the late 1990s saw the commercialism of FRT.[135] European lawmakers passed an EU Directive[136] to govern such emerging technologies and activity, but these policies were unable to keep up with the breadth and speed of the

---

suspect's photo was incomplete or distorted).

[129] *See* Karen Gullo & Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, ELECTRONIC FRONTIER FOUNDATION (Mar. 12, 2019), https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain.

[130] *See* Garvie, Bedoya, & Frankle, *supra* note 65 (explaining how no state has yet passed laws that regulate police face recognition technology, nor has any state passed laws requiring the disclosure of facial recognition evidence to defense counsel).

[131] *See* Gullo & Lynch, *supra* note 129 (explaining that *Brady* evidence is information that could exonerate a defendant, such as knowing that the defendant was identified using a flawed process involving error-prone technology such as FRT).

[132] *See* Paris Martineau, *Cities Examine Proper—and Improper—Uses of Facial Recognition*, WIRED (Oct. 11, 2019 10:05 AM) https://www.wired.com/story/cities-examine-proper-improper-facial-recognition/ (describing the FRT currently deployed at a Manhattan apartment building and the push to install a FRT system at a Brooklyn, New York complex).

[133] *See* Martineau, *supra* note 132 (relating the reasons residents fought the implementation of FRT at their Brooklyn complex: it was often inaccurate, and it amounted to tenant harassment and an "extreme invasion of privacy").

[134] K. Brown, *supra* note 28, at 435.

[135] *Privacy and Civil Liberties Hearing, supra* note 5, at 14.

[136] *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR (last visited Apr. 21, 2020), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

revolution.[137] With the technological advancements came cyber threats, revelations by rogue insiders on the secret and often unethical manner in which state and private actors were gathering and using our data, and demands by private citizens to own and control their personal data.[138]

The European Union ("EU") recognizes data protection as a basic human right, as set out in Article 8 of the Charter of Fundamental Human Rights of the European Union.[139] Since the Charter's passing in 2000, the EU has steadily moved toward increased privacy protection and individual rights over personal data, and in 2016 it passed the General Data Protection Regulation ("GDPR"), which established uniform laws protecting consumer data and regulating its handling by any corporation who engages European citizens.[140] Thus, its effect is global because non-EU entities wishing to engage Europeans must abide by the GDPR.[141] Moreover, the GDPR applies when data is processed on equipment located in the EU, which prevents businesses from utilizing non-EU entities to sidestep the law.[142]

The GDPR qualifies biometrics as a special category of personal data, defining it as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[143] Recognizing the value of facial features because they are unique to an individual, it limits how organizations collect and use video surveillance and faceprints used for access control.[144] GDPR additionally requires data holders to employ cybersecurity controls to ensure that access to data is available only to those authorized to view it.[145] Finally, the GDPR requires an individual's active

---

[137] *See* Jocelyn Kryslik, *How the Evolution of Cybersecurity Has Led to GDPR*, BOBS GUIDE (Apr. 11, 2017), https://www.bobsguide.com/guide/news/2017/Apr/10/how-the-evolution-of-cybersecurity-has-led-to-gdpr/.

[138] *Id.*

[139] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, OCT. 26, 2012, 2012 O.J. (C 326) 391.

[140] *See* Carla Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 191 (2019).

[141] *Id.* at 191.

[142] W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 28 (A.B.A. Book Publishing ed., 2015).

[143] Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 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), 2016 O.J. (L 119) 34 [hereinafter GDPR].

[144] Mohammed Murad, *How Biometrics Complement GDPR Regulations,* IRIS ID (June 3, 2019), https://www.irisid.com/home-biometrics-complement-gdpr-regulations/.

[145] *Id.*

consent before a company can use his data.[146] The data must be collected and retained for specific and legitimate purposes, and must not be further processed in any way that is incompatible with either the specified purpose or the collection of the data.[147] Non-compliance can result in gargantuan penalties: up to €20 million or 4 percent of a company's annual worldwide revenue, whichever is greater.[148] By early 2020, 160,921 data breaches had been reported, with violators paying $126 million in fines. [149] Although significant, many in the EU believe these figures reflect "spotty enforcement" and "underwhelming fines,"[150] an indication Europeans will continue to enforce the GDPR, and eventually step up the penalties.

B. U.S. Regulations: The Response at Home

1. The Federal Level

The United States has no equivalent for some of the key EU regulations regarding data privacy.[151] The GDPR has, for all twenty-seven EU member states, strengthened privacy laws, recognized biometrics as protectible personal data, and enforced compliance.[152] Meanwhile, the U.S. federal government has engaged in what can be described as reactionary legislation, laws meant to address specific circumstances that have arisen with the proliferation of technology. For example, the Driver's Privacy Protection Act of 1994 restricts the sale of driver license photos to private parties, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 regulates the use and disclosure of an individual's health information, and the Gramm-Leach-Bliley Act of 1999, amended in 2015, restricts financial institutions' ability to share personal data.[153] However, the GAO has noted that none of these or other federal laws address biometric data broadly.[154] As a result, the laws do not extend to face recognition, nor can they extend to

---

[146] Llaneza, *supra* note 140, at 192.
[147] VOSS & WOODCOCK, *supra* note 142, at 17–18.
[148] Murad, *supra* note 144.
[149] Scott Ikeda, *GDPR Fines Top $126 Million With Over 160,000 Data Breaches Reported*, CPO MAGAZINE (Feb. 3, 2020), https://www.cpomagazine.com/data-protection/gdpr-fines-top-126-million-with-over-160000-data-breaches-reported/.
[150] *Id.*
[151] FEN OSLER HAMPSON & ERIC JARDINE, LOOK WHO'S WATCHING: SURVEILLANCE, TREACHERY, AND TRUST ONLINE 129 (Centre for International Governance Innovation ed., 2016).
[152] Kelly A. Wong, *The Face-Id Revolution: The Balance Between Pro-market and Pro-Consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 258 (2020).
[153] *GAO Report, supra* note 7, at 33.
[154] *Id.*

circumstances other than those explicitly covered by each law.[155]

The Federal Trade Commission ("FTC") has in recent years begun flexing its regulatory muscle in response to a string of data breach and misuse scandals. For example, in 2019 alone, the FTC was instrumental in securing a $700 million settlement from Equifax, a $136 million penalty against Google and a YouTube subsidiary, and a record $5 billion penalty against Facebook– the largest ever in U.S history, representing a whopping 23% of Facebook's 2018 profits.[156] In addition to the fine, Facebook was required to take specific measures to avoid future incidents, such as setting up higher-level oversight and submitting to more stringent audits.[157] Although high penalties and forced measures are generally good deterrents for improper corporate behavior, absent clear guidelines, there is still much controversy over what constitutes improper handling of biometric data.[158]

2. Cities and Agencies Rejecting Facial Recognition Technology

As more is learned about the scope of FRT and its potential for exploitation by unregulated interests, some government agencies and U.S. cities have chosen to ban the technology altogether in the absence of any realistic hope Congress will pass comprehensive legislation in the near future that either bans or curtails the technology.[159] San Francisco, Oakland, Portland, Berkeley, and the Boston suburbs of Somerville and Brookline have banned FRT.[160] Police departments and cities across the country are debating the merits and concerns of the technology and considering similar bans.[161]

---

[155] *Id.*

[156] *See* Allison Grande, *The Biggest Privacy & Cybersecurity Developments of 2019*, LAW360 (Dec. 20, 2019, 1:25 PM), https://www.law360.com/articles/1228763/the-biggest-privacy-cybersecurity-developments-of-2019 [hereinafter Grande, *The Biggest Privacy*] (touching on some of the most notable data breach cases of 2019); *see also* Allison Grande, *FTC, Facebook Say $5B Privacy Deal Benefits Consumers*, LAW360 (Jan. 27, 2020, 8:58 PM EST), https://www.law360.com/articles/1237786/ftc-facebook-say-5b-privacy-deal-benefits-consumers [hereinafter Grande, *FTC*] (noting the details of the deal reached between the FTC and Facebook).

[157] *See* Grande, *FTC*, *supra* note 156.

[158] *See GAO Report, supra* note 7, at *Preface* (noting the disagreement amongst stakeholders on what risks FRT presents and whether the loss of privacy is offset by its benefits).

[159] *See* Matt O'Brien, *Why Some Cities, States and Lawmakers Want to Curb Facial Recognition Technology*, USA TODAY (Dec. 17, 2019 6:56 PM) https://www.usatoday.com/story/tech/2019/12/17/face-recognition-ban-some-cities-states-and-lawmakers-push-one/2680483001/.

[160] *Id.*; Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the US*, , CNN BUSINESS (Sept. 9, 2020 8:06 PM), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

[161] *See* O'Brien, *supra* note 159 (citing the city of Springfield, Massachusetts as one of the cities considering a ban on FRT).

California Governor Gavin Newsom signed a temporary moratorium on police department use of facial recognition with body cameras, mirroring similar restrictions in other states.[162] The concern over the civil liberties, privacy, and racial justice issues has even prompted FRT developers like Microsoft and Kairos to refuse to sell the technology to police agencies.[163]

3. State Privacy Legislation

In recent years, some states have begun enacting bills that address the management of biometric data including face recognition. The leader of this kind of legislation is undoubtedly Illinois, who in 2008 passed the Biometric Illinois Privacy Data Act ("BIPA")[164] which recognizes the unparalleled uniqueness of biometrics and the importance of protecting it from misuse.[165] BIPA defines biometric data as any information based on an individual's biometric identifier that is used for identification purposes, which would include facial recognition.[166] It outlines the proper collection, management, disclosure, and disposal of biometric data.[167] It sets out requirements for notifying individuals in writing and obtaining their consent prior to disclosure of their data to a third party.[168] Importantly, BIPA provides individuals with a private right of action, which allows any aggrieved party to sue for up to $1,000 per violation and $5,000 per intentional or reckless violation.[169] In 2019, the courts in a California case involving Facebook and an Illinois case involving Six Flags Entertainment determined that for purposes of Article III standing, any violation constitutes a cognizable and concrete injury-in-fact under BIPA.[170] The implications are astounding: anyone can bring suit as soon as there is a violation of BIPA.[171] Since these rulings, cases brought

---

[162] *Id.*
[163] *See id* (discussing Microsoft President Brad Smith's refusal to equip a California police department's squad cars and body cameras with its facial recognition software); *see also* Solon, *supra* note 20 (explaining that FRT developer Kairos has refused to provide the government with its software over concerns about biometric surveillance).
[164] 740 Ill. Comp. Stat. 14/1 et seq.
[165] Wong, *supra* note 152, at 238.
[166] 740 Ill. Comp. Stat. 14/10.
[167] Wong, *supra* note 152, at 240.
[168] *Id.* at 261.
[169] Llaneza, *supra* note 140, at 181–82.
[170] Jeffrey Rosenthal & David Oberly, *Biometric Privacy In 2020: What Companies Can Expect*, LAW360 (Feb. 4, 2020, 2:23 PM), https://www.law360.com/articles/1240262/biometric-privacy-in-2020-what-companies-can-expect- [Rosenthal & Oberly, *What Companies Can Expect*].
[171] *See* Mark A. Olthoff, Russell S. Jones Jr., & Elizabeth M. Marden, *Facebook "Tagged" in Certified Facial Scanning Class Action*, NAT'L L. REV. (Aug. 28, 2019) https://www.natlawreview.com/article/facebook-tagged-certified-facial-scanning-class-

under BIPA have multiplied, with payouts ranging from $80 to $1,300 per member in class action lawsuits.[172] Facebook was forced to settle for $650 million,[173] and other companies could potentially face large settlements unless they bring their practices into compliance with BIPA.[174] Thus, Illinois' powerful biometric privacy legislation has set the bar for other U.S. states to follow.[175]

Other states enacted biometric privacy laws early on, but none as comprehensive and consumer-friendly as Illinois. Texas passed the Capture or Use of Biometric Identifiers (CUBI) legislation shortly after BIPA went into effect.[176] Although it closely mirrors BIPA, it lacks the same teeth: it fails to define biometric information (much less mention facial recognition), and despite requiring notice and consent prior to biometric data being used for commercial purposes, it fails to define "commercial purposes."[177] While Washington state in 2017 passed H.B. 1493 restricting the commercial use of biometric identifiers, the legislation is seen as a business-friendly version of BIPA due to more relaxed regulations regarding the manner in which data is gathered or subsequently used, and the fact that notification and consent are not always mandatory.[178] Furthermore, both Washington and Texas bypassed the private right of action, leaving litigation in the hands of the state

---

action (discussing the Ninth Circuit Court of Appeals ruling holding that mere collection of a person's biometric data without his or her consent constituted real or threatened injury under BIPA).

[172] *See* Richard R. Winter, Rachel C. Agius, William F. Farley, *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts.

[173] Malathi Nayak, *Facebook Sweetens Biometric Privacy Accord to $650 Million*, BLOOMBERG (July 23, 2020, 4:55 PM), https://www.bloomberg.com/news/articles/2020-07-23/facebook-proposes-650-million-to-settle-biometric-privacy-case.

[174] *See* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (explaining that the Facebook and Rosenbach rulings have "opened the floodgates to a new wave of extremely costly litigation . . . ").

[175] *See* Allison Grande & Ben Kochman, *BIPA Bares Its Teeth in Facebook Biometric Privacy Deal*, LAW360 (Jan. 30, 2020 10:39 PM), https://www.law360.com/articles/1239383/bipa-bares-its-teeth-in-facebook-biometric-privacy-deal (citing the Facebook $550 million settlement as a key test proving the unique power of BIPA).

[176] Tex. Bus. & Com. Code Ann. §503.00.

[177] *See* Llaneza, *supra* note 140, at 10.

[178] *See* Wong, *supra* note 152, at 242–44 (detailing the reasons H.B. 1493 is viewed as business-friendly, among them the fact that "a person is not obligated to provide notice nor obtain consent for biometric identifiers that are merely captured, collected, or enrolled in furtherance of a security purpose, or in the alternative, are merely captured for a commercial purpose.").

attorney general.[179]

The only state to enact biometric privacy laws rivaling the scope and force of BIPA is California, which passed the California Consumer Privacy Act ("CCPA") that went into effect in January 2020.[180] Taking its cue from the GDPR, the CCPA gives California residents broad rights over their biometric data. It generally lays out strict guidelines requiring companies to be transparent about the personal data collected and how it is disclosed or shared; it gives consumers control over how their data is sold or shared, as well as the option to have it deleted; and it requires websites to have clear and conspicuous "opt out" options for consumers not wishing their personal data to be monetized.[181] Furthermore, the CCPA creates a private right of action like BIPA, and currently serves as a landmark law that puts pressure on the U.S. Congress to enact legislation that protects Americans' data privacy rights.[182]

In November 2020, California passed the California Privacy Rights Act (CPRA), which amends and supersedes the CCPA.[183] Set to become effective on January 1, 2023, the CPRA expands the framework of the CCPA in several important ways that will directly impact the use of FRT.[184] For example, it defines a new subcategory of "sensitive" personal information ("Sensitive PI") such as biometric and genetic information, the processing of which Californians will have greater control over.[185] The CPRA also makes businesses more accountable to consumers with regard to the use of their Sensitive PI.[186] Furthermore, the CPRA gives consumers the power to partially limit profiling, defined as the automated processing of personal information in order to "analyze or predict aspects of a person's preferences, economic situation, work performance, health, interests, behavior, location,

---

[179] *See* Llaneza, *supra* note 140, at 12.

[180] Cal Civ Code Div. 3, Pt. 4, Title 1.81.5.

[181] *See California Consumer Privacy Act: A Reference Guide for Compliance*, J.D. SUPRA 3 (Oct. 22, 2019) https://www.jdsupra.com/legalnews/california-consumer-privacy-act-a-94563/.

[182] *See* Llaneza, *supra* note 140, at 15.

[183] *See* Brandon P. Reilly and Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020) https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed (describing the passage of the CPRA).

[184] *See* Michael Bahar, Mary Jane Wilson-Bilik and Alexander F. L. Sand, *California's New Privacy Law, the CPRA, Was Approved: Now What?*, LEXOLOGY (Nov. 9, 2020) https://www.lexology.com/library/detail.aspx?g=5a7edce9-26af-487c-8877-7a815945954d [hereinafter *California's New Privacy Law*].

[185] *See* Reilly & Lashway, *supra* note 183 (explaining that under the CPRA, consumers will have a new right to restrict the use and disclosure of Sensitive PI).

[186] *See California's New Privacy Law*, *supra* note 184 (describing the requirements that businesses limit and disclose the use and retention of Sensitive PI).

reliability, or movements."[187] FRT users who fail to comply with the new regulations will have to contend with the newly created California Privacy Protection Agency (CPPA), which has investigative, enforcement, and rulemaking powers.[188] These as well as other new, robust measures make the CPRA the likely precursor to future federal privacy legislation in the U.S.[189]

IV. FUTURE TRENDS

A. How FRT Will Be Used

FRT supporters continue to find new uses for facial recognition, pushing the envelope and delving into areas unknown. Facebook, for example, has applied for patents that would allow its FRT to detect customers in physical stores and match them to their social networking profiles.[190] And the technology is being used in Denmark soccer stadiums to fight hooliganism: thousands of soccer match attendees have their faces scanned and compared against a list of banned troublemakers who are denied entrance.[191] In order to not run afoul of the GDPR, authorities run the system only on game days and not on the Internet, and the data, which is cross-checked to avoid false positives, is deleted at the end of the day.[192] A soccer fan's opinion of the new security measure echoes the opinion held by many: "Facial recognition is inevitable."[193]

In America, this idea of the inevitability of FRT can be traced to the 9/11 terror attacks. Although FRT had been used for commercial as well as security purposes, the attacks pushed facial recognition to the forefront of the biometrics industry as the government sought new counterterrorism strategies.[194] Americans seemed to accept this "new" technology that invaded their privacy somewhat in exchange for increased national

---

[187] *See id.* (discussing the new definition of and restrictions on "profiling").
[188] *See* Gretchen A. Ramos, *CPRA Favored by California Voters – Practical Takeaways*, NAT'L L. REV. (Nov. 4, 2020) https://www.natlawreview.com/article/cpra-favored-california-voters-practical-takeaways?utm_content=8d9aba66946c2bd8f122f21c6d39f01a&utm_campaign=2020-11-5Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email.
[189] *See id.*
[190] Singer, *supra* note 42.
[191] Sidsel Overgaard, *A Soccer Team in Denmark Is Using Facial Recognition to Stop Unruly Fans*, N.P.R. (Oct. 21, 2019 5:39 PM) https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans.
[192] *Id.*
[193] *Id.*
[194] *See* JEFFERSON, *supra* note 65, at 72 (describing the emphasis on developing FRT after 9/11).

security.[195] Almost twenty years later, even though facial recognition is being used across many industries and for a variety of purposes, the increasing demand by government and private organizations for its use in surveillance systems is said to be driving the market.[196] Despite the concerns, FRT providers and consumers alike extol the virtues of the technology in programs that help keep our borders and citizens safe.[197]

The TSA's 2018 Biometrics Roadmap is one example, a pilot project carried out in collaboration with CBP to check international travelers' biometrics.[198] Officials contend that the technology has given them the ability to identify more than 14,000 aliens who have overstayed their visas, as well as to identify more than 130 individuals attempting to enter the country with false documents.[199] Even though rights activists denounce such unfettered access to all of a person's data, including images and contact information,[200] organizations will continue, in the name of public safety, to employ FRT in increasingly innovative ways.

There is a logical belief that widespread use of facial coverings during a pandemic like COVID-19 would thwart FRT algorithms and lead to a decline in its use.[201] However, FRT developers have found ways to adapt their technology and are working overtime to improve the accuracy of partially covered faces.[202] In addition, the ability to identify masked personnel from a distance has become crucial to places needing to enable contactless security

---

[195] *See* ANGLIM, *supra* note 7, at 191 (noting that consumers willingly exchange some privacy for the security surveillance technology provides).

[196] *See* Nakar & Greenbaum, *supra* note 3, at 96 ("FRT is already implemented in many areas such as security, commerce, social media, personal use, and even for religious purposes."); *see also Facial Recognition Market to Hit $12 Billion, supra* note 47 ("Growing demand for surveillance systems drives the demand for the global facial recognition market.").

[197] *See supra* Section II.A.ii.

[198] See *Transparency Hearings*, *supra* note 10, at 3 (statement of Austin Gould) (describing the various goals of the Biometrics Roadmap).

[199] TSA BIOMETRIC REPORT, *supra* note 67, at 32.

[200] *See* K. Wehle, *supra* note 29, at 466 (speaking broadly to the need for constitutional regulation and oversight of FRT).

[201] *See* Hvistendahl and Biddle, *supra* note 25 (noting that the use of facial coverings has presented "an obvious roadblock" to the global expansion of FRT).

[202] *See generally* Rebecca Heilweil, *Masks Can Fool Facial Recognition Systems, but the Algorithms Are Learning Fast*, VOX (July 28, 2020 10:20 AM), https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist (Describing the race between companies to update their FRT algorithms to account for masks); *see also* Susan Miller, *Facial Recognition Adapts to a Mask-Wearing Public*, GCN (June 3, 2020), https://gcn.com/articles/2020/06/03/facial-recognition-masks.aspx (describing how FRT providers across the world have been working for months to adapt their technology to recognize mask-wearers, including by adapting the technology to focus on the person's eyes).

and control, driving new demand for the technology.[203] For example, Chinese hospitals are already using FRT that identifies masked nurses –and can eventually check their temperatures– from several feet away at hospital entrances.[204] In Europe and the U.S., some employers have quietly started using advanced FRT to ensure their staff's compliance with mask requirements.[205] Given the magnitude of the COVID-19 pandemic and the expectation that more pandemics will occur,[206] it is not a stretch to imagine other types of employers using FRT to ensure that their essential personnel remain masked at all times.[207]

B. Rejection of FRT

Some FRT opponents reject the use of the technology in any application or measure, citing the abuse or potential for abuse due to indiscriminate use by businesses and government authorities.[208] While some major cities have banned its use outright and others consider partial or total bans,[209] some organizations have not waited for their local government to take action; instead, they have implemented their own ban on the use of FRT within their sphere. Several college campuses, for example, disavowed the use of the technology after being pressured by student advocates.[210] Concert promoter

---

[203] *See* Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther, Plas Emil Agerskov Thuesen & Carolyn Bigg, *Facial Recognition Technology: Supporting a Sustainable Lockdown Exit Strategy?*, DLA PIPER (May 8, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/ (discussing an Irish food producer that implemented advanced FRT in order to make employee clock ins and security access contactless and germless).

[204] *See id.* (discussing the FRT being used in Chinese hospitals at the center of the COVID-19 outbreak).

[205] *See* Yan, *supra* note 25 (noting that restaurants, hotels, and at least one airport have begun using FRT to detect mask-wearing staff).

[206] *See* 9 Nita Madhav Et Al., Disease Control Priorities: Improving Health and Reducing Poverty 315 (Dean T. Jamison, et al. eds., 3rd ed. 2017), https://www.ncbi.nlm.nih.gov/books/NBK525289/pdf/Bookshelf_NBK525289.pdf (explaining that the likelihood of pandemics is growing due to an increase and intensification of contributing trends like global travel and integration, and urbanization).

[207] *See* Yan, *supra* note 25 (contending that more private organizations, such as department stores, could begin using FRT to detect mask-wearers).

[208] *See supra* Section III.B.ii.

[209] *See supra* Section III.B.ii; *see also* Douglas Hook, *Easthampton Passes Municipal Ban on Facial Recognition Tech*, BIZJOURNALS (July 2, 2020, 10:35 AM) https://www.bizjournals.com/boston/news/2020/07/02/easthampton-passes-ban-on-facial-recognition.html (noting Boston's ban on municipal use of facial recognition technology).

[210] *See* STOP FACIAL RECOGNITION ON CAMPUS, https://www.banfacialrecognition.com/campus/ (last visited Apr. 21, 2020) [hereinafter STOP FRT] (citing several schools such as Harvard University, Stanford University,

Live Nation has no plans to begin using it.[211] At least three major FRT developers have announced they will not allow their technology to be used by law enforcement,[212] and one big one –Amazon– faced pushback last year from its own shareholders when it began to market its facial recognition software to police departments.[213]

FRT providers have taken notice and have begun to call for national standards that would essentially restrict the use of FRT rather than outright ban it.[214] Microsoft, IBM, and Google have each called for such measures, saying the government must address the current debates so that individuals' rights are protected as the technology grows.[215] Analysts, however, believe this sudden interest in regulations is the industry's attempt to dissuade lawmakers from weighing an outright ban on the technology.[216] Tech firms would clearly prefer restrictions on FRT use to the types of prohibitions that some of the nation's major cities are considering.[217] Thus, industry clamor for regulations will likely continue, and based on the federal government's failure to enact legislation thus far, it is likely that states will continue to pass their own biometric data laws.

C. The Future of FRT Regulations in the U.S.

There is a clear trend toward state regulation of FRT where states are enacting new biometric privacy laws or expanding existing ones.[218] New York accomplished both in 2019 by passing its Stop Hacks and Improve Electronic Data Security ("SHIELD") Act; it expanded the definition of

---

Massachusetts Institute of Technology (MIT), and the University of California at Los Angeles (UCLA) that refuse to use facial recognition on their campuses).

[211] *See Biometrics Tech Firms Want Moderation, Not Bans, On Facial Recognition*, PYMNTS (Mar. 8, 2020), https://www.pymnts.com/news/biometrics/2020/tech-firms-want-moderation-not-bans-facial-recognition/.

[212] *See* sources cited *supra* note 164; *see also* Chappell, *supra* note 91 (noting that the largest manufacturer of police body cameras, Axon, declines to sell facial recognition technology).

[213] See *Impact Hearing*, *supra* note 21, at 10–11 (statement of Neema Singh Guliani).

[214] Ryan Tracy, *Tech Firms Seek to Head Off Bans on Facial Recognition*, WALL ST. J. (Mar. 8, 2020 4:32 PM), https://www.wsj.com/articles/tech-firms-seek-to-head-off-bans-on-facial-recognition-11583498034.

[215] *Biometric Tech Firms Want Moderation, Not Bans, On Facial Recognition*, *supra* note 212.

[216] *See* Kaveh Waddell, *IBM calls for regulation to avoid facial recognition bans*, AXIOS (Nov. 6, 2019), https://www.axios.com/ibm-facial-recognition-regulation-ban-50000b77-109d-4472-b4c5-316b858e7d74.html.

[217] *See* Tracy, *supra* note 215 (noting Microsoft's support of state and federal regulations but not bans).

[218] *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, NAT'L. L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [hereinafter *Anatomy of Biometric Laws*].

personal information covered by current law to include biometric data, and it imposed new requirements for data security.[219] In 2019, some states passed targeted privacy legislation: Nevada's gave consumers the ability to opt out of the sale of their data, Maine's required the consumer's consent to use, share, or sell his or her personal data,[220] and Arkansas, California, and Washington each added biometric data to regulations requiring breach notifications.[221] Furthermore, several other states have introduced bills proposing either new legislation of biometric data or strengthening existing consumer protection laws that cover biometrics.[222] Thus, there will be a continued push for state biometric privacy laws to restrict the use of facial recognition.

The federal government has held several hearings in recent years on FRT, its use, its impact, and the need for national guidelines, an idea that enjoys bipartisan support.[223] A staunch conservative, House Representative Jim Jordan even said, "It doesn't matter if it's a President Trump rally or a Bernie Sanders rally, the idea of American citizens being tracked and cataloged for merely showing their faces in public is deeply troubling."[224] Last year, Congress introduced the Commercial Facial Recognition Privacy Act of 2019 ("CFRPA"),[225] which would require certain companies to obtain consent before using FRT to identify or track individuals, or sell their face data.[226] Later in the year, legislators weighed a prohibition on the sale of biometric data as part of the law.[227] Despite all the talk about the inaccuracy of FRT, especially with regard to people of color, and its unchecked and often secret use by government agencies and the private sector, the CFRPA has not made it to a vote.[228]

Another bipartisan bill, the Facial Recognition Technology Warrant Act of 2019,[229] was introduced in November 2019 and seeks to address the privacy and discrimination concerns of the federal government's use of

---

[219] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[220] Grande, *The Biggest Privacy*, *supra* note 157.
[221] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[222] Amanda Lawrence, Sasha Leonhardt & David Rivera, *State Privacy Law Initiatives to Prepare For In 2020*, LAW360 (Feb. 6, 2020 2:54 PM), https://www.law360.com/articles/1241213/state-privacy-law-initiatives-to-prepare-for-in-2020.
[223] *See* Johnson, *supra* note 11 (noting that the Congressional House Oversight and Reform Committee has held three hearings on FRT in the past year alone, and Democrats and Republicans agree on the need for federal oversight on FRT use).
[224] *Id.*.
[225] Commercial Facial Recognition Privacy Act of 2019, S.B. 847, 116th Cong. (2019).
[226] *Id.*
[227] Rosenthal & Oberly, *Legal Landscape*, *supra* note 28.
[228] *See* L. Brown, *supra* note 58.
[229] Facial Recognition Technology Warrant Act of 2019, S.B. 2878, 116th Cong. (2019).

FRT.[230] Under the Act, federal law enforcement authorities would need a probable cause warrant to use FRT to track an individual for longer than seventy-two hours, with a maximum of thirty days. In addition, it would require federal reporting on FRT use to the NIST to gauge and improve accuracy.[231] These provisions are seen as a middle ground of sorts that places limits on facial recognition while still allowing its use in certain cases involving security concerns.[232] The bill is currently pending the Senate Judiciary Committee.

V. ASSESSMENT OF PAST LEGAL RESPONSES; ALTERNATIVES; AND SOLUTIONS

A. Evaluation: What Works, What Doesn't

Proponents and opponents of FRT are increasingly beginning to agree that the lack of federal standards regarding FRT poses the greatest problem for the industry and the public alike. Despite multiple Congressional hearings on the matter and Congress's stated interest in defining biometric privacy laws for the nation, there seems to be disagreement as to whether federal law should always preempt state law in this area, how to enforce these laws, and whether consumers should have a private right of action to pursue litigation for violations.[233] A 2016 attempt to create the "best practices for the commercial use of FRT" failed when rights advocacy groups objected to the lack of an opt-in system for consumers.[234] And while states have been enacting and enforcing their own biometric privacy laws, the regulations differ on key issues, which means the protections consumers are afforded vary from state to state.[235] In addition, FRT supporters argue that the lack of uniformity in state biometrics regulations hinders innovation; businesses risk

---

[230] Chris Coons & Mike Lee, *Facial Recognition Technology Warrant Act Of 2019*, COONS (2019), https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf.

[231] *Id.*

[232] Caitlin Chin, *Highlights: Setting Guidelines for Facial Recognition and Law Enforcement*, BROOKINGS (Dec. 9, 2019), https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/.

[233] *See Impact Hearing*, *supra* note 20, at 28 (comments by Andrew G. Ferguson) (suggesting that the federal government should "set the floor" while state and local governments can create heightened standards); *see also* Rosenthal & Oberly, *Legal Landscape*, *supra* note 27 (discussing Congress' inability to pass FRT regulation despite several hearings and the introduction of bills focusing on different protections).

[234] *See* Nakar & Greenbaum, *supra* note 2, at 119–21 (describing the U.S. Department of Commerce's push in 2016 to release a set of guidelines for FRT use).

[235] *Supra* Section III.B.iii.

costly fines in the testing of new products and services across a market because they may be compliant in one state but not in another.[236] Thus, a national standard is needed.

Of the state legislative frameworks on which to base a national standard, California's CCPA and Illinois' BIPA seem to be the most comprehensive and forward-looking. The CCPA is practically a carbon copy of the GDPR, which is based on the premise that an individual is entitled to control over and protection of his personal data.[237] Due to the CCPA's precise definitions and guidelines, corporations for the most part have been forced to carefully craft their use of FRT and weigh its benefits against the risk of costly litigation and penalties (unlike the GDPR, there are no caps to CCPA fines and they are assessed per violation).[238] Additionally, the fact that the CCPA mirrors the EU's GDPR and is one of the more stringent of the biometric laws in the U.S., compliance with the CCPA often equals compliance with other privacy frameworks including the GDPR. Meanwhile, both the CCPA and BIPA grant consumers the right to bring a claim for violations, opening the door to class action lawsuits which are a powerful deterrent for the mishandling of FRT.

B. Alternatives: Keep the "Wild West" or Ban FRT?

Some proponents of FRT contend that the current federal regulatory environment (no regulations) is inherently the best situation for everyone. It allows the technology to continue to develop, resulting in the developers continuing to find breakthrough ways to employ it, and thereby the market continues to thrive to the tune of billions of dollars.[239] These supporters downplay the First Amendment and privacy rights concerns, suggesting that there is a powerful counter argument about what our expectation of privacy is nowadays, and that we continue to redraw the proverbial line in the sand as we find further positive uses for the technology outweighing the perceived negative consequences.[240] However, according to rights advocates, FRT,

---

[236] Wong, *supra* note 152, at 260.

[237] *See* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in The UK*, WIRED (Mar. 24 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (noting the similarity between the GDPR and the CCPA).

[238] Michael Fertik, *CCPA is a Win For Consumers, But Businesses Must Now Step Up On CX*, FORBES (Jan. 27, 2020 5:40 PM), https://www.forbes.com/sites/michaelfertik/2020/01/27/ccpa-is-a-win-for-consumers-but-businesses-must-now-step-up-on-cx/#68a34d3f6557.

[239] *See Facial Recognition Market to Hit $12 Billion, supra* note 46 (noting the expected growth in the facial recognition market); *see also* Coons & Lee, *supra* note 230 (explaining that an outright ban on FRT could discourage innovation).

[240] *See* K. Brown, *supra* note 28, at 416 (stating that people seem to willingly tolerate privacy

with no oversight in place and wielding the power to assemble sensitive or personal data about private persons,[241] in addition to violating constitutional rights, can be used to harass or even stalk individuals.[242] And as more businesses begin to employ FRT, this will lead to more private and public databases of information than can be shared, monetized, or even hacked and used by bad actors.[243] Therefore, maintaining the status quo is not in the best interest of the consumer or the public at large.

On the opposite end of the spectrum, the argument for a facial recognition moratorium is very much alive. Some feel its use should be halted while the government decides how best to move forward with regulation.[244] Others believe FRT should be suspended until the proper safeguards are actually implemented.[245] Still, others insist there is never a place for FRT in certain locations like college campuses, and urge its complete prohibition as the only way to truly stop the unconstitutional spying on Americans.[246] These advocates claim that judicial rejection of an expectation of privacy while in public, together with deficiencies in current regulations, allow FRT users to deploy the technology despite constitutional barriers.[247] For instance, under the third party doctrine, there is no Fourth Amendment ban on government use of personal data obtained through nongovernmental entities.[248] Thus, using a private business to collect the information allows law enforcement to sidestep the constitutional requirement to obtain a warrant prior to surveillance.[249]

However, many other individuals believe that there are legitimate commercial and law enforcement uses of facial recognition, and a ban could make citizens less safe, as well as discourage important innovation.[250] A

---

intrusions if they safeguard their well-being).

[241] Nakar & Greenbaum, *supra* note 2, at 115.

[242] Solon, *supra* note 20.

[243] *See* Wolfson, *supra* note 81, at 192 ("Data protection has become increasingly important because the development of technology has led to prevalent data collecting and processing in the public and private sectors.").

[244] *See Impact Hearing*, *supra* note 20, at 17 (comments by Andrew G. Ferguson); see also *Impact Hearing*, *supra* note 20, at 14 (statement by Neema Singh Guliani).

[245] ANGLIM, *supra* note 6, at 190.

[246] STOP FRT, *supra* note 210.

[247] *See* K. Brown, *supra* note 28, at 466 (describing how judicial rejection of a reasonable expectation of privacy plus the third party doctrine allows the government to surveil citizens despite constitutional barriers).

[248] *Id.* at 443, 466.

[249] *See id.* at 466 ("The third party doctrine and the longstanding judicial rejection of a reasonable expectation of privacy in matters made public have depleted the Fourth Amendment of vitality for purposes of establishing constitutional barriers to the government's use of FRT to profile and monitor individual citizens.").

[250] Chris Coons & Mike Lee, *supra* note 230.

2006 White House report noted:

> Government and industry have a common challenge in today's global society to provide more robust identity management tools, and identity governance principles on how to deploy these tools intelligently to meet national and international needs. Collaboration among the biometrics community–government, industry and academia–on these common challenges is essential.[251]

This view supports the idea that FRT providers and the government will each benefit if they endeavor to make facial recognition both more reliable and protective of individual rights.[252] One example of how this could work would be a provision requiring all FRT to be assessed for accuracy by a third party who would set the parameters and publicly release the results.[253] The federal government could also require their agencies use a facial recognition program that meets a minimum accuracy rate. Because of this requirement plus the public being informed of each provider's technology's accuracy and potential for unfair bias, market forces would drive sales of the higher quality software, forcing developers producing substandard technology to improve their product or be pushed out of the market. [254] Thus, an FRT provider outperforming the competition will be rewarded with increased sales figures, while the FRT users –and their subjects– are rewarded with reliable results and a reduced risk of racial bias.[255]

Another option for the future of FRT is to require that providers have consumers opt in or out of their services, which would force private organizations to disclose the kind of information they are collecting from consumers and how they plan to use it.[256] Google, for example, requires

---

[251] The National Biometrics Challenge, National Science and Technology Council Subcommittee on Biometrics, page 1, (Aug., 2006), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometrics_challenge_document.pdf.

[252] *See* HAMPSON & JARDINE, *supra* note 151, at 278 (stating that "new kinds of collaborative institutional arrangements" will help manage the evolution of data privacy laws); *see also* Smith, *supra* note 35 (proposing the government pass legislation that incentivizes the development of more accurate FRT).

[253] *See* Smith, *supra* note 35 (contending FRT should be tested for accuracy, in a transparent and even-handed manner, by impartial groups.).

[254] *Id.*

[255] *Id.*

[256] *See* HAMPSON & JARDINE, *supra* note 151, at 17 ("Private corporations must come out of the shadows, come clean about the information they are gathering from us when we use their products and services."); *see also* ANGLIM, *supra* note 6, at 192 ("Suggested best practices

consumers to turn on a "find my face" feature in their smartphones in order to enable facial recognition.[257] Other companies such as Microsoft and MasterCard require the user download software or purchase hardware.[258] Where facial recognition is used in a physical location such as a retail store or a bank, signs should be posted alerting the consumer as to what services will use their facial image should they choose to enter the premises.[259] When a consumer needing a service is forced to choose between surrendering his privacy or seeking that service from a competitor, his ultimate decision will shed light on his opinion of the technology and the importance of his consent. Regardless, consent is fundamental to respecting the rights of individuals over their biometric data, and it should be required in every commercial use of FRT.[260]

C. Solution: There is No One Solution

Ideally, FRT would be regulated under one set of national guidelines that supersedes individual state laws. However, any regulation, whether it be state or federal, should do more than just penalize certain uses of the technology; it should incentivize all stakeholders to view biometric data, the most reliable source of identification, as a precious commodity, inextricably intertwined with an individual's dignity.[261] As such, a faceprint should not be subjected to an unwarranted search and match, or storage in a database without the individual's consent, much less nonconsensual sale to a third party. Any thought to the contrary would mean people would be forced to hide their faces in public spaces in order to prevent government and commercial tracking, as well as the trafficking of their personal data. Striking the right balance so that government and business interests do not infringe on political freedoms and civil liberties is perhaps the greatest challenge the U.S. and other democratic societies face today.[262] Many fundamental human values reside at this crossroads: power, wealth, ethics, respect, knowledge, and the maximization of skills are all in play.[263]

[for commercial FRT use] vary, but most call for disclosing the technology's use and obtaining consent before using it to identify someone from anonymous images.").

[257] ANGLIM, *supra* note 6, at 193.

[258] *Id*.

[259] Smith, *supra* note 35.

[260] *See supra* Section II.B.i.

[261] *See* Neo Sesinye, *Know the value of your digital and biometric data*, IT NEWS AFRICA (Mar. 4, 2019), https://www.itnewsafrica.com/2019/03/know-the-value-of-your-digital-and-biometric-data/ (emphasizing the value of biometric data, and that it is "paramount and therefore deserves the utmost respect and protection").

[262] GUIORA, *supra* note 26, at 77.

[263] Siegfried Wiessner, *The New Haven School of Jurisprudence: A Universal Toolkit for*

1. How Much Is It Worth?

The first step in restoring order to this "wild west" is to properly monetize biometric data, and specifically facial recognition data. This kind of data holds massive value for entities needing to quickly verify individuals attempting to use their service; its authenticity is relied upon to seek out persons of interest, to verify the recipient of a bank wire transfer, or to authorize access to a secure device or space, among the many uses.[264] In addition, commercial enterprises whose business is based upon Internet commerce depend on the value of intangible assets, such as large consumer databases, to adequately exploit their organization's market value, to secure financing, and even turn a relatively easy net profit on a sale to a third party.[265] A clear example of personal data being monetized by the holder (as opposed to the individual) is the post-bankruptcy sale of retailer Sports Authority's customer database for $15 million.[266] If companies use people's biometric data for financial gain, then the data owners must be compensated.[267]

An individual's faceprint should have a real value, even a dollar value, and this should belong to the individual if she chooses to allow the use of her image.[268] Without faceprints, FRT companies are unable to test and continually improve their technology.[269] In addition, companies such as retailers are using these images to make money, images acquired without the persons' knowledge and at basically no cost other than the initial purchase of the facial recognition software.[270] Around 2.5 billion photos are uploaded to Facebook alone every month. So long as FRT users are allowed to sell those images without consumer knowledge, consent, or compensation, the low cost

---

Understanding and Shaping the Law, 81 ASIA PACIFIC L. REV. 45, 51–52 (2010).

[264] *See supra* Section I.A.

[265] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 428 (2018) [hereinafter Elvy, *Commodifying Consumer Data*].

[266] *Id.* at 431.

[267] *See* Solon, *supra* note 20 (arguing that strict rules on FRT are especially applicable when private organizations collect and utilize a great number of facial images).

[268] *See generally* Magali Eben, *Market Definition and Free Online Services: The Prospect of Personal Data as Price*, 14 I/S: J. L. & POL'Y FOR INFO. SOC'Y 227 (2018) (proposing that personal data can be monetized and traded for services).

[269] Lafrance, *supra* note 32.

[270] *See Privacy and Civil Liberties Hearing, supra* note 5, at 9 (statement of Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission, stating that the rapid growth in the availability of online photos means companies do not need to purchase identified images, which lowers costs and makes facial recognition technologies commercially viable for many organizations).

and potential profit will remain too seductive a practice to discontinue.[271] Thus, any law addressing the commercial use of facial recognition should have a provision requiring the data initially be acquired from the individual by purchase and with consent.

Attempts have been made to translate this idea to dollars and cents.[272] In 2014, New York-based company Datacoup began compensating persons for their personal data, in hopes of creating a marketplace for businesses to purchase personal data obtained directly from the consumer.[273] Datacoup may have been ahead of its time; "big data" competitors, able to scour the Internet and scrape massive amounts of personal information (without consumer consent), offered bigger pools of data to Datacoup's clients, and at a lower cost, eventually helping to bring about the company's demise in 2019.[274] Had there been federal laws prohibiting the scraping of people's social media pages and online activity for the nonconsensual monetization of their private data, Datacoup might today be the pioneer of a verdant and equitable marketplace of personal data, including biometrics.

There have been other attempts to monetize personal data.[275] In a privacy-discount program, a company grants consumers a discount on services they are purchasing in exchange for the ability to use their personal data.[276] For example, Internet Service Provider AT&T once offered a $30 discount on its broadband service to customers who consented to the sharing of their browsing data for things like targeted ads.[277] The concept is on point: the consumer is offered monetary value for his personal data, and he is free to decide if he accepts the exchange. It would be up to regulations requiring transparency among other things, to ensure companies do not artificially

---

[271] *Id.* at 9 (statement of Maneesha Mithal) (explaining that FRT is a viable commercial option for many companies because there is no need to purchase the images, which keeps costs low).

[272] *See* Eben, *supra* note 268, at 267–68 (noting companies Datacoup and People.io who offered monetary compensation, discounts, and free goods for their customers' personal data).

[273] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1398 (2017) [hereinafter Elvy, *Paying for Privacy*].

[274] *Datacoup*, WIKIPEDIA, https://en.wikipedia.org/wiki/Datacoup (last visited April 21, 2020).

[275] *See* Eben, *supra* note 268, at 267–68 (discussing the company People.io and how it purchases personal data with credits); *see also* Kate Cox, *Broadband Industry: It's Unfair If Facebook Can Collect Your Data, But AT&T Can't*, CONSUMER REPORTS (Mar. 29, 2016) https://www.consumerreports.org/consumerist/broadband-industry-its-unfair-if-facebook-can-collect-your-data-but-att-cant/ (citing an AT&T discount offer made to its GigaPower fiber optic customers in 2016).

[276] Elvy, *Paying for Privacy, supra* note 273, at 1391.

[277] *See* Cox, *supra* note 275 (discussing AT&T's discount for personal data offer to its customers).

inflate the costs of their services in order to pay for the discounts being offered. AT&T was accused of exactly this, a "pay for privacy" program where customers unwilling to surrender their privacy were forced to pay more than those who consented.[278] With transparency requirements in place, the same innovative minds that found ways for their business to profit off assets they acquired for free should have no trouble finding ways to reward customers who give consent, without punishing those who do not.

2. Speaking of Transparency . . .

The public sector should not be left out of transparency requirements. People should, at the very least, be made aware when the government is accessing their biometric data and for what purpose. Without this knowledge, we are unable to hold our governments and elected officials accountable with regard to privacy and surveillance, and relying on the goodwill of the FRT users is unacceptable in a society of checks and balances.[279] Situations that require secrecy can be dealt with in much the same way court records and proceedings are sealed depending on the circumstances.[280] Furthermore, keeping the public in the dark about how their biometric data is being used denies the opportunity for a frank and realistic discussion on how the evolution of technology impacts our society and what types of controls we want as a nation and as a global citizen.

In 2013, National Security Agency ("NSA") contractor Edward Snowden revealed to the world that the NSA's PRISM program was monitoring the phone records and Internet activity of millions of Americans and non-Americans with the help of Internet moguls like Google, Apple, and Facebook.[281] The revelations opened a debate on the ethical implications of secret surveillance in the name of national security, and what protections we as a country believed people were entitled to.[282] Each time we learn that our biometric data is being gathered, analyzed, disclosed, and shared without our

---

[278] *Id.*

[279] HAMPSON & JARDINE, *supra* note 151, at 16–17.

[280] *See* Robert Timothy Reagan, *Sealing Court Records and Proceedings: A Pocket Guide*, FEDERAL JUDICIAL CENTER 1–2 (2010), https://www.fjc.gov/content/sealing-court-records-and-proceedings-pocket-guide-0 (explaining generally how and why some court records and proceedings are sealed from the public).

[281] Michael L. Rustad & Thomas H. Koenig, *Towards A Global Data Privacy Standard*, 71 FLA. L. REV. 365, 401 (2019); *Edward Snowden was NSA Prism leak source – Guardian*, BBC NEWS (June 10, 2013), https://www.bbc.com/news/world-us-canada-22836378.

[282] *See The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/. (discussing the ethics and security debates that occurred in the wake of Snowden's leak of the PRISM program).

knowledge, similar discussions ensue, and public trust in the government and private sector is eroded.[283] It is time this information be publicly reported, and several advantages will flow from such a requirement.

First, this knowledge would protect an individual's Fourth Amendment privacy rights more generally than a provision requiring something as specific as a warrant prior to surveillance. For example, if law enforcement is required to report that it is using FRT to track or identify an individual, agents will be more likely to seek out warrants beforehand, as well as provide this information to a defendant, as a means to prevent both key evidence from later being suppressed in court and convictions from being reversed.[284] Detailed reporting would also shed light on whether the technology was used in approved ways, potentially eliminating highly questionable practices such as using forensic sketches or celebrity photos to identify suspects, which would be cause for a mistrial if something similar were done with fingerprints.[285] Moreover, requiring organizations to divulge when and how they are using FRT—potentially encroaching on First Amendment freedoms as well—will allow government agencies and legislators to model their own reporting framework, one that can withstand public scrutiny and rebuild the public's trust in the government and the commercial industry.[286] These are important wins for rights advocates as well as for the government.

Yet another way to protect individuals with reporting is by monitoring accuracy rates and ensuring they comply with federal requirements. With FRT, better accuracy means less racially biased results.[287] In addition to this oversight, the government could use federal purse strings to incentivize due diligence and compliance with reporting requirements. Congress has the power to regulate most state and local law enforcement FRT systems because

---

[283] *See* HAMPSON & JARDINE, *supra* note 151, at 255 (citing a 2016 CIGI-Ipsos survey where 78 percent of people surveyed were concerned about their information being monitored as a result of the increasing number of Internet enabled devices, and 79 percent expressed concern over the sale and purchase of their private data); *see also* YUE LIU, *supra* note 23 and accompanying text.

[284] *See generally* 1 PRETRIAL MOTIONS IN CRIMINAL PROSECUTIONS § 5-1 (2020) (explaining that suppression of Brady evidence could lead to a reversal of a conviction).

[285] *See Impact Hearing*, *supra* note 20, at 30 (testimony of Clare Garvie); *see also* Harwell, *Police Have Used Celebrity Look-Alikes*, *supra* note 106 (noting questionable uses of FRT such as using altered photos, composite sketches, and celebrity photos to match criminal suspects).

[286] *See* YUE LIU, *supra* note 23 and accompanying text.

[287] *See* Queenie Wong, *Why Facial Recognition's Racial Bias Problem is So Hard to Crack*, CNET (Mar. 27, 2019 5:00 A.M.), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/ (noting that Amazon improved its FRT accuracy, which "reduced the error rates for identifying women and darker-skinned men by up to 20 times.").

they are purchased with federal funds.[288] Not only could they require certain standards and limits when FRT is used, they could incentivize FRT providers to improve their technology by rewarding better quality with preference in the contract bidding process. With this kind of transparency in place, facial recognition could still be used by government agencies in meaningful ways that are significantly less likely to infringe on individual rights than the current free-for-all in the FRT landscape.

3. It's All About the Money

At the end of the day, all organizations must be profitable. Both private and public sector organizations place high value on financial stability, and threats to profitability are to be avoided at all costs.[289] When it comes to privacy laws, giving people the ability to sue an entity that violates their rights basically empowers them with a weapon all organizations fear: messy, complex, and expensive litigation that is often coupled with negative publicity.[290] Currently, only BIPA and the CCPA grant private individuals this power, and a string of recent high-stakes data breach scandals may prove the private right of action, which could result in actual and statutory damages, is in fact the powerful deterrent it is designed to be.[291]

Under the CCPA, which took effect on January 1, 2020, plaintiffs may seek actual damages or statutory penalties of $100 to $750 per violation.[292] Lawsuits against two major players, home security system company Ring and video conferencing company Zoom, have already been filed by consumers.[293] Meanwhile, under BIPA, statutory penalties alone range from $1,000 to $5,000 *per violation*.[294] In 2019, just one week after Facebook agreed to a

---

[288] *See Impact Hearing*, *supra* note 20, at 14 (testimony of Clare Garvie).

[289] *See Anatomy of Biometric Laws, supra* note 218 (recommending companies take a proactive approach towards compliance with emerging biometric privacy laws because under BIPA, plaintiffs could seek costly statutory damages, injunctive relief, actual damages, and recovery of attorney fees and litigation costs).

[290] *See* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (contending that BIPA statutory damages are a considerable incentive for plaintiffs and attorneys to pursue class action lawsuits for alleged violations).

[291] *See supra* Section III.B.iii.

[292] *See* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKERLAW 1, 6 (Nov. 21, 2018), https://www.bakerlaw.com/articles/alan-friel-laura-jehl-create-chart-comparing-ccpa-and-gdpr.

[293] *See* Molly F. Martinson, *Zoom and Gloom: Early CCPA Lawsuits Against Zoom Seek to Expand Private Right of Action*, WYRICK PRACTICAL PRIVACY BLOG (Apr. 7, 2020), https://practicalprivacy.wyrick.com/blog/zoom-and-gloom-early-ccpa-lawsuits-against-zoom-seek-to-expand-private-right-of-action (citing the Ring suit filed in February 2020 and two Zoom suits filed in March 2020).

[294] *See* Grande & Kochman, *supra* note 175.

$550 million settlement,[295] a class action suit was filed against Google in Illinois, alleging the tech giant was gathering facial images, converting them to faceprints, and creating face templates without the consumer's consent, in violation of BIPA.[296] The lawsuit adds to a growing list of BIPA suits against major companies, such as The Home Depot and Walmart, and more class actions are likely to be filed unless companies take measures to bring themselves into compliance.[297]

Elsewhere, biometric privacy law protections vary from state to state. Were the federal government to enact a biometric data law allowing for a private right of action, albeit limited, FRT providers and users would have one set of national standards to meet and thus a clear view on how to avoid being sued by private consumers so they can focus on innovation.[298] With the prevalence of FRT being used across state lines and no national guidelines for companies to follow, many predict a surge in litigation that will tie up the courts and cost companies billions in settlements, with no end to this trend in sight.[299] Thus, the incorporation of a private right of action in federal legislation would serve to guide FRT providers and users towards compliance with the regulations.

VI. CONCLUSION

The facial recognition technology used today in everything from home appliances to smartphones to security cameras is thanks to the pace with which creators have been able to develop and improve the technology.[300] While this ability to innovate is laudable, it has been made possible in part thanks to a lack of uniform, federal regulations that would address important

---

[295] *See supra* note 173. (Although the original settlement amount was a record-breaking $550 million, the district judge refused to approve it, citing concerns it would fail to compensate millions of Illinois users. Facebook raised its offer to $650 million in July 2020).

[296] Wendy Davis, *Google Hit With New Lawsuit Over Faceprints*, MEDIAPOST (Feb. 7, 2020), https://www.mediapost.com/publications/article/346807/google-hit-with-new-lawsuit-over-faceprints.html.

[297] *Id.*

[298] *See* Llaneza, *supra* note 140, at 22 (asserting that a federal law granting consumers a private right of action would put companies on notice as to their existing data privacy policies); *see also supra* note 235.

[299] *See* Wong, *supra* note 152, at 252 (expecting litigation to increase under BIPA after recent rulings); *see also* Rosenthal & Oberly, *What Companies Can Expect*, *supra* note 170 (stating that recent court rulings have opened room for extremely costly litigation considering the nature and extent of the violation).

[300] *See* Trepp, *supra* note 15 (noting how FRT has improved dramatically with the assistance of AI).

public concerns, including the infringement of constitutional rights.[301] Despite limited support for the continuation of this "wild west" of biometrics, as well as for some kind of moratorium on FRT use, only a balanced approach will succeed.[302]

The federal government should look to BIPA, the CCPA/CPRA, and the GDPR as guideposts for the implementation of a much needed national standard on FRT, where providers and users, who are the ones benefiting from and profiting off of our data, are the ones to primarily shoulder the burden of FRT's consequences.[303] Congress should pass a law that requires consumers be compensated for their data, that there be detailed reporting on the use of FRT, and that individuals have a private right of action against FRT users.[304] Only when public and private sector organizations are forced to recognize the tangible and protectible value of biometric data will they reckon the impact of FRT on rights we hold to be fundamental.

---

[301] *Supra* Section V.B.
[302] *Id.*
[303] *Supra* Section II.A.ii and II.B.
[304] *Supra* Section V.C.

PUBLIC POLICY AND THE INSURABILITY OF CYBER RISK

Asaf Lubin*

In June 2017, the food and beverage conglomerate Mondelez International became a victim of the NotPetya ransomware attack. Around 1,700 of its servers and 24,000 of the company's laptops were suddenly and permanently unusable. Commercial supply and distribution disruptions, theft of credentials from many users, and unfulfilled customer orders soon followed, leading to losses that totaled more than $100 million. Unfortunately, Zurich, which had sold the company a property insurance policy that included a variety of coverages, informed Mondelez in 2018 that cyber coverage would be denied under the policy based on the "war exclusion clause." This case, now pending, will be a watershed moment for the cyber insurance industry, highlighting the great ambiguity around the insurability of certain types of cyber risk and the scope of coverage that insurers will provide in the case of a cyber incident.

The literature on the insurability of cyber risk has focused all of its attention on questions of economic efficiency and viability. Scholarship has, for example, examined the actuarial challenges in cyber risk modeling and the likelihood for adverse selection resulting from information asymmetries and lack of historical claims data. Scholars have so far avoided a different set of considerations rooted not in economics but rather in public policy analysis of societal values. This paper lays the framework for such an analysis. Relying on traditional insurance and torts jurisprudence, the paper makes the public policy case for limited legal interventions in the indemnification of three controversial categories of cyber harm: (1) acts of

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University, Maurer School of Law, Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, Affiliated Fellow at the Information Society Project at Yale Law School, Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Visiting Scholar at the Federmann Cyber Security Center at Hebrew University of Jerusalem. This work was supported by funding from the Federmann Cyber Security Center in conjunction with the Israeli National Cyber Directorate. The research was further supported by funding from the William and Flora Hewlett Foundation under grant 2018-7277.

This work benefited from the excellent comments of participants at faculty workshops at Indiana University Maurer School of Law, Loyola Los Angeles Law School, UC Hastings Law School, and University of Syracuse Law School. This paper further benefited from comments during workshops and events organized by the University of Geneva, New York University, the U.S. Secret Service Cyber Policy, Strategy and Outreach Division, the Information Society Project at Yale Law School, Third Way, The Berkman Klein Center for Internet and Society at Harvard University, the Israeli National Cyber Directorate, and the Federmann Cybersecurity Center at Hebrew University. I wish to further thank Professors Tom Baker and Daniel Schwarcz for their guidance, support, and feedback throughout this process. I further wish to thank João Marinotti, Itai Ben-Artzi, and Andreas Kuehn for comments on previous versions of the paper. Thank you to Jacob Przada, Charlie Bland and the student editors at JOLTTX for all their incredible hard work in preparing this piece for publication.

cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; and (3) administrative fines for violations of statutory data protection regulations. In so doing, the paper highlights systemic challenges to cyber insurance underwriting while explaining insurers' role in increasing societal cyber posture by reducing the likelihood of moral hazard and suboptimal cyber-norms enforcement.

TABLE OF CONTENTS

I. INTRODUCTION

Referred to as "the most devastating cyberattack since the invention of the Internet,"[1] the NotPetya malware[2] wreaked havoc around the world during the month of June 2017.[3] As a propagation method, hackers relied on a "watering hole" technique, an attack which compromises a particular website or software known to be used by the hacker's unsuspecting targets.[4] The hackers infected the servers of a financial software program called MEDoc, which businesses operating in the Ukraine commonly use to file taxes.[5] The compromised MEDoc servers then delivered the NotPetya malware to corporations within Ukraine and around the world.[6] NotPetya spread "automatically, rapidly, and indiscriminately," gaining administrator access to infected machines and leveraging that power to commandeer other computers on the network.[7] Once inside the network the malware irreversibly

---

[1] Andy Greenberg, *The Untold Story of NotPetya, The Most Devasting Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[2] Malware, a malicious software, is a computer code that is introduced in some way into a target computer, server, or network with the intention of causing harm. Trey Herr identifies three fundamental components that are part of any malware: a Propagation Method, Exploits, and Payload. A propagation method is "the means of transporting malicious code from origin to target" (e.g., a phishing email, a compromised website, a dropper software, or an infected removable storage device). Exploits "act to enable infection . . . by taking advantage of vulnerabilities in the target system" (e.g., flaws, bugs, and errors in software that allow the malware to access a device, spread between computers, escalate privileges, and execute the payload). Finally, the Payload is "code written to achieve some desired malicious end" (e.g., deletion of data, manipulation of an industrial control system, or theft of information). For further reading see Trey Herr, *PrEP: A Framework for Malware & Cyber Weapons*, 13(1) J. INFO. WARFARE 87, 88 (2014).

[3] NotPetya took its name from its resemblance to the ransomware Petya, a piece of criminal code that surfaced in 2016 and extorted victims to pay for a key to unlock their files. While many initially suggested that the 2017 infection resulted from the same malware, researchers at Kaspersky lab concluded that this was a different strand of ransomware and thus dubbed it NotPetya. *See* Danny Palmer, *A Massive Cyberattack is Hitting Organizations Around the World*, ZDNET (Jun. 27, 2017), https://www.zdnet.com/article/a-massive-cyberattack-is-hitting-organisations-around-the-world/.

[4] *See generally* Sumayah Alrwais et al., *Catching Predators at Watering Holes: Finding and Understanding Strategically Compromised Websites*, Annual Computer and Security Applications Conference (2016).

[5] Ellen Nakashima, *Ukraine's Ransomware Attack Was a Ruse to Hide Culprit's Identity, Researchers Say*, WASH. POST (Jun. 29, 2017), https://www.washingtonpost.com/world/national-security/this-weeks-global-ransomware-attack-was-a-ruse-to-deflect-attention-from-the-true-culprit-researchers-say/2017/06/29/da455a0e-5cf0-11e7-9b7d-14576dc0f39d_story.html.

[6] Greenberg, *supra* note 1.

[7] *Id*.

encrypted the master boot records of all infected devices and demanded the payment of $300 worth of bitcoin to decrypt them.[8] While masquerading as a "ransomware" attack,[9] this attack was in fact not financially motivated.[10] Western intelligence agencies have concluded that NotPetya was launched by Russia's GRU military spy agency as part of its cyber campaign against the Ukraine.[11]

Irrespective of the perpetrator, the White House estimates that NotPetya

---

[8] *Id*.

[9] The Departments of Justice, Homeland Security, and Health and Human Services define a ransomware as a "type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted." *See Ransomware: What It Is and What to Do About It*, DOJ (2016), https://www.justice.gov/criminal-ccips/file/872766/download. For more on ransomware attacks and regulatory responses to address them see *Combating Ransomware: A Comprehensive Framework for action*, INST. SEC. & TECH. (2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf [hereinafter Ransomware Task Force Report].

[10] Liam Tung, *'Russian Military Behind NotPetya Attacks': UK Officially names and Shames Kremlin*, ZDNET (Feb. 15, 2018), https://www.zdnet.com/article/russian-military-behind-notpetya-attacks-uk-officially-names-and-shames-kremlin/ (noting that initially NotPetya was "thought to be ransomware, but security researchers quickly concluded that it was more likely to be destructive malware designed to wipe systems"); *see also* Iain Thomson, *Everything you Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide*, THE REGISTER (Jun. 28, 2017), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/ (citing computer security veteran The Grugq, "Although there is significant code sharing, the real Petya was a criminal enterprise for making money. [NotPetya] is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibility deniable cover of ransomware.").

[11] *See* Press Release, U.K. National Cyber Security Centre, Reckless Campaign Of Cyber Attacks by Russian Military Intelligence Service Exposed (Oct. 3, 2018) (referring to the June 2017 attack NCSC assess "with high confidence that the GRU was almost certainly responsible"); *see* Press Release, U.K. Foreign Office, Foreign Office Minister Condemns Russia for NotPetya Attacks (Feb. 15, 2018) ("UK judges that the Russian government was responsible for the NotPetya cyber-attack of June 2017 . . . The attack masqueraded as a criminal enterprise but its purpose was principally to disrupt. Primary targets were Ukrainian financial, energy and government sectors. Its indiscriminate design caused it to spread further, affecting other European and Russian business."); *see* Press Release, U.S. Embassy in Belarus, Statement from the Press Secretary (Feb. 15, 2018) ("In June 2017, the Russian military launched the most destructive and costly cyber-attack in history . . . It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict"). Similar statements were issued by Canada, Denmark, Lithuania, Estonia, and Australia as part of a coordinated diplomatic effort. *See* Stilgherrian, *Blaming Russia for NotPetya was coordinated diplomatic action*, ZDNET (Apr. 12, 2018), https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

cost more than $10 billion in total damages.[12] A large number of multinational corporations experienced paralyzing businesses interruptions, including pharmaceutical company Merck (whose damages are estimated at $870 million), Delivery Company FedEx (whose damages to its European Subsidiary TNT Express are estimated at $400 million), and Danish Shipping company Maersk (whose damages are estimated at $300 million).[13] Those companies' financial losses were collateral damage; their injuries were a spillover from the alleged Russian state-sponsored attacks on its neighbor to the west.

The food and beverage conglomerate *Mondelez International* was another victim of the NotPetya attack.[14] Around 1,700 of its servers and 24,000 of its computers became permanently unusable at the end of June 2017.[15] Thousands of boxes of Oreos and Ritz Crackers were left waiting in packaging centers as the attack disrupted commercial supply and distribution chains and made it impossible for *Mondelez* to fulfill customer orders.[16] Ultimately, the attack led to losses that totaled more than $100 million for the company.[17]

Mondelez had an all-risk property insurance policy with *Zurich American Insurance*.[18] The policy covered "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction . . . [and] Actual loss sustained and extra expenses incurred by the insured during the period of the interruption resulting from the failure of the Insured's electronic data processing equipment or media to operate."[19] *Mondelez* thus filed an insurance claim seeking compensation for at least a portion of its NotPetya losses.[20] In June 2018 *Zurich* informed *Mondelez* that cyber coverage would be denied under the policy based on an exclusion listed therein which limited indemnification in cases of damages resulting directly or indirectly from "a hostile or warlike action . . . by any government or sovereign power."[21]

The *Mondelez v. Zurich* case, still pending before an Illinois court as of

---

[12] Greenberg, *supra* note 1 (noting that the White House assessment was confirmed to *WIRED* by former Homeland Security Adviser Tom Bossert).
[13] *Id*.
[14] Compl., Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008, 2018 WL 4941760, at *1 (Ill. Cir. Oct. 10, 2018).
[15] *Id.*
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*.

April 2022, will be a watershed moment for the cyber insurance industry.[22] While the case does not stem from a standalone cyber insurance product, it nonetheless highlights the great ambiguity around the scope of coverage that insurers will provide in the case of a cyber incident and the evidentiary requirements for tortious attribution in cyberspace.[23] The case, which has now received national attention,[24] thus offers an opportune moment for self-reflection for the insured, insurers, and regulators around the limits of insurability of both existing and future cyber exposure.

Increased economic risk from cyberattacks and data breaches has led to the rise of cyber insurance as a means for risk prevention and management.[25]

---

[22] *See* Justine Ferland, *Cyber Insurance – What Coverage In Case of An Alleged Act of War?*, 35(4) COMPUT. L. & SEC. REV. 369, 375 (2019) (noting that "not only is [the Mondelez case] the first significant legal dispute in the insurance field concerning the recovery of costs resulting from a cyber-attack, but it is also the first time that an insurance company is invoking the war exclusion to decline coverage for an allegedly state-sponsored cyber hack. Should it proceed to trial and notwithstanding who is the successful party, it is therefore certain to have important impacts on the contents and limits of future traditional and cyber-specific insurance policies."). *See also* Scott Shackelford, *Wargames: Analyzing the Act of war Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE J. L. & TECH. 362, 396–97 (2021). Note that a parallel case also stemming from the NotPetya incident, has already been decided earlier this year. *See* Merck & Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18, 2022 WL 951154, at *1 (N.J. SUPER. CT. LAW DIV. Aug. 2, 2018) In *Merck & Co. Inc. vs. Ace American Insurance Co.*, Judge Thomas J. Walsh ruled in favor of the policyholder. *Id.* at *6. In an important yet controversial win to policyholders, the decision reasoned that given its "plain meaning" and "applicable caselaw" the war exclusion did not cover non-"traditional" forms of warfare like cyberattacks. *Id.* The judge clearly construed the exclusion against the insurer and in favor of the insured, opening the door for further appeals as well as for more specifically tailored cyber insurance exclusions. *See generally* Andrea Vittorio, *Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War'*, BLOOMBERG LAW (Jan. 19, 2022), https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war.

[23] Merck Pharmaceutical filed a similar suit in the Superior Court of New Jersey against a number of its first party property insurers and reinsurers asserting claims for breach of contract and declaratory judgment for their denial of coverage under a similar "war like" exclusion. *See* Merck & Co., Inc. v. Ace American Insurance Co., No. UNN-L-002682-18 (N.J. SUPER. CT. LAW DIV. Aug. 2, 2018).

[24] *See, e.g.*, Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html; Oliver Ralph & Robert Armstrong, *Mondelez Sues Zurich in Test for Cyber Hack Insurance*, THE FINANCIAL TIMES (Jan. 9, 2019), https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e.

[25] ANDREW COBURN ET. AL., SOLVING CYBER RISK: PROTECTING YOUR COMPANY AND SOCIETY 235 (2019) (suggesting that cyber insurance "is rapidly becoming a standard component of companies' risk management strategy to protect themselves against cyber loss.").

The global cyber insurance market is expected to grow by 21% this year and reach $9.5 billion in gross written premiums at the end of this year. That number is expected to grow to over $20 billion by 2025.[26] These policies cover varied costs associated with the perils of operating a business in the digital age. Stand-alone cyber insurance policies now offer coverage for an array of both first-party cyber harms (such as a business interruption and network shutdown triggered by an attack on third-party suppliers or cloud-service providers) and third-party cyber harms (such as costs for notification and credit monitoring services and legal fees associated with data breaches of users' information).[27]

Despite the imminent ubiquity of cyber insurance in the United States, scholarship on the insurability of cyber risk is still in its infancy. Most of what has been written has focused solely on the economic viability of these cyber insurance products. Following the criteria laid down by the likes of Robert Mehr and Emerson Cammack in *Principles of Insurance,* this body of work has centered on addressing the following questions: (1) does cyber risk involve a large group of homogeneous exposure units? (2) does cyber risk produce losses that are definite as to time, place, amount, and causes? (3) does cyber risk produce losses that are accidental or fortuitous? (4) is the potential loss from cyber risk large enough to cause hardship? (5) is the cost of cyber insurance economically feasible? (6) is the chance of cyber loss calculable? and (7) can cyber perils produce loss to a great many insured units at one time?[28]

Examples of scholarship that have adopted these economic questions as guideposts for insurability determinations abound. These include, among others,[29] papers that have examined the aggregation risks associated with

---

[26] Edward Gately, *Cyber Insurance Market to Jump in 2021 as Cybercrime Surges*, CHANNEL FUTURES (Dec. 24, 2020), https://www.channelfutures.com/vertical-markets/cyber-insurance-market-to-jump-in-2021-as-cybercrime-surges.

[27] *See infra* Section II.

[28] ROBERT I MEHR & EMERSON CAMMACK, PRINCIPLES OF INSURANCE 34–37 (1976) (noting that these seven criteria are either essential or a mere substitutable requisite for a successful insurance plan. Suggesting further that only criteria (1) and (7) are truly essential. Nonetheless concluding that the "foregoing criteria of insurability are not rigidly followed. Cases are on record in which coverage is written in violation of one or more of them . . . [nonetheless,] these criteria must be viewed as the optimum to achieve"). For a complete survey of the literature around criteria for insurability of risk see Joan T. Schmit, *A New View of the Requisites of Insurability*, 53(2) J. RISK & INS. 320 (1986).

[29] Other important and more recent works include Erin Kenneally, *Ransomware: A Darwinian Opportunity for Cyber Insurance*, 28 CONN. INS. L. J. (forthcoming, 2021); Bryan Cunningham & Shauhin A. Talesh, *Uncle Sam RE: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping*, 28 CONN. INS. L. J. (forthcoming, 2021); Christopher C. French, *Five Approaches to Insuring Cyber Risks*, 81 MD. L. REV. 103 (2021); Kenneth S. Abraham & Daniel Schwarcz, *Courting*

cyber insurance,[30] the contemporary gaps in coverage of cyber harms,[31] the actuarial challenges in cyber risk modeling,[32] the difficulties in wording and pricing cyber insurance policies,[33] the private governance benefits and pitfalls of enforcing cyber security standards through commercial insurance,[34] and the information asymmetries and lack of historical claims data that are preventing the cyber insurance market from maturing.[35]

While all of these papers offer foundational, theoretical insight, and empirical data as to the economic benefits of insurance as a tool in cyber risk prevention and mitigation, they fail to provide a normative path forward. These papers tend to ignore an equally important set of concerns rooted not in economics but rather in philosophy and political science.[36] To reference

---

Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe, 28 CONN. INS. L. J. (forthcoming, 2021).

[30] *See e.g.*, Davis Hake et. al., *Cyber Insurance and Systemic Market Risk*, EASTWEST INSTITUTE (Jun. 5, 2019), https://www.eastwest.ngo/cyberinsurance; Daniel M. Hoffman, *Advancing Accumulation Risk Management in Cyber Insurance*, THE GENEVA ASS'N (2018), https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf.

[31] *See, e.g.*, Robert H. Jerry & Michele Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurer's Responses to the Perils of E-Commerce*, 8 CONN. INS. L. J. 7 (2010); Philip Rawlings, *Cyber Risk: Insuring the Digital Age*, 128 BRIT. J. INS. L. 1 (2014); Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191 (2017).

[32] *See, e.g.*, Yogesh Malhotra, *Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling Beyond Value-at-Risk (VaR): Risk Uncertainty, and Profit for the Cyber Era*, NAT'L ASS'N OF INS. COMMISSIONERS (Jun. 24, 2017); Maochao Xu & Asa Lei Hua, *Cybersecurity Insurance: Modeling and Pricing*, SOC. ACTUARIES (2017), https://www.soa.org/globalassets/assets/Files/Research/Projects/cybersecurity-insurance-report.pdf.

[33] *See, e.g.*, Hemantha Herath & Tejaswini Herath, *Copula Based Actuarial Model for Pricing-Cyber Insurance Policies*, 2(1) INS. MKT. & CO. ANALYSES AND ACTUARIAL COMPUTATIONS 7 (2011); Sasha Romanosky et. al., *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk*, 5 J. CYBERSECURITY 1 (2019).

[34] *See, e.g.*, Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY: J. AM. B. FOUND. 1, 3 (2017); Trey Herr, *Cyber Insurance and Private Governance: The Enforcement Power of Markets*, 13 REG. & GOVERNANCE 1, 5 (2019); Daniel W. Woods & Tyler Moore, *Does Insurance have a Future in Governing Cybersecurity?*, IEEE SECURITY & PRIVACY 21 (2019).

[35] *See, e.g.*, Christian Biener et. al., *Insurability of Cyber Risk: An Empirical Analysis*, 40 GENEVA PAPERS RISK & INS. ISSUES & PRAC. 131 (2015).

[36] KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 3 (1986) (noting that some features of the insurance market "are left to individual choice" while others are regulated. Abraham further notes that "legal rules police the borderline between these realms by separating the issues that are subject to collective

Baruch Berliner's insurability criteria, these are "societal" considerations, distinguished from mere actuarial and market requirements.[37] These public policy considerations are part of a collective approach to insurance law, so far overlooked by the literature. Scholarship around the insurability of cyber risk as a reflection of societal norms and expectations is practically non-existent. Kenneth Abraham's astute observation that insurance scholarship is "the province of specialists focusing more on technical detail than on underlying structure and purpose"[38] thus seems most visible in the cyber insurance literature to date.

In November 2012, the U.S. Department of Homeland Security hosted a workshop on cybersecurity insurance involving insurance carriers, corporate risk managers, cyber experts, academics, and representatives of federal agencies. During the workshop "most participants agreed that every kind of cyber-related loss is potentially insurable—so long as there is a business case for offering insurance."[39] In considering the business case participants focused on only two conditions: "a value that can be assigned to some tangible or intangible asset, and a party that is willing to pay premiums to restore that value should a loss occur."[40] However, adopting a public policy

---

resolution through law from those that are left to individual decisions in the marketplace." Those rules implement collective decisions "about the scope, nature, price, and amount of insurance coverage that is desirable in different settings and about appropriate influence of public policies and principles on these features of insurance coverage. Regulation of these sort involves more than merely technical insurance issues; it involves *fundamental questions of political and legal philosophy*.") (emphasis added).

[37] Baruch Berliner has proposed a set of "dimensions of insurability" which have to be gone through by the professional risk carrier "like a checklist when assessing the insurability of risk." *See* Baruch Berliner, *Large Risks and Limits of Insurability*, 10 GENEVA PAPERS ON RISK & INS. ISSUES & PRAC. 313, 325 (1985); *See generally* BARUCH BERLINER, LIMITS OF INSURABILITY OF RISK (1982). Berliner lists five "actuarial" insurability criteria which include: (a) randomness of the loss occurrence, as in an occurrence needs to be intendent and predictable); (b) maximum possible loss must be manageable; (c) average loss amount upon occurrence must be moderate; (d) average period of time between two loss occurrences (the loss exposure) must be large; (e) Moral Hazard and Adverse Selection (caused in part due by information asymmetries) must be not excessive. Berliner further lists two "market" insurability criteria: (f) insurance premium needs to cover cost recovery and be affordable; (g) cover limits must be acceptable. Finally, Berliner introduces two insurability criteria that are "societal", those include (h) public policy, meaning that the insurance needs to be consistent with societal values; and (i) legal restrictions, meaning that all applicable law allows for such coverage. For an application of Berliner's insurability criteria see Christian Biener & Martin Eling*, Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*, 37 GENEVA PAPERS ON RISK & INS. ISSUES & PRAC. 77 (2012).

[38] ABRAHAM, *supra* note 36, at 3.

[39] Cybersecurity Insurance Industry Readout Reports, Cybersecurity & Infrastructure Security Agency (2012), https://www.cisa.gov/publication/cybersecurity-insurance-reports [hereinafter DHS Report].

[40] *Id*.

model for analyzing the insurability of cyber risk is important in order to provide an alternative lens through which players in the market may view questions around redistribution of risk.

This paper aims to lay the groundwork for a public policy analysis of the cyber insurance market. To accomplish this task, this paper focuses on three controversial categories of cyber harm: (1) acts of cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; and (3) administrative fines for violations of statutory data protection regulations.

Recognizing that many of the perils of the digital age are not unique but merely a cyber manifestation of already well-theorized non-cyber equivalents,[41] this paper proceeds to examine the rich history of each equivalence. Cyber terrorism insurance, for example, is examined as a subset of terrorism insurance, and ransomware coverage is understood by analogy to broader kidnapping and ransom policies.

Once these parallels are laid out, the paper examines whether the historical rationales that undergirded the general policies remain applicable in light of the scale and effects of contemporary cyber harms. Where there is a mismatch, this paper moves to propose limited regulatory interventions that could assist in achieving societal goals around the enforcement of cyber norms while simultaneously reducing the likelihood of moral hazards and adverse selection.

Insurance for an emerging technological risk is an evolving product. With each passing year significant changes occur to the markets, to risk analytics, and to the regulatory ecosystem. Nonetheless, capturing snapshots in the history of an insurance product can provide important insights into the underlying questions, concerns, and goals of future public policy. This paper was originally drafted in and contains examples from 2019 and 2020.[42] The COVID-19 pandemic has certainly changed the nature and size of the cyber

---

[41] Jerry & Mekel, *supra* note 31, at 8 (noting that "[i]ronically, the risks posed by e-commerce are not nearly as novel as the medium that makes such transactions possible. In fact, traditional causes of action abound . . . . Rather than presenting new theories of liability, the Internet's inherent accessibility has increased the rapidity and scale of these torts and infringements, should they occur.").

[42] This paper mostly reflects the world as of 2020, when the paper was originally drafted. For the author's updated analysis see Asaf Lubin, *Insuring an Evolving Technology*, 28(1) CONN. INS. L.J. 131 (2022). For other contemporary works see, *e.g.*, Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118, (2021); Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of Cyber Insurance Catastrophe*, 27 CONN. INS. L.J. 1 (2021); H. Bryan Cunningham & Shauhin A. Talesh, *Uncle Sam RE: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping*, 28(1) CONN. INS. L.J. 1 (2021); Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L.J. (forthcoming, 2022).

insurance market.[43] Despite these changes, the regulatory framework (or lack thereof) has remained largely unaltered. Therefore, the analyses and proposals of this paper continue to provide a useful guide to future policymakers and academics.

This paper proceeds in the following order. Section II introduces the Cyber Insurance Market. The section discusses the common characteristics of the standalone cyber insurance product, its scope of coverage and common exclusions, as well as the contemporary market for cyber insurance in the United States. The section then proceeds to highlight some of the key challenges in cyber insurance underwriting and modeling.

Section III moves to introduce the literature on public policy and insurable exposure. The section defends the application of a system of societal considerations in determining insurability, whereby "neither a free market nor a collective approach predominates."[44] In doing so, the section highlights the literature on Public-Private Partnership (PPPs) in enhancing cybersecurity, to justify further the need for public policy analysis of the cyber insurance market. Second, the section makes the case for technology-neutral regulation of the cyber insurance industry.

Section IV discusses three categories of cyber risk: cyber terrorism and state-sponsored cyberattacks, ransomware attacks, and fines for data protection violations. For each category, the paper analyzes whether existing historical and traditional rationales for insurability apply, based on a comparison to equivalent non-cyber perils. For each cyber risk, the paper proceeds to propose certain regulatory adjustments that could help shape the insurance process moving forward to maximize societal benefits. Table 1 at the end of the paper provides a summary of those regulatory adjustments.

Section V concludes.

II. THE CYBER INSURANCE MARKET

A. The Contemporary Market for Cyber Insurance

1. The Demand

While insurance for certain technological and computational errors and omissions has been on offer since the late 1980s, the standalone cyber

---

[43] COVID-19 was a contributing reason for the delayed publication of this paper. Updating the paper would have meant losing a historical snapshot of the nature of cyber insurance at the beginning of this decade that could serve future analysis and regulation. While certain sections of the paper have been revised and updated, as a whole, I mostly kept the work as it was.

[44] ABRAHAM, *supra* note 36, at 3.

insurance product is a relatively new addition to the portfolio of brokers and insurers.[45] In the early 2000s, even after the Y2K bug scare,[46] cyber policies were still hard to come by and most insurers offered limited and insufficient coverage to the perils of the internet age through traditional policies, such as Commercial General Liability (CGL), Errors and Omissions (E&O), and Directors and Officers (D&O) policies.[47]

The California Security Breach and Information Act entered into force in July 2003 and marked an important tidal shift in U.S. enforcement of data protection standards.[48] This breach notification law, and those that followed, mandates businesses to disclose any security breach that results in the exposure of personal information. Today, one can find breach notification laws in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.[49] California was also the first State to amend its breach

---

[45] For further reading on the history of the cyber insurance market see Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INSURANCE JOURNAL (Sept. 22, 2014), https://www.insurancejournal.com/magazines/features/2014/09/22/340633.htm.

[46] Kesan & Hayes, *supra* note 31, at 256 (noting cases of "insurance coverage for the cost of mitigating the infamous Y2K bug that caused millions of people to worry about whether the shift from 1999 to 2000 in computer clocks would cause mass chaos at midnight of January 1, 2000.").

[47] Jerry & Mekel, *supra* note 31, at 29 (concluding that "[t]oday's businesses, especially those utilizing technology, cannot afford to assume they are covered for cyber-risks simply because they have traditional coverages, such as CGL, E&O, and D&O policies, in place."). *See also* Paula M. Yost, Paul E.B. Glad, and William T. Barker, *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Computer Data*, 54 SMU L. REV. 2055 (2001) ("The fact that the terms of an insurance policy fail to support coverage for cyber-liability simply means the insurer has not provided it and the policyholder has not paid for it. That the standard liability insurance policy fails to protect against this new risk is hardly astounding. Purchasers of CGL coverage vary greatly in terms of their exposure to risk, and CGLs are typically designed to ensure the type of risks against which *most* policyholders need protection.").

[48] California Security Breach Information Act, S.B. 1386 (requiring organizations to notify all affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement," if their confidential or personal data is lost, stolen, or compromised, unless that data is encrypted.) The law currently defines only Social Security numbers, driver's license numbers, banking information, passwords, medical and health insurance information, and data collected through automatic license plate recognition systems, as personal information which breach must be reported. This is subject to change with the adoption of Personal information: data breaches, Cal. AB-1130 (Amended May 16, 2019) (expands notification requirements to biometric data, such as fingerprints, and iris and facial recognition scans, and to tax identification numbers, passport numbers, military identification numbers, and unique identification numbers issued on a government document.). For further reading see Zack Whittaker, *California to Close Data Breach Notification Loopholes Under New Law*, TECH CRUNCH (Feb. 21, 2019, 4:22 PM), https://techcrunch.com/2019/02/21/california-data-breach-laws/.

[49] *Security Breach Notification Laws: Views from Chief Security Officers*, The Samuelson Law, Technology & Public Policy Clinic, Univ. of California-Berkeley School of Law

notification law to demand, under certain circumstances, that affected persons be provided with identity theft prevention and mitigation services, such as a credit monitoring program.[50] In part due to these stringent regulatory requirements as well as being a primary target for more significant attacks, data breach costs for organizations are the highest in the United States when compared to the rest of the world, standing at around $8.64 million on average.[51]

But the notification and credit monitoring costs are only one of four process-related costs that drive the range of expenditures associated with an organization's data breach. Other costs concern detection and escalation (including forensic and investigative activities and crisis team management), post-data-breach responses (including legal and public-relations expenditures, regulatory fines, and the issuance of new accounts and credit cards), and lost-business costs (including reputational harms, revenue losses from systems' downtime, and costs of lost consumers).[52]

IBM Security and Ponemon Institute concluded that an average total cost of a data breach in 2020 stood at $3.86 million globally. A remote workforce (necessitated predominantly due to COVID19 restrictions) was "found to increase the average total cost of a data breach… by nearly $137,000, for an adjusted average of $4 million."[53] In prior reports, IBM Security and Ponemon Institute found that the average global probability of a material data breach (a breach involving a minimum of 1,000 lost or stolen records containing Personally Identifiable Information, or PII[54]) recurring to the same

---

(2007), https://www.law.berkeley.edu/files/cso_study.pdf; ALISSA M. DOLAN, CONG. RSCH. SERV., R44326, DATA SECURITY AND BREACH NOTIFICATION LEGISLATION: SELECTED LEGAL ISSUES (2015).

[50] Joseph J. Lazzarotti, *California Becomes First State to Require Credit Monitoring Services Information Following a Data Breach*, JACKSON LEWIS P.C. (Oct. 1, 2014), https://www.jacksonlewis.com/resources-publication/california-becomes-first-state-require-credit-monitoring-services-information-following-data-breach. The fact that only a handful of States have adopted the credit monitoring requirement is immaterial, as the California law applies to any business that collects data of California residents, and therefore would apply to most medium-to-large businesses with clients nationwide.

[51] Ponemon Institute LSC, *2020 Cost of a Data Breach Report* 12 (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report [hereinafter IBM's Cost of a Data Breach Report] (The second largest cost average was seen in the Middle East with $6.52 million. The average total cost increased in 12 of 16 countries or regions that were studied in both 2019 and 2020, with the biggest increase in Brazil, at 29%.).

[52] *Id.* at 7. *See also* COBURN ET. AL., *supra* note 25, at 5–12.

[53] *Id*. at 3.

[54] There are a variety of definitions for PII in various law, regulation, and agency guidance documents. *See* SIMON L. GARFINKEL, NAT'L INS. OF STANDARDS & TECH., NISTIR 8053, DE-IDENTIFICATION OF PERSONAL INFORMATION §1.4.2 (2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (discussing the variety of definitions for PII in various law, regulation, and agency guidance documents). *See also*

company over a two-year period stood at 27.9%.[55]

These figures are not surprising. Since 2005 the Privacy Rights Clearinghouse has identified more than 11 billion records that have been breached in nearly 9000 publicly reported cases of data security compromises across the United States.[56] The rise in cybercriminal activity around the theft of PII, and the adoption of state and federal data breach notification regulation increasing public awareness, served and continues to serve as the primary driver for the growth of the cyber insurance market.[57]

Losses from ransomware attacks are also on the rise. According to the FBI, an average of 4,000 ransomware attacks occur every day in the U.S. alone, [58] with experts predicting that a ransomware attack on businesses will

---

Erika McCallister et. al., Nat'l Inst. of Standards & Tech., Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) § 2-1 (2010) (quoting GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information (2008), http://www.gao.gov/new.items/d08536.pdf), https://www.dla.mil/Portals/104/Documents/GeneralCounsel/FOIA/Privacy/NIST%20SP%20800-122%20Guide%20to%20Protecting%20Confidentiality%20of%20PII.pdf (defining PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.").

[55] Ponemon Institute LSC, *Cost of a Data Breach Study: Global Overview* 3, 9 (2018), https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf [hereinafter IBM's Cost of a Data Breach] (additionally noting that the average time to identify the breach was 197 days and the average time to contain the breach was 69 days, with companies that contained the breach in less than 30 days saving over $1 million).

[56] *Chronology of Data Breaches, PRIVACY RIGHTS CLEARINGHOUSE,* https://www.privacyrights.org/data-breaches (last visited Mar. 1, 2021). According to a study by the information security firm Risk Based Security in the first six months of 2019 alone there have been more than 3,800 publicly disclosed breaches exposing more than 4 billion compromised records. *See Cyber Risk Analytics: 2019 Mid-Year QuickView Data Breach Report*, RISK BASED SECURITY (Aug., 2019), https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report. *See also* Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019, 6:31 AM), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#52eafdf7bd54 (summarizing the 2019 MidYear QuickView Data Breach Report).

[57] *See, e.g.*, *2018 Survey of Cyber Insurance Market Trends*, PARTNERRE5 (Oct. 2018), https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf [hereinafter PartnerRe 2018 Cyber Insurance Survey] (noting that among the 270 brokers and 70 underwriters from around the globe that were interviewed for the purposes of the study, 56% identified "news of cyber-related losses experienced by others" and 50% noted "experiencing a cyber-related loss," as the "top driver(s) of cyber product sales").

[58] *See Ransomware Prevention and Response for CISOs: How to Protect Your Network from*

occur every 11 seconds by the end of 2021.[59] In the second quarter of 2019, the average ransom payment stood at $36,295 and the average downtime stood at 9.6 days on average.[60] By 2020 the average ransom payment rose to $312,493 (an 861% increase), with downtime more than doubling to 21 days on average.[61]

These examples help explain why the World Economic Forum has identified cyber-attacks and data fraud or theft as two of the top five risks to the global economy today, coming just behind extreme weather conditions, natural disasters, and the threat of climate change.[62]

2. The Supply

Against this backdrop, cyber insurance was introduced to support private and public entities in managing this rising risk.[63] Contemporary cyber insurance coverage takes the form of one of three potential policies: (1) a

---

Ransomware, FBI 2, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Mar. 5, 2022).

[59] *Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion*, NAT'L L. REV. (Feb. 13, 2020), https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion.

[60] These statistics are based on the quarterly reports of the information security firm Coveware. Coveware's reports analyze anonymized ransomware data handled by the security firm's incident response team and other incident response firms that rely on Coveware's incident response platform. *Global Ransomware Marketplace Report: Q2 2019*, COVEWARE (Jul., 2019), https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread.

[61] Ransomware Task Force Report, *supra* note 9, at 7.

[62] *See The Global Risks Report 2019*, WORLD ECONOMIC FORUM 8 (14th ed., 2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. *See also Counting the Cost: Cyber Exposure Decoded*, LLOYDS 7 (Jul. 10, 2017), https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost [hereinafter LLOYDS REPORT] (suggesting that a malicious hack taking down a cloud service provider could result in estimated losses of $53 billion and attacks on computer operating systems run by a large number of businesses around the world could result in estimated losses of $28.7 billion. These figures parallel losses triggered by Superstorm Sandy, the second costliest tropical cyclone on record with costs of between $50–$70 billion).

[63] For the purposes of this paper's analysis, I exclude personal cyber policies. These are policies offered to individuals as opposed to businesses and organizations. It is predominantly geared to cover identity theft in cases of mass data breaches but may also include coverage for cyber extortion payments or for the costs of data restoration. For example, State Farm offers upgrading one's homeowner's insurance with an endorsement that covers losses relating to cyber-attacks, with a limit of $15,000 for just $25 premium per year. To read more, see Mark Fitzpatrick, *What is Personal Cyber Insurance? And How Can Homeowners Buy a Policy?*, VALUEPENGUIN (Mar. 5, 2019), https://www.valuepenguin.com/personal-cyber-home-insurance.

standalone cyber insurance dedicated policy; (2) an endorsement of cyber coverage, as a package, within an existing insurance line, such as commercial crime insurance, P&C, D&O, and E&O, and most recently home owners insurance;[64] or (3) coverage provided under a traditional policy that does not explicitly reference cyber as being either included or excluded from coverage.[65] While the first two categories of policies offer explicit cyber protections, the latter is "silent" and "non-affirmative,"[66] and therefore poses significant risk of exposure and legal uncertainty to both insurers and the insured.[67] As a result of this growing uncertainty, the New York Department of Financial Services issued an insurance circular in February 2021 requiring "all authorized property/casualty insurers that write cyber insurance" to "manage and eliminate exposure to silent cyber insurance risk."[68] The circular is the first attempt at state regulation of cyber insurance in the United States.

In a PartnerRe survey of 270 brokers and 70 underwriters from around the globe, it was confirmed that the most popular reason (70%) for why buyers will prefer moving from endorsement policies to standalone policies is the fact that they are seeking dedicated limits available expressly from cyber markets.[69] As one broker noted "the coverage granted [under an "endorsement" cyber coverage] is very limited and creates somewhat of an illusion that the insured is covered for cyber threats, when in fact most of

---

[64] *Id.*

[65] *EU-U.S. Insurance Dialogue Project, February 2020 Summary Report*, EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY 3 (Oct. 31, 2018), https://www.eiopa.europa.eu/sites/default/files/publications/eu-us-cyber-insurance-wg-feb-2020.pdf [hereinafter EIOPA, The Cyber Insurance Market].

[66] For further discussion see *Affirmative vs. Silent Cyber: An Overview*, EUROPEAN GUY CARPENTER & COMPANY LLC (Oct., 2018), http://www.guycarp.com/content/dam/guycarp/en/cmp/Affirm%20vs%20Silent%20Cyber%20Briefing%20FINAL%20(2).pdf.

[67] Compare, for example, the following two cases which highlight legal uncertainty. In Zurich American Insurance Co. v. Sony Corp. of America et. al., N.Y. SUP. CT. 651982/2011 (Feb. 21, 2014) the court considered a Sony PlayStation hack that resulted in the compromise of 77 million users' data, and losses of $2 billion. Sony's Coverage B of CGL (Personal and Advertising Injury Coverage) was silent about cyber coverage. The court deemed the policy inapplicable, however, noting that a cyber intrusion by hackers leading to theft of data was not akin to "oral or written publication . . . violating a person's right to privacy." The case was ultimately settled before the appeal. On the other hand, in Hartford Casualty Insurance Company v. Corcino & Associates et al., No. 13-3728, 2013 WL 5687527, at *1 (C.D. Cal. Oct. 7, 2013) the court reached the opposite conclusion, finding that a silent CGL policy did cover third-party hacking in the case of a data breach of hospital records involving 20,000 patients.

[68] Insurance Circular Letter No. 2, *Cyber Insurance Risk Framework*, N.Y. DEP'T. FIN. SERV. (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

[69] PartnerRe 2018 Cyber Insurance Survey, *supra* note 57, at 7.

these endorsement coverages are narrow in scope and often with small limits."[70]

As with all lines of insurance, cyber coverage is differentiated between First- and Third-Party coverage (i.e., costs directly borne by the insured, versus those incurred in liability to others, often through litigation). Common coverage areas include network business interruption, data restoration costs, loss of income, cost of claims, defense, settlement and other legal fees, crisis management and public relations, forensic investigations, extortion payments, and credit monitoring and call center expenses in data breach cases.[71] In 2019 average premiums were priced between $10,000 and $25,000, with limits ranging between $10–25 million and reaching as high as $50 million.[72] With the rise in ransomware losses over the past two years, however, "premiums have gone up by 7% on average for small firms and between 10% and 40% for medium and large businesses."[73] In fact, some insurers, namely in the areas of education and healthcare, have gone further in "reducing their exposure by reducing coverage, lowering coverage limits, and putting a lower cap on ransomware payouts. Others have begun adding more restrictive policy terms and including additional exclusions."[74]

Corporate actors are not the only ones jumping on the insurance bandwagon. Recent trends have seen governments acquiring cyber insurance policies. More than a dozen states now have such programs in place, with the first being the state of Montana in 2011.[75] Georgia has the largest cyber coverage, paying $1.8 million per year in premiums for $100 million in coverage and a $250,000 deductible per cyber-related incident.[76] Cities, too, are turning to insurance. The Houston City Council, for example, paid $471,000 in August 2018 for cyber coverage. Houston's cyber insurance policy offers coverage for up to $30 million in expenses related to security

---

[70] *Id*.

[71] *See* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance*, 43 L. & SOC. INQ. 417, 427 (2018).

[72] For a complete analysis of all available coverage, scope of coverage, and the average costs across the market in the United States see Romanosky et. al., *supra* note 33, at 2; COBURN ET. AL., *supra* note 25, at 238–39 (Table 9.1).

[73] Jai Vijayan, *Ransomware Losses Drive Up Cyber-Insurance Costs*, DARK READING (Jun. 29, 2021), https://www.darkreading.com/risk/ransomware-losses-drive-up-cyber-insurance-costs/d/d-id/1341436.

[74] *Id.*

[75] Jenni Bergal, *Worried About Hackers, States Turn to Cyber Insurance*, INSUR. J. (Nov. 13, 2017), https://www.insurancejournal.com/news/national/2017/11/13/470991.htm; Brian Tumulty, *More State Governments are Buying Cyber Insurance*, BOND BUYER (Feb. 20, 2021), https://www.bondbuyer.com/news/cyber-insurance-grows-among-state-governments.

[76] *Id.*

breaches in the city's computer networks.[77] In fact, most of the 25 largest U.S. cities have, or are now in the process of acquiring, cyber insurance, according to the *Wall Street Journal*.[78]

According to NAIC, as of 2020, 136 individual insurers offered standalone cyber insurance policies to businesses and individuals in the U.S.[79] The U.S. market accounts for approximately 85%–90% of all gross written premiums, while the EU accounts for only about 5%–9%.[80] Within the U.S. market, the top 10 insurers wrote 79.8% of the total standalone cyber insurance policies issued domestically.[81]

In an academic study involving the content analysis of 235 cyber insurance policy dockets collected from Pennsylvania, New York, and California, the most common exclusions included criminal or fraudulent acts, negligent disregard for computer security, loss to systems not owned or operated by the insured, bodily injury and physical damage, and contractual liability.[82] Note that nearly half of all policies examined further excluded claims related to war, military action, state-sponsored operations, or terrorism, as well as claims related to extortion or ransom. Nonetheless, a third of all policies explicitly included coverage for ransomware attacks, and in a few rare cases cyber-terrorism and military action were too explicitly covered.[83]

---

[77] *Id*.

[78] Scott Calvert & Jon Kamp, *More U.S. Cities Brace for 'Inevitable' Hackers*, WALL STREET JOURNAL (Sept. 4, 2018), https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401. Note that such policies may be purchased through municipal intergovernmental risk pools and not through commercial insurers. For example, the Houston cyber insurance policy was purchased through the Texas Municipal League risk pool. For more on intergovernmental risk pools and self-insurance as an alternative to commercial insurance policies see John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539, 1558–66 (2017).

[79] *See* Denise Matthews, *Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement*, National Association of Insurance Commissioners (Dec. 4, 2020), https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_1.pdf [hereinafter NAIC Cybersecurity Insurance Report].

[80] OECD, ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 60 (2017), https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page1.

[81] NAIC Cybersecurity Insurance Report, *supra* note 79, at 2.

[82] *See* Romanosky et. al., *supra* note 33, at 7.

[83] *Id*. at 7–8. In all other cases coverage was neither excluded nor explicitly provided. Note that this study relies only on policies from the admitted markets (policies that were filed with the state insurance commissions and comply with all state regulations). There is a question as to the amount of cyber insurance being sold through the excess and surplus insurance lines. At least according to some estimates, "as much as 90% of the cyber insurance market is with nonadmitted carriers." *Id*. at 3, n.11. Especially with regards to coverage of ransomware, cyber-terrorism, and state-sponsored attacks, it is fair to assume those would

Exclusions such as these are one reason why despite major developments in the cyber insurance market, cyber risk remains significantly underinsured. The cyber insurance gap, which is the value of assets at risk not covered by insurance policies, is most striking in the case of a catastrophic cyber event. According to a study by Lloyds, a malicious hack taking down a major cloud service provider could result in estimated losses of $53 billion worldwide, of which the uninsured gap could be as high as $45 billion (meaning that less than a fifth of the economic losses, 17%, will be covered).[84] In the case of an exploitation of a mass vulnerability on a computer operating system run by a large number of businesses worldwide, losses are estimated at $28.7 billion, of which as much as $26 billion may not be covered (meaning that only 7% of economic losses are covered).[85]

There is significant variation in engagement with cyber insurance around the globe,[86] and while the U.S. cyber insurance market is by far the most mature, uninsured cyber risks outside the U.S. could have indirect negative effects on U.S. markets.[87] Other reasons for the cyber insurance gap include: (a) declining availability of cyber insurance and rising costs as supply chain attacks and ransomware hacks continue to wreak havoc;[88] and (b) caution taken by both insurers and insured given uncertainties surrounding cyber insurance underwriting and the costs of coverage.

---

be covered more regularly through the excess lines. *See also Commonality of risk assessment language in cyber insurance Recommendations on Cyber Insurance*, EU AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA) 16–17 (Nov., 2017), https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance [hereinafter ENISA Report] (concluding that of the 10 examined policies from EMEA carriers, 9 covered cost of ransom payment explicitly and the last one offered coverage through an endorsement); BAIRD WEBEL, CONG. RSCH. SERV., R45707, TERRORISM RISK INSURANCE: OVERVIEW AND ISSUE ANALYSIS FOR THE 116TH CONGRESS (Apr. 26, 2019), (citing a Treasury Department finding that "50% of the standalone cyber insurance policies (based on premium value) included terrorism coverage.").

[84] LLOYDS REPORT, *supra* note 62, at 48.

[85] *Id.*

[86] Consider for example the EU market, which is still at its infancy. As of 2017 it comprised of only 50+ carriers generating roughly $3–4 billion in premiums, with the expectation that it will reach some $20 billion in premiums by 2025. *See* ENISA report, *supra* note 83, at 16.

[87] Increased globalization and continued technological change and digitalization open the door for "downstream effects", especially along the supply, service, and distribution chains. As I discuss below, ambiguity around liability and scope coverage in this context opens the door for potential losses. For the distinction between "first order consequences" and "second and third order consequences" from a cyber-attack see Hake et. al., *supra* note 30, at 14 n.23.

[88] Nicolás Rivero, *Ransomware hacks are pushing cyber insurance premiums to record levels*, QUARTZ (July 21, 2021), https://qz.com/2036127/ransomware-hacks-are-driving-up-premiums-for-cyber-insurance/.

B. The Cyber Insurance Underwriting Process

1. How Do Insurers Underwrite Cyber Risk?

Underwriting refers to the "collective process that insurers use to decide whether or not to offer coverage to a prospective insured and, if so, at what amounts, […and] of course, at what price."[89] To be sustainable, an insurer has to be able to underwrite based on the specific characteristics of the covered risk. This requires a combination of two separate bodies of knowledge. First, the insurer has to develop a working understanding of the general risk environment. In the cybersecurity context, insurers have turned to various international and national cybersecurity voluntary standards, including among others,[90] the International Organization for Standardization (ISO) and International Electrotechnical Commission's (IEC) 27001/2 standard[91] and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[92] Insurers

---

[89] *See* Tom Baker & Sean Griffith, *Predicting Corporate Governance Risk: Evidence from the Directors' & Officers' Liability Insurance Market*, 74 U. CHI. L. REV. 487, 508 (2007).

[90] Other standards worth mentioning include the Information Technology Infrastructure Library (ITIL) developed by the joint-venture AXELOS. ITIL essentially provides a set of interrelated best practices that provide guidance for developing, delivering, and managing enterprise IT service; Control Objectives for Information and Related Technology (COBIT), which is a framework created by Information Systems Audit and Control Association (ISACA) for IT governance and management; and The Open Group's Architecture Framework (TOGAF). At the heart of the TOGAF framework is the Architecture Development Method, or ADM. It describes the methodology for developing and managing an enterprise architecture's lifecycle through continuous/cyclic and iterative phases. *For further reading* see *COBIT vs ITIL vs TOGAF: Which Is Better For Cybersecurity?*, UPGUARD (Aug. 23, 2019), https://www.upguard.com/articles/cobit-vs.-itil-vs.-itsm-which-is-better-for-cybersecurity-and-digital-resilience.

[91] Under the ISO/IEC 27001/2 standard organizations are required to establish an information security management system (ISMS), which involves systematically examining information security risks and designing and implementing a comprehensive suite of information controls (including *e.g.* around access control, cryptography, physical and environmental security, human resource security, incident management, and supplier relations). Ultimately each Organization will follow a PDCA cycle: Plan (establish the ISMS policies, objectives, and procedures), Do (Implement the ISMS), Check (assess and measure the performance of the processes under the ISMS) and Act (undertaking corrective and preventive actions on the basis of internal ISMS audits). *See* ISO/IEC 27001:2013, Information Technology Security Techniques, Information Security Management Systems – Requirements (2d ed.), https://www.iso27001security.com/html/27001.html.

[92] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Version 1.0 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Under this standard organizations follow both the Framework's core which comprises of a "a set of activities to achieve specific cybersecurity outcomes, and

also rely on industry-specific standards, such as the Payment Card Industry Data Security Standard (PCI DSS) that targets organizations handling branded cardholders' data,[93] or the European Telecommunications Standards Institute (ETSI) TS-103-645, a standard establishing a security baseline for Internet-connected consumer products,[94] known as Internet-of-Things (IoT).[95] Indeed, today, "all leading insurers see the use of cybersecurity standards as an indicator of risk awareness and maturity."[96] They seek to

---

references examples of guidance to achieve those outcomes." *Id.* at 6. These are divided into five major functions (Identify, Protect, Detect, Respond, and Recover) which themselves are then subdivided into groups of categories (including for example "asset management" or "detection processes"). The standard further follows a set of framework implementation tiers running from 1-4 that describe the "increasing degree of rigor and sophistication in cybersecurity risk management practices." *Id.* at 7–11. For the U.K. equivalent standard, *see 10 Steps to Cyber Security*, The National Cyber Security Centre (Nov. 17, 2018), https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security (Originally published in 2012, it is now adopted by most of the top 350 companies listed on the London Stock Exchange. It encompasses a risk management regime which covers a large number of categories similar to those adopted under the NIST framework.).

[93] For further reading on the standard's specific requirements, *see* Asim Mahmood, *An Introduction to PCI DSS*, CRYPTOMATHIC (Mar. 23, 2018), https://www.cryptomathic.com/news-events/blog/an-introduction-to-pci-dss.

[94] For further reading on the standard's specific requirements, *see* TS 103 645, *Cyber Security for Consumer Internet of Things: Technical Specification*, ESTI, Version 1.1.1 (2019-02), https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

[95] IoT, the internetworking of devices, buildings, vehicles, and appliances, is rapidly expanding. Sensors, actuators, software, and network connectivity are increasingly embedded in everyday products like smart cars, wearable and portable fitness trackers and smart home security systems. There is no common definition for the 'Internet of Things'. The most recent version of the Internet of Things (IoT) Cybersecurity Improvement Act now pending before Congress, defines IoT devices as a "physical object" that: "(1) is capable of connecting to and is in regular connection with the internet, (2) has computer processing capabilities that can collect, send, or receive data; and (3) is not a general-purpose computing device, including personal computing systems, smart mobile communications devices, programmable logic controls, and mainframe computing systems." *See* IoT Cybersecurity Improvement Act of 2019, S.734 (11 March 2019). Note that this definition excludes traditional computing systems and smartphones, whereas other definitions might not. *See e.g.,* Mehdia Ajana El Khaddar & Mohammed Boulmalf, *Smartphone: The Ultimate IoT and IoE Device*, *in* SMARTPHONES FROM AN APPLIED RESEARCH PERSPECTIVE 137 (Mohamudally ed., 2017). For a broader theoretical discussion around their nature and scope of IoT devices, *see* Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L. REV. 583 (2019). David Rose had called these devices "enchanted objects," as they took ordinary things and made them extraordinary. DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 7 (2014). For a general analysis of the technological considerations, economic environment, and legal approaches to the Internet of Things, *see* ROLF H. WEBER & ROMANA WEBER, INTERNET OF THINGS: LEGAL PERSPECTIVES (2010).

[96] *See* ENISA Report, *supra* note 83, at 22.

determine whether their insureds are complying with these external benchmarks as a main tool for risk assessment. At the same time, however, given the lack of consensus both internationally and domestically around a legally binding cybersecurity standard,[97] cyber insurers are picking-and-choosing from a relatively large pool of standards and incorporating them into their underwriting process in non-uniform ways.[98] A prospective cyber insurance buyer, thus "may face different questions regarding the compliance to or application of security standards from different carriers."[99]

A second way insurers tackle the issue of developing general cyber institutional expertise, is through partnering with third-party vendors of information security services as well as legal and compliance firms who provide *ex ante* risk assessment services.[100] Insurers also hire cybersecurity

---

[97] The U.S. position was articulated by J. Michael Daniel, former Special Assistant to President Obama and Cybersecurity Coordinator who contended that a "consensus-based, private sector-driven international standards development process, with input from all interested stakeholders, is superior to a top-down, national government-controlled approach to standards." (J. Michael Daniel, *Engaging the International Community on Cybersecurity Standards*, Press Release, White House (Dec. 23, 2015), https://obamawhitehouse.archives.gov/blog/2015/12/23/engaging-international-community-cybersecurity-standards). This may be true, but only in the long haul. International consensus takes a long time to crystallize, and in the meantime the lack of regulation translates to a lack of certainty forcing private insurers to maneuver through uncharted terrain in search of a map and a compass.

[98] *See* Romanosky et. al., *supra* note 33, at 12 ("The focus on sensitive data, particularly those to debit and credit card transactions and the detailed questions concerning PCI/DSS standard compliance is not surprising given that in the past decade data protection industry standards and data breach laws have developed and have been widely institutionalized in the USA . . . It is noteworthy, however, that standards and frameworks for information technology management, such as the ITIL and COBIT are not mentioned, and in only one instance was an ISO standard mentioned. Also, the recently developed NIST Cybersecurity framework is not mentioned, though from conversations with carriers, they are beginning to integrate it into these questionnaires.").

[99] *See* ENISA Report, *supra* note 83, at 22. Woods et. al., show that even where the insurers commit to adopting a particular standard, such as the internationally recognized ISO/IEC 27001/2 security management scheme, their underwriting process may still show bias towards certain security control and not others. For example, of the 24 cyber insurance proposal forms they examined 15 mentioned "a business continuity plan", which could indicate that insurers are more familiar with traditional controls common in their other lines of insurance and are prioritizing them over other controls which they might be less familiar with. *See* Daniel Woods et. al., *Mapping the coverage of security controls in cyber insurance proposal forms*, 8 J. INTERNET SERV. & APP. 1, 10 (2017). Another market failure could be triggered by a perverse incentive scheme for insurers, as they note "a rational insurer is concerned with the controls which directly mitigate the risks that they are liable for, creating a question of misaligned incentives" especially when each insurer is cautious about the scope of coverage they provide. *Id*. at 11.

[100] *See* Romanosky et. al., *supra* note 33, at 12–13 (noting that "carriers employed the services of other companies to help develop premiums," while additionally collecting

experts to work in-house. It is now common to see former upper echelon cyber specialists and agents from the FBI or GCHQ move into the insurance world.[101] This development is welcome, as it increases the capacity of the insurers to properly examine cyber posture and to compute effective pricing and premiums. Insurers with in-house cyber expertise could thus play a more positive role as promoters, and in certain scenarios even enforcers, of cyber norms and best practices.[102] In fact, as insurers acquire a greater understanding of the cybersecurity threat landscape, feedback loops are beginning to emerge where the insurers are the ones providing insight to the information security community and not the other way around.[103]

In addition to a proper understanding of the general threat environment, insurers must also develop an intimate familiarity with their policyholders' particular cyber risks. To acquire such level of knowledge, insurers traditionally rely on a combination of three principal sources of information: the written application (which includes standardized questionnaires), independent research of publicly available data, and personal meetings with the insured.[104] By relying on these sources, insurers produce a set of data

---

"industry, academic, or government reports" about basic loss data which was then used to develop risk models); *See* Russ Cohen, Cyber COPE: Transforming Cyber Underwriting, CHUBB 7 (Oct. 2016), https://www.chubb.com/us-en/_assets/doc/chubb-cyber-cope-whitepaper_09.16.pdf (noting that Chubb worked with "strategic allies within the cyber security industry to develop a set of questions that provides the necessary data elements to help underwriters comprehensively assess cyber risk."). Recently, Cisco, Apple, Aon and Allianz announced a risk management initiative integrating all of their services to ensure greater resiliency. *See Cisco, Apple, Aon, Allianz introduce a first in cyber risk management*, Press Release, APPLE (Feb. 5, 2018), https://www.apple.com/newsroom/2018/02/cisco-apple-aon-allianz-introduce-a-first-in-cyber-risk-management/. While this offers yet another positive example of expanding cyber capacity on the part of insurers, the development also triggers complicated questions around conflicting ethical and regulatory obligations that each of the vendors possesses.

[101] *See* Oliver Ralph, *Insurers pay premium for cyber security experts*, FINANCIAL TIMES (Jun. 6, 2018), https://www.ft.com/content/017fb9fa-5d01-11e8-9334-2218e7146b04.

[102] Consider in this regard recent reporting that the world's biggest insurers plan to work together on an assessment of the most effective cybersecurity software and technology sold to businesses. *See* Leslie Scism, *Insurers Creating a Consumer Ratings Service for Cybersecurity Industry*, WALL STREET JOURNAL (Mar. 26, 2019), https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600.

[103] *See, e.g.*, Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 205-13, 247-48 (2012) (describing how insurers can modify policyholder behavior through ex ante coverage requirements); Kesan & Hayes, supra note 31, at 268 ("Insurers are in a unique position to push companies to adopt more consistently secure data-security practices including encryption, firewalls, intrusion detection systems, and stronger internal controls for data handling.").

[104] *See* Baker & Griffith supra note 89, at 510–11 (the process carries with it some legal sanctions to ensure its quality, as Baker and Griffith write: "[b]ecause an applicant furnishing

points that contribute to evaluating the overall risk. For example, global insurer Chubb has developed an underwriting process it calls "Cyber COPE" which combines all data to produce a comprehensive analysis of four measurements: the insured's Components (e.g., number of endpoints and network connections, software versions, and data center locations), Organization (policyholder's industry, quality of IT and security policies, use of industry standards), Protection (use of firewalls, monitoring, encryption, and incident response readiness policies), and Exposures (types of outsourcing, amounts of sensitive data, any political or criminal motivation against the insured).[105]

In assessing the individual risk posed to a buyer, insurers turn to yet another external benchmark in the form of ratings. In May 2019, Moody slashed Equifax's rating outlook from stable to negative, citing costs associated with a 2017 data breach as the reason.[106] It was the first-time cybersecurity was ever relied upon as a justification for a downgrade by Moody.[107] In the same way that credit reporting agencies review a company's financials and assign consumer and bond credit scores that are used to evaluate a company's economic stability, so have cyber security firms began to offer a "security rating" for insurers that based on open-source assessment of a company's cybersecurity posture.[108] Lacking direct access to the

---

untrue information creates the basis for a subsequent rescission action, the credibility of information provided through the application is enhanced."); *See also* Anya E.R. Prince, *Tantamount to Fraud?: Exploring Non-Disclosure of Genetic Information in Life Insurance Applications as Grounds for Policy Rescission*, 26 HEALTH MATRIX 255, 281 (2016) ("The underlying policy rationale for allowing insurance rescissions is that individuals should not be unjustifiably rewarded for making a misrepresentation on an application, especially a knowing one. If insurers would not have approved the application based on omitted information, why should they ultimately be responsible for paying the beneficiaries the claim?").

[105] *See* Cohen, *supra* note 100, at 3. Note that the original COPE (construction, occupancy, protection, exposure) is a traditional property insurance underwriting framework.

[106] In September of 2017, the Credit Reporting giant Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. *See* Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (Jul. 22, 2019), https://www.nytimes.com/2019/07/22/business/equifax-settlement.html. The total costs from the cleanup are estimated at $1.4 billion. *See* Matthew J. Schwartz, *Equifax's Data Breach Costs Hit $1.4 Billion*, BANK INFO SECURITY (May 13, 2019), https://www.bankinfosecurity.com/equifaxs-data-breach-costs-hit-14-billion-a-12473.

[107] Kate O'Flaherty, *Equifax Becomes First Firm To See Its Outlook Downgraded Due To A Cyber-Attack*, FORBES (May 28, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/05/28/equifax-becomes-first-firm-to-see-its-outlook-downgraded-due-to-a-cyber-attack/#194599c45671.

[108] *See e.g. Cyber Insurance Risk Assessment: Data Sheet*, MANDIANT (2018) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-cyber-

networks of the insured,[109] insurers turn to insurance technology companies and information security firms to assist them in developing cyber risk profiles for underwriting purposes.

Based on both the general threat analysis and the particular needs of the insured, insurers move to price their cyber insurance products. One study of cyber insurance policies concluded that pricing strategies vary significantly across cyber insurers. Some insurers adopt *a flat rate model* (computing premiums on the basis of a fixed price for first- and third-party coverage to all insureds).[110] Others adopt a *flat rate with hazard groups* approach (computing premiums on the basis of a fixed rate and a single modifier based on identification of "hazard group"—low, medium, or high—depending on the business type, scope of online activity, and amounts of stored PII).[111] A third category of insurers adopt a *base rate analysis* (with the base rate being assessed "as a function of the insured's annual revenues or assets," then multiplied by both industry specific risks—*e.g.* non-profit vs. for-profit, public vs. private, retail vs. healthcare—and standard insurance variables—*e.g.* historical claims, time retention, coinsurance).[112] Finally, a fourth category of insurers rely on base rates with security questions (adjusting the

---

insurance-risk-insurance.pdf (This FireEye service is designed for insurance provides and applies the COPE model to provide a grading of the technology and processes employed so to facilitate the identification and classification of cyber risk); BitSight Security Ratings for Cyber Insurance, BitSight, https://www.bitsight.com/security-ratings-cyber-insurance ("Unlike subjective questionnaires and self-assessments, BitSight provides an easy-to-understand rating along with a comprehensive report, including 12 months of historical data and comparisons with industry benchmarks." The data is provided through a web-based platform and can be used both for underwriting and to continuously monitor a company's security performance alerting them when potential threats or unusual activity are detected). *See also* Shauhin A. Talesh & Bryan Cunningham, *Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. 967, 999–1001 (2021) (describing the role of cybersecurity firms in conducting "endpoint vulnerability assessments" as well as analysis companies' "IP address, domain name, and other publicly accessible information," including from the dark web, to produce ranking).

[109] Insurers offer, on an optional basis, penetration testing and scanning of systems through external information security providers with which the insurer contracts. None of these third-party vendors provide the insurer access or knowledge about the networks of the insured (especially not post-incident), but the insurer nonetheless may prefer to rely on them in deciding to reduce premiums or remove sub-limits, as they were personally picked by the insurer for the quality of their services. See Understanding Cyber Insurance – A Structure Dialogue with Insurance Companies, EIOPA 8 (2018) https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf [hereinafter EIOPA, Understanding Cyber Insurance].

[110] *See* Romanosky et. al., *supra* note 34, at 13–17.

[111] *Id.*

[112] *Id.*

rate in light of direct responses to questions in the questionnaire).[113] Ultimately, the level of sophistication of premium calculation on the basis of any of these strategies remains unclear. This is because "it is highly unlikely that any insurance underwriter would know the marginal reduction in risk" resulting from failure to adopt a particular standard or practice such as use of two-factor authentication or the running of annual penetration testing on the insured's network.[114]

2. Key Challenges for Cyber Insurance Underwriting

In May 2018, Warren Buffett argued against his holding company Berkshire Hathaway becoming a leader on cyber insurance, suggesting that "I don't think we or anybody else really knows what they're doing when writing cyber," and concluding further that if anyone says otherwise, they are "kidding themselves."[115]

The primary reason why cyber insurance underwriting is proving so difficult concerns the lack of historical claims data and security data. Beyond the relatively short length of time cyber risk has been written, there are additional factors that exacerbate informational gaps: the dominance of a few insurance companies and their reluctance to share much of their emerging dataset and models,[116] the refusal of companies who have suffered an attack to publicly disclose necessary security data, and the cautious approach of governments' cybersecurity agencies in releasing intelligence around national cybersecurity threats.[117] In the absence of historical data, cyber insurers are forced to rely on qualitative models for developing policies. This

---

[113] *Id*.

[114] *Id*. at 16.

[115] Katherine Chiglinsky & Sonali Basak, *Buffett Cautious on Cyber Insurance Because No One Knows Risks*, BLOOMBERG (May 5, 2018), https://www.bloomberg.com/news/articles/2018-05-05/buffett-cautious-on-cyber-insurance-because-no-one-knows-risks. *See also* Trey Herr, *Cyber Insurance and Private Governance: The Enforcement Power of Markets*, 15 REG. & GOVERNANCE 98, 99–101 (2021) (suggesting that insurers generally are underinformed to be able to make proper risk assessments).

[116] *See* DHS Report, *supra* note 39, at 15 ("Many [workshop] participants identified a lack of information sharing about cyber risks and the frequency, magnitude and loss impact of actual and potential cybersecurity incidents as a major obstacle to preventing a more robust cybersecurity insurance market. One participant stated that top carriers don't want to share such information – among themselves or with government – because they ultimately 'give more than they get.' He added, however, that carriers would be more inclined to share if there was business value to doing so.").

[117] *See generally* Elizabeth Blosfield, *Data Deficit Remains Key Challenge for Cyber Insurance Underwriters*, INSUR. J. (Jun. 18, 2019), https://www.insurancejournal.com/news/national/2019/06/18/529663.htm (analyzing the data deficit as a challenge to cyber insurance underwriting).

may result in suboptimal pricing. As a number of researchers from the RAND Institute noted humorously in a presentation given during the 2019 annual FTC PrivacyCon:

> How do carriers price cyber risk? Suboptimally [the three most common statements you hear from carriers with regards to pricing are:]
> "Limitations of available data have constrained the traditional actuarial methods used to support rates." (*Translation: "We don't know"*); "The base retentions were set at what we believe to be an appropriate level for the relative size of each insured" (*Translation: "We're guessing"*); "The rates for the above-mentioned coverages have been developed by analyzing the rates of the main competitors." (*Translation: "We're using someone else's guess"*).[118]

The European Insurance and Occupational Pensions Authority (EIOPA) concluded in a 2018 report that the most frequently mentioned industry concern regarding current cyber insurance underwriting practices "was the tendency of broadening coverage, terms, and conditions."[119] As the report goes on to explain, insurers showed this tendency in the light of "increasing competition and a limited understanding of the risks."[120] As a result, insurers are unable to properly assess the indemnity required to recover a business from new and ever-developing cyber events, and simply succumb to policyholders' market demands.[121] The report ultimately concluded that "insurers may be underwriting cyber risk based on minimal information, without the use of any modeling."[122]

Yet another concern relates to the security questionnaires upon which the carriers rely.[123] These questionnaires are common practice in the insurance industry and aim at standardizing the process of soliciting the best possible

---

[118] Sasha Romanosky et. al., *Content Analysis of Cyber Insurance Policies*, PRIVACYCON PRESENTATION (last visited June 2019), https://www.ftc.gov/system/files/documents/public_events/1223263/panel012_cyberinsurance_policies.pdf; s*ee also* DHS Report, *supra* note 39, at 33 (noting that carriers are making up pricing schemes "as they go along.").

[119] *See* EIOPA, The Cyber Insurance Market, *supra* note 65, at 2–4.

[120] *Id*.; *see also* Woods & Moore, *supra* note 34, at 6 (concluding that "The private governance role of cyber insurance is limited by market dynamics. Competitive pressures drive a race-to-the-bottom in risk assessment standards and prevent insurers including security procedures in contracts.").

[121] EIOPA, The Cyber Insurance Market*, supra* note 65, at 6–7.

[122] *Id*.

[123] Talesh & Cunningham, *supra* note 108, at 996 (describing the cyber insurance application as "rigid, mechanical, check-the-box format inadequate for the prospective insurance buyer to communicate accurately the company's cybersecurity posture.").

comprehensive understanding of the overall security posture of an applicant.[124] Some of the questions, however, seem intentionally vague and open the door for a later denial of coverage. For one anecdotal example, consider a questionnaire from a major carrier that asks under the "Risk Control Self-Assessment" rubric the prospective insured to clarify whether they prominently disclose their privacy policy "and always honor it." To add insult to injury, the insured is given the option of only answering Yes or No to this question in the questionnaire, without the ability of elaborating further.[125]

One study examined 45 of these questionnaires. It concluded that the focus of most of the surveys centered around data protection and data breach notification laws, emphasizing amounts and types of data managed by the applicant.[126] On the other hand, there was little attention given "to the technical and business infrastructure, and their interdependencies with [the] environment in which the applicant is operating."[127]

Further work around translating cybersecurity best practices into the language of insurance questionnaires is therefore necessary. At the same time, however, we need to be careful not to turn the entire cyber insurance underwriting process into a technical checklist-driven exercise based on a set

---

[124] *See* Romanosky et. al., *supra* note 33, at 8.

[125] The questionnaire is dated March, 2018 and is available with the author. A common exclusion in cyber insurance policies results from a failure to follow minimum required security practices, including "any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing." The case of Columbia Casualty Co. v. Cottage Health System, No. 16-56872 (9th Cir. Jan. 26, 2018) offers a good example. Cottage Health System suffered a data breach that resulted in the release of 32,500 private health-care patient records stored on network servers that Cottage owned and maintained. Columbia Casualty defended Cottage in a lawsuit brought by Cottage's patients, and after Columbia reached a settlement with the patients, Columbia filed a declaratory judgment action against Cottage, seeking reimbursement of the costs in defending the patients' lawsuit ($5,179,483 in settlement and defense costs). Columbia alleged that Cottage made misrepresentations and/or omissions of material fact concerning its data-breach risk controls when Cottage applied for the cyber policy. The application contained a "Risk Control Self Assessment" rubric which included a list of questions, four of which asked Cottage about checking security patches, replacing default settings, and other actions. The contract included a minimum required practices endorsement as a condition of coverage as well as continuous maintenance of all risk controls identified in the application. The case has since been voluntarily dismissed without a substantive decision on these issues, but it still highlights a common limitation on coverage. Some might see this case as a positive, as the exclusion incentivizes corporations to comply with basic cybersecurity policies so that they would not lose the coverage. Others might wonder how the insurer let the insured get to a point where basic security controls were not being followed.

[126] *See* Romanosky et. al., *supra* note 33, at 11–12.

[127] *Id*. at 12.

of compliance benchmarks.[128] Ari Waldman has shown how "privacy law [has failed] to deliver its promised protections in part because the responsibility for fulfilling legal obligations is being outsourced to layers of compliance professionals who see privacy law through a corporate, rather than substantive lens."[129] The concern is that a similar phenomenon of cybersecurity accreditation and compliance verification through third-party vendors is now emerging with the insurers pushing in the same direction.[130] As noted by Woods et. al., adopting a "check-box compliance view of network security" prevents accurate risk assessment, as it fails to take "a holistic and responsive view of risk management."[131] Such a process, if it becomes the underwriting norm, would not promote greater cybersecurity, and could undercut the social goals of increasing private market governance

---

[128] Cunningham & Talesh, *supra* note 29, at 425–26 (describing how insurers act as *de facto* compliance managers for organizations dealing with cyber security threats).

[129] Ari E. Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776 (2020), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6386&context=law_lawreview.

[130] Consider for example the evolving European Cybersecurity certification framework, which is being developed under the EU Cybersecurity Act. As described by the European Commission:

> The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. It will attest that ICT products and services which have been certified in accordance with such a scheme comply with specified requirements. In particular, each European scheme should specify: a) the categories of products and services covered, b) the cybersecurity requirements, for example by reference to standards or technical specifications, c) the type of evaluation (e.g. self-assessment or third party evaluation), and d) the intended level of assurance (e.g. basic, substantial and/or high). To express the cybersecurity risk, a certificate may refer to three assurance levels (basic, substantial, high) that are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. For example, a high assurance level means that the product that was certified has passed the highest security tests. The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

The EU Cybersecurity Certification Framework, THE EUROPEAN COMMISSION (Jun. 24, 2020), https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[131] Woods et. al, *supra* note 99, at 10 (internal quotation marks omitted).

of institutional cybersecurity designs.[132]

Finally, one needs to take into account aggregated risks from cyber catastrophes. As risks to data are by definition non-territorial,[133] they introduce an additional exposure point that is difficult to measure. The EastWest Institute identified two primary mechanisms through which "damage from an incident can cascade across systems."[134] These include common vulnerabilities (exploits, either patched or unpatched, that are present throughout a system that is in widespread use by multiple consumers, e.g. a vulnerability in Microsoft's operating system) and concentrated dependencies (widespread reliance on a single or few vendors for a critical platform or software, e.g., a major cloud service provider or common operating system).[135] As the report concludes:

> Due to the uncertainty around systemic cyber risk, it is possible that current premiums may not be adequate to cover losses in the event of a catastrophic scenario. Much of the data and modeling for cyber risks draws on past events (as is typical in many other sectors). However, because cyber risk is a rapidly evolving area, predicting loss scenarios on past performance creates uncertainty around the true risk exposure of the cyber insurance market.[136]

Responding to these informational gaps insurance companies and brokers have turned to analysis of big data to enhance their understanding of the market. "Through collecting and analyzing information on cyber breaches, including loss amounts and type of information lost, big data allow insurers to explore the scope of cyber events in a way not previously possible."[137] These insurers then contract with cybersecurity firms who employ "machine-learning algorithms and natural language processing algorithms" to produce company-specific and industry-specific predictive models and assessments.[138] But as Talesh and Cunningham show, the use of these tools

---

[132] In fact, some small-to-medium businesses are forced to choose between cyber insurance and information security services, given their limited financial resources. Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 379, 385 (2014). If the former provides less cybersecurity assurances than the latter, favoring it over the other, could in the long haul result in a lowering of our collective security.

[133] *See generally* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015).

[134] *See* Hake et. al., *supra* note 30, at 5.

[135] *Id*.

[136] MEHR & CAMMACK, *supra* note 28, at 11 ("The contributions of insurance to society are significant, although not without their costs. On balance, however, the gains outweigh the costs.").

[137] Talesh & Cunningham, *supra* note 108, at 997.

[138] *Id.* at 1002–03.

in the industry has proven "limited, inaccurate, and misleading."[139] This is because the tools depend on data which, for the most part, has proven unreliable and incomplete.[140]

Ultimately, all of the above listed challenges to cyber insurance underwriting are part of a security economics literature that is tested through empirical analysis of individual cyber insurance policies and processes.[141] At the same time, however, a different body of literature is missing. Such scholarship would seek to examine the insurability of cyber risk not from the perspective of economic efficiency alone, but rather while taking into account societal public policy needs. This paper proceeds to lay down such a framework and to apply it to four categories of cyber harm currently the subject of cyber insurance debates.

III. PUBLIC POLICY AND INSURABLE EXPOSURE

Insurance comes with various costs. D'Arcy calls this "the dark side of insurance," when the costs insurance creates to society, either directly or indirectly, get out of control.[142] It is in those moments that insurance regulation steps in. Often, the legal intervention is used to promote economic efficiency: reducing externalities, eliminating transactional costs, removing information asymmetries that trigger adverse selection, and ensuring competitive pricing. Cyber insurance scholars have already made proposals for legal interventions that focus on economic efficiency. In this spirit, for example, Kesan and Hayes suggested introducing governmental programs for information sharing of cyber insurance claims data while adopting legislation that could unify privacy and data protection regulations and cybersecurity standards.[143] Others have called to make cyber insurance compulsory for certain industries as a means for speeding-up the pace of market growth, diversification, and maturity.[144]

---

[139] *Id.* at 1019.
[140] *Id*.
[141] *See* Woods et. al, *supra* note 99, at 3 (drawing a distinction between two bodies of academic work. The first being a "stream of literature of the field of Security Economics" which focuses on the insurance market at large and its misplaced incentives and the second being "a multidisciplinary look at individual cyber insurance policies").
[142] Stephen P. D'Arcy, *The Dark Side of Insurance*, *in* INSURANCE, RISK MANAGEMENT AND PUBLIC POLICY 163, 178 (Gustavson and Harrington eds., 1994).
[143] *See, e.g.*, Kesan & Hayes, *supra* note 31, at 273–76 (discussing various government interventions either in mandating cyber-insurance coverage for certain industries, developing programs for information sharing, introducing tax credits for cybersecurity investment; subsidizing premiums; and adopting legislation that could uniform privacy and data protection regulation).
[144] *See, e.g.*, Jan Martinez Lemnitzer, *Why cybersecurity insurance should be regulated and*

But there is also a different kind of a legal intervention. This intervention might come at the expense of the particular business interests of individuals, favoring the promotion of certain societal values through rearranging, redistributing, and re-spreading risk.[145] A public policy approach to insurance law is one willing to make certain sacrifices around market freedom so to achieve other gains for society, all while recognizing that societal attitudes towards risk are dynamic and constantly shifting.[146] Adopting this approach invites the "intuitive pragmatist" administrator, adjudicator, and legislator to assess and prioritize values of liberty, utility, and equality pertaining to each risk and where necessary engage in limited interventions.[147]

While it is true that all law is shaped by some "intuitions of public policy,"[148] insurance law is unique given that at the heart of every insurance policy stands a contract. The ability of a commercial insurer and a policyholder to enter into a binding contract is limited by public policy as embodied in statutory, administrative, and common law.[149] As Kenneth

---

compulsory, J. CYBER POL'Y (Feb. 2021). Lance Bonner, Note, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 277 (2012) (proposing government intervention in the form of mandating contractors and sub-contractors working with federal and state government to acquire cyber insurance); Minhquang N. Trang, Note, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and, Mitigate Data Breaches*, 18 MINN. J.L. SCI. & TECH. 389, 425 (2017) (suggesting the implementation of a "mandatory cyber risk regime" that would protect "at-risk corporations and the public at large"); Angela Yu, Note, *Let's Get Physical Loss of Use of Tangible Property as Coverage in Cyber Insurance*, 40 RUTGERS COMPUTER & TECH L.J. 229, 253–54 (2014) (positing that the government may have a role in financially contributing to the current gaps in cyber-loss coverage, until the market is more sustained).

[145] *See* ABRAHAM, *supra* note 36, at 13–18.

[146] *Id.* at 29–31, 36.

[147] *Id.* at 18–20.

[148] OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1881).

[149] *James v. Fulcord*, 5 Tex. 512, 520 (1851) ("that contracts against public policy are void and will not be carried into effect by courts of justice are principles of law too well-established to require the support of authorities"); *see, e.g.,* RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981):

> § 178. When a Term is Unenforceable on Grounds of Public Policy
>
> (1) A promise or other term of an agreement is unenforceable on grounds of public policy if legislation provides that it is unenforceable or the interest in its enforcement is clearly outweighed in the circumstances by a public policy against the enforcement of such terms.
>
> (2) In weighing the interest in the enforcement of a term, account is taken of
>
> (a) the parties' justified expectations,
>
> (b) any forfeiture that would result if enforcement were denied,
>
> (c) any special public interest in the enforcement of the

Abraham and Schwarcz note, the public policy doctrine represents "judicial sensitivity to the difference between good and evil, fairness and unfairness, straight dealing and over-reaching. Even when all other tests for the validity of insurance policy provisions have been exhausted, this residual category of restrictions on what may or may not be included in a policy remains."[150]

In this regard public policy need not be seen as an "unruly horse,"[151] for more often it is tied to a chariot driven by the cautious pen of a regulator or the slow-moving gavel of established case law.[152] Public policy, in this regard, represents an external intervention which serves to realign the balance

---

particular term.

(3) In weighing a public policy against enforcement of a term, account is taken of

(a) the strength of that policy as manifested by legislation or judicial decisions,

(b) the likelihood that a refusal to enforce the term will further that policy,

(c) the seriousness of any misconduct involved and the extent to which it was deliberate, and

(d) the directness of the connection between the misconduct and the term.

Cf. David Adam Friedman, *Bringing Order to Contracts Against Public Policy*, 39 FLA. ST. U. L. REV. 563, 612–13 (2012) (noting that Section 178 of the Restatement is rarely employed by Courts, and instead of engaging in such "weighing" Courts prefer to rely on either law, regulation, or established case law to void a contract on grounds of public policy); *see also* Note, *A Law and Economics Look at Contracts Against Public Policy*, 119 HARV. L. REV. 1445 (2006) (providing a comprehensive survey of case law in contracts pertaining to the public policy defense); M. P. Furmston, *The Analysis of Illegal Contracts*, 16 U. TORONTO L.J. 267 (1966) (same).

[150] *See* KENNETH S. ABRAHAM & DANIEL SCHWARCZ, INSURANCE LAW AND REGULATION: CASES AND MATERIALS 98 (7th ed., 2020).

[151] *Richardson v. Mellish* (1924) 130 Eng. Rep. 294, 303 (Burrough J.) ("If it be illegal, it must be illegal either on the ground that it is against public policy, or against some particular law. I, for one, protest . . . against arguing too strongly upon public policy; it is a very unruly horse, and when once you get astride it you never know where it will carry you. It may lead you from the sound law. It is never argued at all but when other points fail.") Winfield colorfully referred back to the metaphor of a horse reviewing law reports on the Public Policy doctrine: "at times the horse has looked like even less accommodating animals. Some judges appear to have thought it more like a tiger, and have refused to mount it at all, perhaps because they feared the fate of the young lady of Riga. Others have regarded it like Balaam's ass which would carry its rider nowhere. But none . . . has looked upon it as a Pegasus that might soar beyond the momentary needs of the community." (Percy H. Winfield, *Public Policy in the English Common Law*, 42 HARV. L. REV. 76, 91 (1928)).

[152] Friedman, *supra* note 149, at 620 ("I contend that the horse today is not "very unruly"—that discernable patterns emerge in looking at the common run of cases . . . . A systematic look at judicial opinions involving the public policy defense… can shed different light on the public policy defense and narrow the areas of unruliness.").

between "efficiency" and "fairness."[153] We shouldn't fear the introduction of public policy. Rather we should fear a private insurance market that may stifle public debate and endanger societal security due to collective action problems. Especially where social benefits do not translate in terms of private profitability, a public entity could guide private operators beyond business model responses and towards the promotion of a public good.[154]

This is particularly true in the context of cybersecurity, where the continued evolution of policy is dependent on effective public-private partnerships (PPPs) and on the realization that no single actor can figure it out alone.[155] The public sector has certain strengths in dealing with the national security threat posed by cybercrime and cyberconflict. Government agencies are better positioned to collect foreign intelligence and collaborate with other national and international actors in investigating and circumventing potential cyber threats and in developing a holistic view around management of cyber risk.[156] These capabilities and the knowledge base complement the specific expertise and experiences that the private industries and markets bring to the table.[157] Businesses and industries should thus be working with the state, not in isolation from it, recognizing that their corporate decision-making is umbilically tied to all of our collective security.

The Intelligence and National Security Alliance (INSA), an Arlington-

---

[153] See generally, Ronen Avraham, Kyle D. Logue & Daniel Schwarcz, *Understanding Insurance Antidiscrimination Laws*, 87 S. CAL. L. REV. 195, 201–02 (2014).

[154] *See* Madeline Carr, *Public-Private Partnerships in National Cyber-Security Strategies*, 92(1) INT'L AFF. 43, 56–57 (2016).

[155] *See* Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, N.Y.U. CTR. ON L. AND SEC., 1–2 (2014), http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf. Indeed, the NIST framework discussed above in *supra* note 98, was the result of the Cybersecurity Enhancement Act of 2014 which directed NIST to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure." *See* Cybersecurity Enhancement Act of 2014, § 101, Pub. L. No. 113-274, 128 Stat. 2971 (2014). This law is an often-cited example of an effective public-private partnership.

[156] *See* Arnav Jagasia, *A Look Into Public Private Partnerships for Cybersecurity*, WHARTON PUBLIC POLICY INITIATIVE (Apr. 18, 2017), https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for#_edn5; s*ee also Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*, INTELLIGENCE AND NATIONAL SECURITY ALLIANCE 6 (Nov. 2009), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_AddressingCyber_WP.pdf [hereinafter *INSA Report*].

[157] Stephen H. Linder, *Coming to Terms With the Public-Private Partnership: A Gramma r of Multiple Meanings*, 43 AM. BEHAVIORAL SCIENTIST 35, 47 (noting that in most instances of PPP "each party brings something of value to the others to be invested or exchanged," and suggesting further that "there is an expectation of give-and-take between the partners, negotiating differences that were otherwise litigated").

based not-for-profit professional organization bringing together public and private members of the U.S. intelligence community, has identified three goals for an effective cybersecurity PPP. First, the partnership must "define, identify, and watch for behaviors of concern;" second, it must ensure "compliance with the partnership's security standards, sanctioning those who fail to comply;" and finally, it must provide means to "conduct forensic examinations following disruptions, analyze vulnerabilities, fix security shortcomings and effectively attribute attacks to their perpetrators."[158]

These three goals should also guide any public policy intervention into the cyber insurance market. Regulators and insurers should work together to identify "behaviors of concern" in the cyber insurance market, develop security standards and ensure that the market incentivizes compliance with them, and collaborate around the prevention of cybercrime and the enforcement of cyber norms.

In *Ethics, Morality, and Insurance*, John D. Long introduced nine "ethical pillars," which he understood as "generally acceptable behavioral standards which are conducive to the long-range availability and use of insurance."[159] Long summarized these pillars in the following grandiose way:

> Insurance presupposes a yearning for *achievement*, a drive of *acquisitiveness*, a desire to *preserve* what is valuable, a bit of *apprehension* about the future, a readiness to *obey* the law, a sense of *honesty*, a fondness for *tradition*, a willingness to accept *personal responsibility* and accountability, and a measure of *charity* towards others in society.[160]

For Long, an *achievement* and *acquisition* orientation to insurance law was required and centered around the freedom of the insurer and the insured to redistribute resources and to accumulate wealth.[161] At the same time, however, Long recognized the limits to such an orientation, acknowledging that where crime or tort is committed, or where acquisition of wealth reaches some "extreme magnitude," redistribution should not be welcomed.[162] Moreover, to avoid moral hazard, insurers must ensure that their policy holders remain apprehensive and concerned about the future and about their personal responsibilities in relation to it.[163]

Insurance further requires "a certain orderliness in human affairs,"

---

[158] *INSA Report*, *supra* note 156, at 8.
[159] JOHN D. LONG, ETHICS, MORALITY, AND INSURANCE: A LONG-RANGE OUTLOOK, 26 n.9 (1971).
[160] *Id*. at 43 (emphasis added).
[161] *Id*. at 26–29.
[162] *Id*. at 27–29.
[163] *Id*. at 31–32, 38–39.

particularly the establishment of laws that minimize long-run loss and adverse selection while increasing good faith and good measures.[164] Some insurance types involve legal infractions (e.g., insurance for identity theft, cyber terrorism, or ransomware), but "the domain of insurability is narrow."[165] As the probability of illegal action increases over a certain period, insurance becomes less and less "appropriate as a loss-sharing device until the point is reached where it is altogether useless."[166] Achieving a desirable societal level of cyber norms enforcement is thus pivotal for maintaining a functioning insurance market.

None of Long's pillars is a *sine qua non* for a functioning insurance system. Rather, all nine pillars should be examined together on a sliding scale. Doing violence to one or multiple of the pillars does not make the insured subject uninsurable. Rather "some deviation is inevitable, but the insuring process can absorb it only as long as it occurs infrequently."[167] Those transactions would remain "within the pale of insurance," until such time as the aberration becomes the norm, at which point the process will disintegrate.[168]

Long devoted a chapter of his book to issues of emerging technology.[169] Writing in 1971, he played the role of an oracle, examining how these nine ethical pillars could help guide the insurance process in the future as it is faced with new dimensions in scientific and technological development.[170] Long particularly focused on what he called the "concept of cybernetics," which today we know as "artificial intelligence."[171] In so doing, Long foresaw the vibrant debate that has since emerged in academic writing around liability and insurance structures for autonomous vehicles, killer robots, and other technologies engaging in algorithmic decision-making and machine learning.[172] To be sure, this paper is centered around cybersecurity risks and

---

[164] *Id*. at 34–37.
[165] *Id*.
[166] *Id*.
[167] *Id*. at 42.
[168] *Id*. at 30–31 (suggesting further that "quantification of the maximum tolerable division is probably impossible except with the use of overly simplified assumptions.").
[169] *Id.*
[170] *Id*. at 199–237.
[171] *Id*. at 229 (describing a cybernetic system as one capable not only of performing tasks, "but also of learning how to improve its performance on the basis of its earlier mistakes or how to alter its performance as necessitated by change in its environment").
[172] *See, e.g.,* David C. Vladeck, *Machine without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 146–47 (2014); Bryan Casey, *Robot Ipsa Loquitur*, 108 GEO. L.J. 225 (2019); Omri Rachum-Twaig, *Whose Robot is it Anyway?: Liability of Artificial-Intelligence-Based Robots*, 2020 U. ILL. L. REV. 1140 (2020); Carrie Schroll, *Splitting the Bill: Creating a National Car Insurance Fund to Pay for Accidents in Autonomous Vehicles*, 109 NW. U. L. REV. 803 (2015); Curtis E.A. Karnow, *Liability for*

not those unique risks introduced by agents of artificial intelligence.[173] Nonetheless, Long's ethical pillars—which he developed himself to examine the intersection of insurance and technology—are useful to determine as a matter of *lex ferenda* how the cyber insurance process could evolve to take into account more public policy considerations.

Legal intervention is necessary, under Long's ethical pillars, as a check on destructive market behavior and as a means for preserving certain societal values at the expense of individual profit-amassing desires.[174] These destructive market behaviors manifest themselves in the cyber insurance market and therefore justify potential intervention. Indeed, as Knutsen and Stempel write: "[u]sing insurance as an incentive for good cyber-loss risk management produces some questionable results and places a great deal of influence and responsibility on an industry whose incentives are about

---

Distributed Artificial Intelligences, 11 BERKELEY TECH. L.J. 147 (1996); Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 VA. L. REV. 127 (2019); James M. Anderson et. al., *Rethinking Insurance and Liability in the Transformative Age of Autonomous Vehicles*, RAND CORPORATION (2018), https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF383/RAND_CF383.pdf; Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CALIF. L. REV. 1611 (2017); Elizabeth Fuzaylova, *War Torts, Autonomous Weapon Systems, and Liability: Why a Limited Strict Liability Tort Regime Should Be Implemented*, 40 CARDOZO L. REV. 1327 (2019); Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016).

[173] This distinction is not so clear cut. The introduction of an autonomous system or of algorithms into a field of practice (such as in medicine, justice, or hospitality) opens the door to a whole menu of risks and potential harms. Some of these risks, for example a biased decision-making process will be outside the scope of a traditional cyber insurance policy. *See, e.g*., Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023 (2017) For example, if my doctor was replaced by a robot, and that robot made an error in judgment, such a hypothetical will be examined through the lenses of a malpractice suit covered by professional liability insurance. On the other hand, the introduction of an autonomous or otherwise "smart" device opens the door for hackability. Consider in this regard the Fiat Chrysler hacking case before District Court for the Southern District of Illinois. *Flynn v. FCA U.S. LLC*, No. 15-cv-00855-SMY-RJD, 2020 WL 1492687 (S.D. Ill. 2020). The owners in each class allege that they overpaid for vehicles because the infotainment systems installed in the cars were vulnerable to hacking. Ord. Granting in Part and Denying in Part Defendants' Motions for Summary Judgment and Plaintiffs' Motion to Certify Class at 214–15, Flynn v. FCA U.S. LLC, 327 F.R.D. 206 (S.D. Ill. 2018). The District Court certified in July 2018 three classes of Dodge, Jeep, and Chrysler owners. Id. at 227.In so doing, the court agreed that there were enough facts to support consumers' fraud and warranty claims. *See* generally id. For the purposes of our analysis, it matters not if the cars in question are autonomous vehicles or merely "smart" cars capable of internet connectivity (the cars were in fact of the latter category). What matters is that the hackability opened the door for a liability suit which could be covered by a standalone cyber insurance product.

[174] LONG, *supra* note 159.

controlling underlying financial risk to themselves, not necessarily buttressing the societal interests of loss prevention beyond the insurable sphere of a particular insurance policy."[175]

IV. THE CASE FOR LEGAL INTERVENTIONS FOR INSURING CYBER RISK

A. Indemnification for Cyber Terrorism and State-Sponsored Cyberattacks

1. The Risk of Cyber Terrorism and State-Sponsored Attacks

On January 29, 2019, Director of National Intelligence Daniel Coats presented to the Senate Select Committee on Intelligence the intelligence community's "Worldwide Threat Assessment."[176] In his report, Coats noted that "growing availability and use of publicly and commercially available cyber tools" increases the possibility for terrorist organizations to cause significant remote harms to the United States.[177] Identifying cyber terrorism as one of the biggest threats to the U.S. homeland, he concluded that "terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects by defacing websites or executing denial-of-service attacks against poorly protected networks—with little to no warning."[178]

The analysis Coats provided focused mostly on "enabling" and "disruptive" cyber terrorist operations. In so doing, he avoided a third category of cyber capabilities—"destructive" operations which involve cyberattacks that achieve kinetic effects, direct or indirect physical damage, injury, or death.[179] Indeed, while almost "all terrorist organisations operating

---

[175] JEFFREY W. STEMPEL & ERIK S. KNUTSEN, STEMPEL AND KNUTSEN ON INSURANCE COVERAGE 680 (4th ed. 2020).

[176] *Worldwide Threat Assessment of the US Intelligence Community Hearing Before the S. Comm. on Intelligence*, 116th Cong. 1, at 6 (2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (statement for the record of Daniel R. Coats, Director, Office of the Director of National Intelligence).

[177] *Id*. at 7.

[178] *Id*. at 6.

[179] The Cambridge Centre for Risk Studies distinguishes between "enabling" cyber operations (online activities supporting terrorist organizations' operations, such as publicity, propaganda and recruitment), "disruptive" cyber operations (online activities that disrupt information technology systems, including breach of networks, exfiltration of digital information, and denial of service attacks (DDoS)), and "destructive operations. For further reading, *see* TAMARA EVAN ET. AL., CYBER TERRORISM: ASSESSMENT OF THE THREAT TO INSURANCE 13 (Tamara Evan ed. 2017).

today exhibit 'enabling' cyber capability," they have so far "failed to demonstrate advanced skills in 'disruptive' capabilities and may be some way short of the skills required for 'destructive' capability."[180]

The closest example of a successful cyber terrorism operation against the U.S. involved a 2015 minor hack by Junaid Hussain and the Islamic State's Hacking Division, the CyberCaliphate.[181] In this operation, the hackers managed to take control over U.S. Central Command's YouTube and Twitter accounts.[182] The hackers used the accounts to post taunting propaganda, including "kill lists" of the names and addresses of serving military personnel, exhorting followers to attack them physically.[183] Other ISIS attacks have similarly been of minor strategic importance—the defacement of Croatia's NATO website, breaching a server of the United Nations Development Programme (UNDP), and a phone-based denial-of-service attack against the U.K.'s Counterterrorism Command hotline.[184]

It is true that policy discourse around cyber threats is dominated by "alarmist rhetoric" that is unhelpful at times and potentially even dangerous.[185] Nonetheless, these minor cyber terrorist operations demonstrate ISIS and other terrorist organizations' appetite for carrying out

---

[180] *Id.* at 6 ("The key conclusion of this report is that, while various types of cyber attack are becoming more commonplace, the most relevant cyber terrorist actors currently pose a low likelihood of inflicting severe physical destruction through digital means before 2020. At present, the major terrorist groups posing a threat to the West are motivated by mass casualty attacks; the cyber tools available to these actors currently provide far less chance of major injury than a traditional explosive, knife or vehicle attack.").

[181] *See* John P. Carlin*, Inside the Hunt for the World's Most Dangerous Terrorist,* POLITICO (Nov. 21, 2018), https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643.

[182] Elliot C. McLaughlin, *ISIS Jihadi Linked to Garland Attack Has Long History as Hacker*, CNN (May 7, 2015), https://www.cnn.com/2015/05/06/us/who-is-junaid-hussain-garland-texas-attack/index.html. For profiles of Junaid Hussain, *see id*.; Carlin, *supra* note 181. Hussain was the founding member of an English-language online recruitment collective dubbed by the FBI as "The Legion" or "Raqqa 12." *See* Nafees Hamid, *The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain*, 11 CTC SENTINEL 30, 34 (2018) ("Other notable members included fellow British nationals Reyaad Khan from Cardiff, Raphael Hostey from Manchester, as well as the Australian Neil Prakash. Together, this band of propagandists reached thousands of English speakers around the world through their public posts and attempts to groom and inspire potential attackers via one-on-one online contact."). From within ISIS territory, he would use various social media tools and mobile apps to communicate with likely recruits. *Id.* at 34. On August 24, 2015, Hussain was killed near Raqqa in a U.S. drone strike. *Id.* at 35. Junaid Hussain was considered the head of the Islamic State Hacking Division (ISHD). *Id.*

[183] COBURN ET. AL., *supra* note 25, at 136–37.

[184] *See* Hamid, supra note 182, at 32.

[185] Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 84 (2011).

such attacks. The likelihood of an attack from both lone-wolf radicalized cyber operations and more advanced organizational affronts, including destructive cyber operations, is only likely to increase in parallel with the spread of vulnerabilities embedded within the devices that help run our digital economies, political systems, and social networks.[186]

While the threat of cyber terrorism has yet to fully materialize, state-sponsored cyberattacks are now a common phenomenon. The Digital and Cyberspace Policy program at the Council on Foreign Relations has aggregated 324 publicly available examples of state-attributed cyber incidents since 2005.[187] Nearly one third of these attacks (105) targeted private sector entities, and nearly all caused significant economic losses.[188] These attacks were committed either directly by national cyber and intelligence agencies or, more often, indirectly by hacking groups operating under the direction and control of their foreign sovereign handlers. These state-sponsored attackers are considered Advanced Persistent Threats (APTs) given the immense capabilities and budgets in their possession.[189] APTs use two specific techniques that make their cyberattacks more likely to cause large-scale significant losses:

First, states rely on software security flaws that have yet to be patched. These "zero-day" vulnerabilities pose the risk for systemic and aggregated harms, especially where the vulnerable software is used by a large number of consumers or by a dominant vendor or provider.[190] Because of their unlimited

---

[186] COBURN ET. AL., *supra* note 25, at 138–39 ("As militant jihadists become more accomplished, it is likely that they will use cyber means to augment and enhance their physical attacks . . . Spectacular and deadly cyber attacks may be an aspiration of these groups, and it is important to monitor any improvements in capability of these threat actors . . . .").

[187] *Cyber Operations Tracker*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/cyber-operations/ (last visited Aug. 20, 2019).

[188] *Id*. (examples of state-sponsored attacks on private entities include the 2018 hacking of German energy firms (attributed to Russia), the 2016 and 2017 attempts to steal nearly a billion dollars from banks via compromise the SWIFT inter-banking network (attributed to North Korea), the 2015 and 2016 disruptions to Ukrainian power grids (the first suspected large-scale power outages enabled by a cyberattack, attributed to Russia), the 2014 to 2017 Cloud Hopper operation targeting intellectual property from aerospace, engineering, energy, pharmaceuticals and telecommunications firms (attributed to China), and the 2014 targeting of AMC Theaters and Sony Pictures (attributed to North Korea)).

[189] COBURN ET. AL., *supra* note 25, at 139–140.

[190] Hake et. al., *supra* note 30, at 20–22 (citing as examples of such zero-day vulnerabilities the EternalBlue exploit which targeted a Windows vulnerability and was used in the NotPetya attack, as well as the Heartbleed, Meltdown and Spectre vulnerabilities). *See also* LLOYDS REPORT, *supra* note 62, at 34–35 (Lloyds further suggests that the average zero-day exploit lasts 6.9 years in the "wild." Once identified it takes an average of 22 days to develop an exploit, "which contrasts unfavourably with the estimated average of 100–245 days needed to remediate the vulnerability." As Lloyds concludes, "even if a company is diligent

resources, APTs have the means to either self-engineer or purchase this dangerous cyber weaponry from the black markets.[191] When they are not relying on malicious software, APTs use "Living Off the Land" (LotL) tactics. LotL attacks, also known as "Fileless" attacks, "exploit[ing] legitimate and trusted tools or applications in a computer to gain entry into a system, cutting out the need to execute malicious files to launch an attack."[192] By engaging in these LotL attacks APTs may "elude traditional detection techniques such as antivirus software, as there is no payload to trigger the malware signature. Fileless malware increases the rate of successful infection and anonymity of the group, reducing the risk of legal action against the actors and raising threats to corporations across sector and size."[193]

2. Common Exclusions and the Cyber Insurance Coverage Gap

Both state-sponsored attacks and cyber terrorism are currently under-insured.[194] This is owed to specific exclusionary language common to insurance policies.[195] As has already been highlighted in the *Mondelez* example, policies are often subject to language excluding "warlike" sovereign acts. The U.S. Court of Appeals for the Second Circuit interpreted this historical exclusion in its 1974 decision in the *Pan Am Flight 83* case. The Pan Am flight was hijacked over London in September 1970 by the Popular Front for the Liberation of Palestine. After landing the plane in Cairo, and not before letting all the passengers depart, the hijackers exploded the Boeing 474 jumbo jet in retaliation for U.S. support of Israel.[196] Relying on its all-risk aviation policy, Pan Am sought coverage from its insurer, Aetna. Litigation soon followed, as Aetna sought to exclude coverage on the basis of a war exclusion clause found in the policy.

The Second Circuit, citing the international law writings of ICJ judge

---

in its patching, the frequency of these events means that the overwhelming likelihood is that malicious actors will make their way into a network if determined to do so.").

[191] ANDREW COBURN ET. AL., CTR FOR RISK STUDIES, UNIV. OF CAMBRIDGE JUDGE BUS. SCHOOL, CYBER RISK OUTLOOK 9 (2019).

[192] *Id.* at 10 (noting that "between January and July of 2018, LotL attacks were estimated to have increased by 94%.").

[193] *Id*.

[194] *See* Romanosky et. al., *supra* note 33; *see also supra* text accompanying note 84. *See also* Michelle E. Boardman, *Known Unknowns: The Illusion of Terrorism Insurance*, 93 GEORGETOWN L. J. 783, 796–98 (2005).

[195] *See* NAIC Cybersecurity Insurance Report, *supra* note 79; OECD, *supra* note 80.

[196] Raymond H. Anderson, *Hijackers in Cairo Say They Blew Up 747 in Retaliation for. U.S. Support of Israel*, N.Y. TIMES (Sept. 8, 1970), https://www.nytimes.com/1970/09/08/archives/hijackers-in-cairo-say-they-blew-up-747-in-retaliation-for-us.html.

Hersch Lauterpacht, concluded that "war is a course of hostility engaged in by entities that have at least significant attributes of sovereignty."[197] The hijackers, however, "were the agents of a radical political group," not a sovereign government.[198] The Court thus decided that the exclusions did not apply because the hijackers' acts were criminal rather than military. The Court bolstered its finding of a narrow interpretation of the war exclusion by referring back to the district court's reasoning:

> There is no warrant in the general understanding of English, in history, or in precedent for reading the phrase "warlike operations" to encompass (1) the infliction of intentional violence by political groups (neither employed by nor representing governments) (2) upon civilian citizens of non-belligerent powers and their property (3) at places far removed from the locale or the subject of any warfare. (4) This conclusion is merely reinforced when the evident and avowed purpose of the destructive action is not coercion or conquest in any sense, but the striking of spectacular blows for propaganda effects.[199]

The war exclusion and the *Pan Am Flight* case predate the cyber era. Whether or not the Illinois court in the *Mondelez* case will continue to adopt such "a narrow reading"[200] of what constitutes "war" in cyberspace, will involve a factually intensive analysis of the NotPetya attack. The Court will rest its reasoning on both its understanding of the parties' intentions and the unique features of interstate cyber operations as exemplified in NotPetya. The burden will be on Zurich to show that the exclusion applies, given that ambiguous terms in an insurance policy are construed strictly against the insurer and in favor of coverage.[201]

In *Mondelez* we seem to have spillover collateral damage resulting from a cyber campaign launched by Russia against the Ukraine. At first blush this would seem to meet the requirements laid out in *Pan Am*. Nonetheless, Zurich is likely to face a number of hurdles in establishing its argument in favor of

---

[197] Pan American World Airways, Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989, 1012 (2d Cir. 1974).
[198] *Id*. at 1015.
[199] *Id.* at 1015–16 (quoting Pan American World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp. 1098, 1130 (S.D.N.Y. 1973)).
[200] In re Sept. 11 Litig., 751 F.3d 86, 92–93 (2d Cir. 2014) (stating that such "a narrow reading" achieves "the parties' contractual intent, insulating the policyholder from loss."). *See also* Holiday Inns Inc. v. Aetna Ins. Co., 571 F. Supp. 1460, 1463 (S.D.N.Y. 1983) (adopting a similar narrow interpretation).
[201] *See, e.g.*, Outboard Marine Corp. v. Liberty Mutual Ins. Co., 607 N.E.2d 1204, 1217 (Ill. 1992). This is especially true for exclusionary clauses which must be clear and free from doubt if they are to be used to deny coverage.

an exclusion. First, according to the Tallinn Manual, the most robust academic study of international law in cyberspace,[202] there are "significant legal and practical challenges stand[ing] in the way of definitively concluding that a cyber operation has initiated an international armed conflict. To date, no international armed conflict has been publicly characteri[z]ed as having been solely precipitated in cyberspace."[203] The bar thus seems to be set high for insurers to distinguish between covered criminal activity and excluded armed hostile military operations. Most cyber operations, even ones that caused significant economic losses, would simply not rise to the level of triggering a war from an international legal perspective.[204]

Moreover, in order to prove the existence of a warlike act, Zurich would need to establish that NotPetya originated from a sovereign power. It will have to show how Russia's responsibility for the attack is more likely than not under a "preponderance of the evidence" standard.[205] Zurich would therefore be forced to rely on the public declarations of attribution made by western intelligence agencies, who themselves are unlikely to be compelled to further testify on those declarations.[206] It remains to be seen whether the court in Illinois would be satisfied with such uncorroborated statements. If not, Zurich would have to provide complex expert opinion and forensic analysis to be able to support its claims for attribution. As the literature indicates, however, cyber attribution is hindered by both technological limitations (due to the use of technology that obscures the identity of the perpetrators) and legal constraints (which demand the showing of effective

---

[202] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) (produced by a group of international experts on behalf of the NATO Cooperative Cyber Defence Centre of Excellence proposing rules to govern). *But see* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L. L. 583 (2018) (critiquing the manual).

[203] TALLINN MANUAL 2.0, *supra* note 202, at 384.

[204] One might try to color the events in the Crimea and Eastern Ukraine beginning in 2014 as triggering an armed conflict, either international or non-international, that is ongoing to this date. There would be legal and factual challenges under international humanitarian law in establishing such an argument. *See generally* Agnieszka Szpak, *Legal classification of the armed conflict in Ukraine in light of international humanitarian law*, 58 HUNGARIAN J. LEGAL STUD. 261 (2017). Even if there was an ongoing armed conflict, whether a set of cyber operations conducted outside the theater of war and zone of conflict should be deemed associated with that war, is a matter for legal interpretation.

[205] *See* Ferland, *supra* note 22, at 371 (citing to the Illinois Supreme Court Committee on Pattern Jury Instructions in Civil Cases (eds.), *Illinois Pattern Jury Instructions: Civil, §21.01*, Illinois Courts (last visited Mar. 7, 2021), www.state.il.us/court/CircuitCourt/CivilJuryInstructions/21.00.pdf, to suggest that this evidentiary standard will bind in the context of a civil trial under an insurance contract).

[206] *See generally* Stilgherrian*, supra* note 11 (observing that norms regarding attribution and responses have been minimal in the past).

or overall control by the nation-state on each of the operations committed by the hacking group).[207] Intelligence agencies are thus one of only a few actors with the capacity to conduct cyber attribution effectively, because they may rely on expansive resources and intimate access into the perpetrator state to reach these conclusions.

In light of the legal difficulties in establishing the war exclusion, stand-alone cyber insurance policies have now moved to introduce additional specialized exclusionary language. For example, some insurers exclude attacks committed by a "government entity or public authority" (a sovereign act exclusion).[208] In so doing, the insurer avoids the need to prove the existence of a state of war under the stringent requirements laid down in the *Pan Am* case and customary international law. Nonetheless, the insurer will still face the challenges of attribution, proving that the attack was made by an entity of the government. Carriers further seek to exclude expanses from acts of cyber terrorism. Given that both domestic and international law lack a uniform definition of terrorism[209] (let alone cyber terrorism[210]), these carriers struggle to develop uniform language to describe such operations.[211]

---

[207] For a further discussion see William C. Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AM. J. INT'L. L. UNBOUND 191 (2019); Berenice Boutin, *Shared Responsibility for Cyber Operations*, 113 AM. J. INT'L. L. UNBOUND 197 (2019); Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks*, 113 AM. J. INT'L. L. UNBOUND 202 (2019); Chimène I. Keitner, *Attribution by Indictment*, 113 AM. J. INT'L. L. UNBOUND 207 (2019); Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AM. J. INT'L. L. UNBOUND 213 (2019).

[208] The policy is dated March, 2018 and is available with the author.

[209] *See* Sudha Setty, *What's in a Name? - How Nations Define Terrorism Ten Years After 9/11*, 33(1) U. PA. J. INT'L. L. 1 (2011) (concluding that "[s]ince neither international norms nor domestic courts provide a significant check against creeping definitions, legislatures must take proactive steps to combat potential overreaching in applying the label of terrorism.").

[210] *See* Sarah Gordon & Richard Ford, *Cyberterrorism?*, 21 COMP. & SEC. 636 (noting that the term cyberterrorism "is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyberterrorism.").

[211] One carrier for example excluded losses from computer failures that directly resulted from an "act of terrorism," which the policy defines as "an act, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of, or in connection with any organization(s) or government(s), committed for political, religious, ideological, or similar purposes including the intention to influence any government and/or put the public, or any section of the public, in fear." *Cyber Security Liability Coverage Form*, PHILADELPHIA INDEMNITY INSURANCE COMPANY (AUG. 2012),
https://www.phly.com/Files/Cyber%20Security%20Liability%20Policy%20Form36-8835.pdf. *Cf. definition* provided in a different policy that specifically excludes cyber terrorism, defined as: "the premeditated use of disruptive activities against any Company's Computer System or network, or the explicit threat to use such activities, with the intention

Both the sovereign act and the cyber terrorism exclusions serve the same purpose that the traditional war exclusion once served: "to prevent insurers from being wiped out by correlated claims . . . that inflict abnormal losses throughout society."[212] While it is true that some (perhaps even many) of the cyber terrorist and state-sponsored attacks occurring today would prove to be non-catastrophic, the mere possibility of a mega-catastrophe resulting from these attacks, is enough to push insurers either to exclude coverage altogether or to limit it significantly with harsh sub-limits and high deductibles. The insures' logic is understandable. If we already believe that terrorism and war-like risks pose a degree of uncertainty that makes them unmanageable,[213] then adding a complexity through a cyber extension of the risk only intensifies the actuarial challenge, further decreasing insurers' appetite. The result is an underinsured major risk that is further subject to ever evolving and confusing exclusionary language across policies.

3. The Parallel to Terrorism Policies and Government Backstops

Following the devastating effects of 9/11, reinsurers attempted to pull out of the terrorism insurance market. "Estimates of insured losses from the 9/11 attacks are more than $45 billion in current dollars, the largest insured losses from a non[-]natural disaster on record. These losses were concentrated in business interruption insurance (34% of the losses), property insurance (30%), and liability insurance (23%)."[214] With such a large hit to their reserves, insurers opted to reduce the number of policies they sold and the amounts those policies covered. The initial panic following 9/11 led many reinsurers to believe that terrorist attacks were "actuarially intractable" and "could not be reliably calculated."[215] Once reinsurers stopped offering coverage, primary insurers, worried about their own lack of sufficient data and models, also sought to withdraw from the market. As a result, at-risk commercial entities were left with an uninsurable risk at a time where it seemed as if they needed an insurance policy the most.

---

to cause harm and further social, ideological, religious, political, or similar objectives, or to intimidate any person(s) in furtherance of such objectives." (Policy dated March, 2018, available with the author).

[212] Jeffrey W. Stempel, *The Insurance Aftermath of September 11: Myriad Claims, Multiple Lines, Arguments over Occurrence Counting, War Risk Exclusions, the Future of Terrorism Coverage, and New Issues of Government Role*, 37 TORT & INS. L.J. 817, 852 (2002).

[213] *See* Boardman, *supra* note 194, at 823 ("Taken together, the extreme difficulty in calculating the terrorism risk, and the high cost of the risk's structure make it both uninsurable and unprofitable. . . . [G]overnment subsidy can solve unprofitability, but nothing short of time can hope to solve the insurability problem.").

[214] WEBEL, *supra* note 83, at 1.

[215] Boardman, *supra* note 194, at 800.

Reacting to these developments, in November 2002 Congress passed the Terrorism Risk Insurance Act (TRIA).[216] TRIA requires insurers to offer certain types of coverage for losses caused by an event that the U.S. government has officially designated as terrorism. If losses from an attack exceed a set amount, a federal backstop kicks in to offset insurers' payouts.[217] The program was amended and extended in 2005, 2007, and most recently in 2015.[218] The program is now set to expire at the end of 2020. According to a recent study by the Congressional Research Center, as a result of TRIA insurers are more capable of bearing terrorism risk and are underwriting under its shadow.[219] Indeed 80% of all stand-alone terrorism policies written

---

[216] Terrorism Risk Insurance Act, Pub. L. No. 107-297, 116 Stat. 2322 (2002).

[217] The criteria set under TRIA is as follows:

> "1. An individual act of terrorism must be certified by the Secretary of the Treasury, in consultation with the Secretary of Homeland Security and Attorney General; losses must exceed $5 million in the United States or to U.S. air carriers or sea vessels for an act of terrorism to be certified;
> 2. The federal government shares in an insurer's losses due to a certified act of terrorism only if "the aggregate industry insured losses resulting from such certified act of terrorism" exceed $180 million (increasing to $200 million in 2020);
> 3. The federal program covers only commercial property and casualty insurance, and it excludes by statute several specific lines of insurance;
> 4. Each insurer is responsible for paying a deductible before receiving federal coverage. An insurer's deductible is proportionate to its size, equaling 20% of an insurer's annual direct earned premiums for the commercial property and casualty lines of insurance specified in TRIA;
> 5. Once the $180 million aggregate loss threshold and 20% deductible are met, the federal government would cover 81% of each insurer's losses above its deductible until the amount of losses totals $100 billion;
> 6. After $100 billion in aggregate losses, there is no federal government coverage and no requirement that insurers provide coverage;
> 7. In the years following the federal sharing of insurer losses, but prior to September 30, 2024, the Secretary of the Treasury is required to establish surcharges on TRIA-eligible property and casualty insurance policies to recoup 140% of some or all of the outlays to insurers under the program. If losses are high, the Secretary has the authority to assess surcharges, but is not required to do so."

WEBEL, *supra* note 83, at 3–4. Note that terrorist acts would not be covered in the event of a state of war, except for workers' compensation insurance.

[218] Terrorism Risk Insurance Extension Act Pub. L. No. 109-144, 119 Stat. 2660 (2005); Terrorism Risk Insurance Program Reauthorization Act, Pub. L. No. 110-160, 121 Stat. 1839 (2007); Terrorism Risk Insurance Program Reauthorization Act, Pub. L. No. 114-1, 129 Stat. 3 (2015).

[219] *See* WEBEL, *supra* note 83, at 12 (noting that "combined policyholder surplus among all U.S. property and casualty insurers was $686.9 billion at the end of 2017 compared to $408.6 billion (inflation adjusted) at the start of 2002. This $686.9 billion has been bolstered by the

in 2017 were TRIA-eligible.[220] Moreover, 80% of all the Commercial Multi-Peril (CMP) and Property/Casualty (P&C) policies now embed terrorism coverage. Nearly 30% of those policies don't charge any additional premiums for the added terrorism risk, while others charge only marginal and competitive premiums.[221] Given this data, some scholars believe that if the program is not extended, "the insurance industry will be unwilling to continue to cover terrorism risk at current levels,"[222] slowly reverting back to its post-9/11 stance.

Others have challenged the usefulness of TRIA. These scholars have argued that "terrorism risk is not more severe than other insurable risks such as natural catastrophes, and a federal backstop stakes public money to protect the insurance industry, and subsidize the terrorism risk insurance premiums for commercial policyholders."[223] They also have argued that TRIA obviates the need for insurers to calculate the risk, underwrite for the risk, and plan ahead by setting aside in reserve the amounts needed to meet all expected losses.[224] As summarized by Boardman:

> If insurers had a better idea than others where and how the risk would next materialize, terrorism insurance could serve a public function. Accurate premium information and proven insurer safety requirements could provide incentives, if such information existed. For now, unfortunately, the private insurance market does not provide a benefit the government cannot. Moreover, the government insurance program raises a greater threat of moral hazard than would a government post-disaster aid program.[225]

It is true that federal reinsurance programs present certain problems.

---

estimated $38 billion in premiums paid for terrorism coverage over the years without significant claims payments.").

[220] FEDERAL INSURANCE OFFICE, U.S. DEP'T. TREAS., REPORT ON THE EFFECTIVENESS OF THE TERRORISM RISK INSURANCE PROGRAM 27 (Jun. 2018), https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2018_TRIP_Effectiveness_Report.pdf.

[221] *Id.* at 17–19.

[222] *See, e.g.*, Jeffrey E. Thomas, *Benefits of the U.S. Program for Terrorism Insurance from a Comparative Perspective*, 4 J. FIN. PERSP. 79, 87 (2017).

[223] Robert J. Rhee, *The Terrorism Risk Insurance Act: Time to End the Corporate Welfare*, CATO INSTITUTE (Sept. 10, 2013), https://www.cato.org/publications/policy-analysis/terrorism-risk-insurance-act-time-end-corporate-welfare.

[224] *See* Boardman, *supra* note 194, at 812.

[225] *Id*. at 842. Note, however, that even Broadman admits that in the context of cyber terrorism, there could be "loss reduction measures" that could be promoted by private insurers. If that is the case, then insurance would have an advantage over all other methods in the policy analyst's tool kit. *Id*. at 840–41.

Global reinsurance markets run on broader risk pools that can offset the risk load of a particular set of risks with premiums from coverage of other uncorrelated risks. Government-run reinsurance, on the other hand, operates differently. By consolidating risk "within the borders of one country or even one political subdivision," it hampers its ability to diversify risk.[226] Nonetheless, under certain unusual circumstances providing government reinsurance is pivotal.[227] In the case of terrorism insurance, not only is the government the holder of the best available underwriting data (gathered through its counter-terrorism surveillance programs), more importantly without its intervention, insurers will refuse to play the game. TRIA-like programs incentivize and where necessary compel the insurers to keep playing. Carriers' ability to ever model the risk of terrorist catastrophes depends on their commitment to remain active market players, acquiring the necessary security and claims data to expand on their actuarial understanding of the risk.

4. Policy Reform

Coverage for cyber terrorism and state-sponsored attacks offers one area where some intervention is needed for public policy reasons. The current state of the market is one of under-insurance. If we are to ever close the cyber insurance gap and address the systemic risks associated with these two types of perils, three particular challenges should be addressed:

a. There is significant divergence between policies around tailored coverage and exclusionary language including terms such as "terrorism," "cyber terrorism," "state-sponsored," and "government entity." Coalescing around uniform and agreed-upon terminology is necessary to increase the stability, clarity, and consistency of the market. Uniformity would provide the insured greater foreseeability around their scope of coverage and therefore reduce hesitancy around the purchase of policy.[228] State legislatures

---

[226] Letter to The Honorable Michael T. McRaith, Director of the Federal Insurance Office at the Department of Treasury, *Comments on Study describing the breadth and scope of the global reinsurance market and the critical role such market plays in supporting insurance in the United States*, R-Street, 3 (Aug. 21, 2012), http://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2012/08/R-Street-Reinsurance-Comments.pdf.

[227] *Id*. at 3–5 (suggesting a three-part test for evaluating whether governments should ever be directly involved in providing reinsurance capacity: (1) There is a strong and long-lived historical precedent that the government uses tax money to pay for the expense to be reinsured; (2) The expense to be reinsured will not be covered by the private sector by ordinary means; (3) The best available underwriting data is largely or entirely in the hands of the public sector and cannot feasibly be released.).

[228] Just by way of a parallel, is noteworthy that we have witnessed an opposite trend in personal-line homeowners' markets. There we saw a move from the presumptive standard

and insurance regulatory agencies (acting individually or through the NAIC)[229] could develop model insurance language that may be picked up by the carriers. States can further regulate policy language through a policy form review process, in which misleading or unclear language is eliminated prior to the policy being authorized to be sold in the market.[230]

b. The *Mondelez* case seems to suggest that domestic courts will be the first venue in which standards around cyber attribution will be determined. This will put a significant burden on judges, who will be called to adapt traditional torts jurisprudence around causality and responsibility to tackle the new challenge of attributing cyber harms. The concern, of course, is that a less-than-tech-savvy judge in a lower court might be called to appreciate the nuances of fact-intensive inquiry into the nature of each individual attack. Judges who refuse such an examination might simply rely on uncorroborated statements from intelligence agencies, opening the door for abuse. After all, "interested policy-makers quickly learn that intelligence can be used the way a drunk uses a lamp post – for support rather than illumination."[231]

In recent years, there have been a number of proposals calling to centralize cyber attribution within a new independent international body, which could evade the risk of politicization and promote uniform cyber attribution standards.[232] Others have pushed for a multiplicity of attributors,

---

ISO language to proprietary policy language that rejects uniformity. *See, e.g.*, Daniel Schwarcz, *Reevaluating Standardized Insurance Policies*, 78 U. CHI. L. REV. 1263 (2011). Schwarcz has recently proposed a legal intervention that would reintroduce uniformity precisely because insurers that depart from standardized language do not always fully internalize the cost of doing so. *See* Daniel Schwarcz, *The Role of Courts in the Evolution of Standard Form Contracts: An Insurance Case Study*, 46 BYU L. REV. 471 (2021).

[229] For further reading on the regulatory role of the insurance commissioners and NAIC, *see* RAYMOND A. GUENTER AND ELISABETH DITOMASSI, FUNDAMENTALS OF INSURANCE REGULATION: THE RULES AND RATIONALES 25–28 (2017).

[230] *Id*. at 34.

[231] THOMAS LOWE HUGHES, THE FATE OF FACTS IN A WORLD OF MEN: FOREIGN POLICY AND INTELLIGENCE-MAKING, 22 (1976).

[232] *See* Eichensehr, *supra* note 207, at 215–16 ("The Atlantic Council suggested a Multilateral Cyber Attribution and Adjudication Council that would provide '"a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes.' Microsoft proposed a multistakeholder attribution body 'consist[ing] of technical experts from across governments, the private sector, academia, and civil society' and modeled on the International Atomic Energy Agency. RAND Corporation researchers went further, proposing a 'Global Cyber Attribution Consortium' that would entirely exclude states. Instead, the Consortium would be comprised of 'technical experts from cybersecurity and information technology companies, as well as academia,' and 'cyber-space policy experts, legal scholars, and international policy experts from a diversity of academia and research organizations.' . . . all of the proposals face an uphill climb: they need buy-in from actors with sometimes divergent interests, and any new entity would take time to build its capabilities and credibility.").

inviting both governments and non-governmental actors to take part in a decentralized system of attribution. In this system each attributor would adopt its own digital forensic standards and methodologies, thereby serving as a check on the others' statements of attribution.[233] Regulators should be mindful of these developments and regulate insurers to embed evolving international standards on attribution into their claims investigations processes.

c. In December 2016 the Treasury Department released guidance clarifying that "stand-alone cyber insurance policies reported under the 'Cyber Liability' line are included in the definition of 'property and casualty insurance' under TRIA. . . ."[234] The Treasury Department went on to clarify that even "non-affirmative" cyber insurance policies that are eligible for TRIA coverage will be covered under the program.[235] This is a step in the right direction. However, three concerns remain, even after this announcement.

First, it remains to be seen whether TRIA will be extended in 2020 for a fourth time. The introduction of cyber terrorist risk should create a new justification for Congress to extend TRIA, and this point should lead the insurers lobbying campaigns for extension. The new extension should also amend TRIA to explicitly incorporate coverage for cyber losses into the statute so that specific rules around limits and recoupment in the case of a cyber incident can be developed.

Second, the U.S. is not the only country to adopt a governmental terrorist backstop mechanism. Other countries have legislated similar, albeit slightly different, models. Of those countries, not all have extended their programs to cover losses from cyber terrorism incidents. The U.K. terrorism insurance pool, Pool Reinsurance Company Limited (*Pool Re*), has extended its coverage to include physical damage and business interruption losses caused by acts of cyber-related terrorism.[236] However, in Australia and Russia cyberattacks are specifically excluded from the definition of a terrorist event

---

[233] *Id.* at 216–17.

[234] Department of the Treasury, *Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program*, 81 Fed. Reg. 95313 (Dec. 27, 2016).

[235] *Id*. ("Certain insurance policies that may contain a 'cyber risk' component or which do not exclude losses arising from a cyber event continue to be written in existing TRIP-eligible lines of insurance and are thus subject to the provisions of the Program."). Note, however, that professional liability insurance is specifically excluded from TRIA coverage, and to the extent that cyber coverage is offered through it, it would not be covered.

[236] *Introduced Remote Digital (Cyber) cover*, POOL RE (Apr. 2018), https://www.poolre.co.uk/history/introduced-remote-digital-cyber-cover/ (noting that the extended coverage does not include "intangible assets" such as data, which are typically addressed in cyber insurance policies).

triggering governmental reinsurance.[237] Realizing that cybersecurity threats do not end at the border, the U.S. should encourage other countries to adopt its policy and extend their governmental terrorism coverage to cyber perils.

Finally, while the focus of the debates has been on extending governmental reinsurance schemes to cover cyber terrorist incidents, no discussion has involved the more substantive issue of state-sponsored cyberattacks. Recall, that unlike cyber terrorism, these attacks have actually materialized and are occurring at a dangerous rate with significant losses. The same logic that guided us in extending TRIA to cover losses for cyber terrorist harms should pave the way for offering a governmental insurance program for covering state-sponsored cyberattacks under certain extreme conditions.

B. Indemnification for Ransomware Payments

1. The Ransomware Epidemic

Ransomware has become a major scourge to both private corporations and local governments. Recall the numbers above provided: an average of 4,000 ransomware attacks occur every day globally with damages hovering around $1 billion annually.[238] While data breach notification laws require entities to notify their consumers when their data is compromised, it's not always clear if ransomware attacks are subject to the same disclosure rules.[239] According to the National Association of Insurance Commissioners (NAIC),

---

[237] For a full survey of national terrorism insurance programs and their extension to cyber perils, *see generally* THE TERRORISM POOL INDEX: REVIEW OF TERRORISM INSURANCE PROGRAMS IN SELECTED COUNTRIES, WILLIS TOWERS WATSON (2019).

[238] *See supra* note 58 and accompanying text.

[239] This is because breach notification rules and data protection regulation such as Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA] and Children's Online Privacy Protection Act, Pub. L. 105-277, 112 Stat. 2681-728 (1998) [hereinafter COPPA] apply only in the case of unauthorized access, acquisition, use or disclosure of particular types of personal information. To determine whether a ransomware event triggers the obligations under such laws is a fact-intensive inquiry that will depend on the specifics of each case. As a whole, however, ransomware attacks are designed to extort money from a victim and not steal PII. If no PII was actually accessed or acquired (only encrypted by the hackers and held for ransom) then obligations may not be triggered. For further analysis *see* Michael Morgan, *Guidance on Ransomware Attacks under HIPAA and State Data Breach Notification Laws*, MCDERMOTT WILL & EMERY (Aug. 8, 2016), https://www.jdsupra.com/legalnews/guidance-on-ransomware-attacks-under-30510/. *Cf. Fact Sheet on Ransomware*, DHHS (Jul., 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (noting that under the HIPAA Breach Notification Rule, notification "is required unless the entity can demonstrate a low probability of compromise of the [Protected Health Information].").

this means that "most ransomware attacks go unreported."[240] This is not surprising, as victims prefer to avoid the reputational costs that might be associated with disclosures and instead seek to deal with the attack on their own.[241]

A particularly troubling trend has been ransomware attacks targeting cities, police departments, and schools. Due to budgetary constraints, these public entities suffer from old and insecure information systems that are particularly susceptible to these attacks. According to one analysis, beginning in 2013 with the first ransomware against local government (targeting the Swansea Police Department in Massachusetts), at least 169 county, city or state government systems have been attacked.[242] Insurers play a growing role in regulating local government's cyber posture and policies. The Alaskan City of Valdez, for example, turned to its insurers to receive authorization of payment to hackers in the sum of $26,000 for a ransomware attack that paralyzed the city's computer infrastructure in June of 2018.[243]

Indeed, ransomware crime has become "many times more lucrative than say, bank robbery, with the advantage of no weapons, disguises, getaway cars, police chases. In fact, practically no risk of getting caught at all."[244] It is truly a business enterprise centered around extortion:

---

[240] *Ransomware*, NAIC (Dec. 6, 2018), https://www.naic.org/cipr_topics/topic_ransomware.htm. Indeed, despite the 4,000 global daily ransomware attacks estimated by the FBI, many of which target the US, a measly 1,493 attacks were reported to the FBI's Internet Crime Complaint Center in 2018 by victims in the US.

[241] *See Annual Internet Crime Report*, IC3, FBI 19 (2018), https://pdf.ic3.gov/2018_IC3Report.pdf. (recording that 1,493 ransomware attacks were reported in 2018 despite an estimated 4,000 global daily attacks).

[242] *See* Allan Liska, *Early Findings: Review of State and Local Government Ransomware Attacks*, RECORDED FUTURE (May 10, 2019), https://www.recordedfuture.com/state-local-government-ransomware-attacks/.

[243] Catalin Cimpanu, *City of Valdez, Alaska admits to paying off ransomware infection*, ZDNET (Sept. 4, 2018), https://www.zdnet.com/article/city-of-valdez-alaska-admits-to-paying-off-ransomware-infection/. *See also* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks (describing a decision of the mayor of Lake City Florida, to pay a ransom of 42 bitcoin – some $460,000 – with its insurer Beazley, an underwriter at Lloyd's of London, reimbursing it for the extortion payment under its cyber insurance policy subject to only $10,000 in deductibles). This is concerning, in part, because some cities are provided insurance through intergovernmental risk pools managed by former mayors and city managers. If commercial insurers have significant limitations in underwriting and modeling cyber risk, one can only imagine what limited resources are available to these risk pools.

[244] Wade Goodwyn, *Ransomware Attacks Create Dilemma For Cities: Pay Up Or Resist?*, NPR (Jul. 9, 2019), https://www.npr.org/2019/07/09/739999730/what-happens-when-hackers-hold-cities-hostage-with-ransomware-attacks.

> There is a growing infrastructure, extortion economy, and organization around the criminal industry of cyber extortion. The extortionists have become professional at the process, including setting up call centers in third-party countries to assist the individuals that they are blackmailing with the necessary payment steps and providing technical support for the unlocking of their data, providing decryption codes for the software. Support extends to helping their victims set up bitcoin bank accounts to make untraceable payments . . . [for it is essential] to sustaining the extortion business model [that] the criminals honor their side of the bargain by freeing up the locked data when the payment is made.[245]

Those who experience a ransomware attack are faced with a dilemma: pay the relatively limited extortion (hackers cleverly seek extortion payments at a price lower than the cost of full recovery) and suffer the moral hazard (encouraging the extortionists "to repeat the crime on other victims" with the extortion payment providing the necessary resources to sustain and expand their operations[246]), or avoid paying and suffer the costs of significant business interruptions and economic losses.

2. The Parallel to K&R Policies

The first Kidnapping and Ransom policies were introduced in 1933 by Lloyd's of London following the kidnapping of Charles Augustus Lindbergh, Jr., the 20-month-old son of the famous aviator. A series of kidnappings by the IRA in the 1970s and 80s introduced a new body of scholarly and parliamentary debate in the U.K. around kidnapping insurance regulation. Some pushed for a ban arguing it was "illogical for the government to take a firm line against conceding to terrorist demands, including the payment of ransom, and yet to give its seal of approval to the availability of insurance designed to reimburse those who do pay."[247]

For a long time British ministers claimed that kidnap insurance "was helpful to the authorities" as the insurance companies "typically used professional security consultants to audit the security procedures of the policyholder, thereby reducing the risk of kidnap in the first place."[248] Banning ransom insurance "would simply force potential victims to go to less well-organised overseas insurance companies that did not insist on the involvement of specialists to improve security standards and that paid out

---

[245] COBURN ET. AL., *supra* note 25, at 54–55.
[246] *Id*. at 54.
[247] Richard J. Aldrich and Lewis Herrington, *Secrets, Hostages and Ransoms: British Kidnap Policy in Historical Perspective*, 44(4) REV. INT'L STUD. 738, 753 (2018).
[248] *Id*. at 752.

more readily."[249]

Ultimately a ban was introduced with the adoption of the 2000 Terrorism Act on Kidnap and Ransom (re)insurance Business. That ban prohibited kidnapping insurance in terrorism cases within the U.K. but allowed U.K. insurers to continue to provide it abroad.[250] Following a series of kidnappings of Europeans by ISIS, the 2015 Counter Terrorism and Security Act made it illegal for any U.K. based insurance company to provide kidnapping insurance in terrorism cases, regardless of the victim's nationality, further providing that such indemnification could trigger criminal liability for the insurer.[251]

In the U.S. a different position was taken. Following a series of kidnapping of corporate officers in Latin America in the 80s, a similar ban on insurance for kidnapping was discussed. The "FBI was anxious to create a climate in which the family of the victim would readily approach them for guidance."[252] The worry, therefore, was that "a ban on insurance was an inhibition to early contact with law enforcement."[253] This is because policyholders were required to notify the FBI prior to indemnification and in fact relied on the FBI during the negotiation with the kidnappers. Ed Meese, the U.S. Attorney General at the time, had an additional concern. He felt squeamish about the idea that the government "might find itself in the difficult position of having caused the death of the victim."[254] This is regardless of the fact that, perversely, the "presence of insurance actually increases the probability of kidnapping."[255]

As it relates to ransomware payments the U.S. Government (USG) position continues to avoid making a decision. Much like Ed Meese in the 1980s, current policy remains squeamish as to the idea of enforcing a rigid rule on victims of ransomware attacks. In a recent guide to Chief Information Security Officers (CISOs), the USG merely "encourages" contacting local field offices of the FBI or the U.S. Secret Service in the case of a ransomware attack.[256] It further discourages paying a ransom to criminal actors, but

---

[249] *Id*. at 754.

[250] *Id*. at 752 (the law made paying a ransom synonymous with financing terrorism, however "because this law only applied within the British jurisdiction, underwriters were free to offer kidnap and ransom policies to companies operating overseas.").

[251] *Id*.

[252] *Id*. at 756.

[253] *Id*.

[254] *Id*. (summarizing a meeting between Ed Meese and U.K. Home Secretary Douglas Hurd).

[255] Gideon Parchomovsky & Peter Siegelman, *The Paradox of Insurance*, Faculty Scholarship at Penn Law 2158, 5 (2020), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3160&context=faculty_scholarship.

[256] HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE, U.S. GOVERNMENT INTERAGENCY TECHNICAL GUIDANCE, 5 (Dec. 2018), https://www.justice.gov/criminal-

ultimately leaving this "serious decision" in the hands of the CISO who is called to evaluate "all options to protect shareholders, employees and customers."[257] Note that the CISO is not called to evaluate broader societal concerns around paying the ransom and funding this larger business of extortion.

The FBI is not alone in adopting non-committal language around enforcement of reporting requirements against victims of ransomware crimes. The U.K. National Crime Agency (NCA) has issued the following warning to businesses as part of its 2018 National Strategic Assessment of Serious and Organized Crime: "Organisations which don't report that they've been the victim of cybercrime are putting others at risk of further attacks and are hampering the authorities' ability to fight against hackers. Underreporting of data breaches continues to erode our ability to make robust assessment of the scale and cost of network intrusions. Many companies are not disclosing data breaches, putting victims at risk."[258] Nonetheless, the NCA too has failed to develop enforcement mechanisms against a failure to report.

3. Policy Reform

a. Most recently Mieke Eoyang and Allison Peters from Third Way observed that part of the reason for the failure to deal with cybercrime is rooted in the way law enforcement operates. They argue that law enforcement needs to "modernize and enhance efforts to identify criminals" as well as develop "better metrics" to assess its progress in stopping such crime.[259]

While this may be true, law enforcement cannot carry out its collective duty if cybercrime is going unreported. There is a growing trend in cyber insurance policies to allow for ransomware extortion payment indemnification without requiring the policy holder to first notify the police or the FBI of the ransom prior to seeking compensation. Insurers argue that making such a demand to policyholders would disincentivize them from acquiring the policy in the first place, as they are worried about potential reputational harms. This collective action problem is resulting in a race to the bottom where it is enough for one insurer to avoid a requirement of notifying the FBI for all insurers to follow suit out of worry of losing business.

---

ccips/file/872771/download.

[257] *Id*.

[258] Danny Palmer, *Cyber crime: Under-reporting of attacks gives hackers a green light, say police*, ZDNET (May 14, 2018), https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/.

[259] Mieke Eoyang & Allisson Peters, Opinion, *Analog Cops and Digital Robbers*, THE BALT. SUN (Jun. 13, 2019), https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0614-cyber-criminals-20190613-story.html.

Note that some policy holders have good reasons not to notify the FBI. As one cyber insurance broker at Marsh explained to me: "I had a situation in which a client reported cyberhack activity to the FBI. The FBI forbid this client from providing any information about the attack to the insurance carrier whatsoever but for that the company had a cyberhack. This is one reason why we cannot incentivize the client to report this information to the FBI. It presents a situation in which the client may not be able to benefit from any insurance solution if they choose to comply with law enforcement directives."[260]

If we are ever to eradicate the crime of ransomware, insurers must be compelled to include a requirement into their policies that demands notification to law enforcement prior to any indemnification. The main rationale not to ban insurance for kidnap and ransom extortion payments has historically been that the insurance industry incentivizes greater cooperation with law enforcement, not lesser cooperation.[261] At the same time, however, law enforcement needs to collaborate with cyber insurers. More work should be done to make sure that information sharing does not penalize the client's insurance recovery, as there are often very strict parameters regarding notification and cooperation in the insurance policy.

b. Looking beyond notification, regulators and enforcement agencies should develop a framework for deciding when societal risk from a particular extortion payment is low or the danger from a failure to pay is high, both of which might justify indemnification. Setting standards for a case-by-case analysis of when to allow for payments could be a first step in a broader national enforcement program. For example, we might allow indemnification in the case of a substantial risk to life and property. We might not allow indemnification if the costs to the policyholder are significantly limited. In those cases where indemnification might be denied, the ransomware should be seen as a mere "cost of doing business" in a digitized world. In this regard, we might begin to think of ransomware costs as similar to "shrink losses" from shoplifting in the retail industry, which amount to around $100 billion worldwide, or 1.82% of global sales, and are not indemnified.[262]

As we wait for a governmental policy, one should appreciate local-government efforts to develop a firm stance. In July 2019, more than 220 U.S. mayors signed on to a resolution not to pay ransoms to hackers. The resolution was adopted at the U.S. Conference of Mayors annual meeting (the

---

[260] Interview with the author (Jul. 24, 2019).

[261] *See* Aldrich, *supra* note 247, at 752.

[262] *See generally* TJ McCue, *Inventory Shrink Cost the US Retail Industry $46.8 Billion*, FORBES, (Jan. 31, 2019), https://www.forbes.com/sites/tjmccue/2019/01/31/inventory-shrink-cost-the-us-retail-industry-46-8-billion/?sh=3180307a6b70 (explaining the impact of "shrink" losses on the U.S. retail industry).

Conference represents 1,400 cities with populations over 30,000).[263] In February 2021 the New York Department of Financial Services introduced an insurance circular that called on all property & casualty insurers that write for cyber insurance to discourage ransomware payments and require notice to law enforcement in case of a breach.[264]

C. Indemnification for Statutory Fines for Data Protection violations

1. The Age of Data Protection and Insurability of Fines

We live in a data monarchy, one in which individuals are considered "data subjects." The kingdom's subjects trade in their personal information, generated and stored by an array of "smart" connected devices, with corporations known as "data controllers" and "data processors." These modern monarchs promise free services in exchange for the continuous and unremitting exploitation of their subjects' data, which they rely on "to predict, monitor and even steer individuals' future behavior."[265]

To alter the relational dynamics in this data driven economy policymakers have moved to adopt bold legal frameworks that seek to "empower individuals to take back control of their personal data."[266] Today, more than a hundred countries have adopted data protection and privacy laws aimed at addressing the inherent vulnerabilities associated with this frightening form of surveillance capitalism.[267]

The European General Data Protection Regulation (GDPR) is perhaps the most expansive framework in the world for ensuring users data protection. At the heart of the regulation are a set of rights that data subjects enjoy including the right to be forgotten, the right to be informed, the right to rectification, and the right to access.[268] The law came into force on 25 May 2018. Under the GDPR, businesses can be fined up to €20 million or 4% of their global annual turnover, whichever is higher. This is the main punitive measure introduced in the act and the primary sword behind its deterrence

---

[263] Oscar Gonzalez, *US mayors resolve not to pay hackers over ransomware attacks*, CNET (Jul. 12, 2019), https://www.cnet.com/news/us-mayors-adopt-resolution-to-not-pay-hackers-over-ransomware-attacks/.

[264] *See* Insurance Circular Letter No. 2, *supra* note 68.

[265] Tomaso Falchetta, Opinion, *Down with the Data Monarchy*, POLITICO (Jan. 28, 2018), https://www.politico.eu/article/down-with-the-data-monarchy-protection-platforms-facebook-whatsapp/.

[266] *Id*.

[267] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[268] *See generally* PAUL VOIGT AND AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE (2017).

effect. We have already witnessed the utilization of this expansive authority. On July 8, the U.K.'s data protection authority, the Information Commissioner's Office, "fined British Airways an eye-popping £183 million ($228 million) for leaking the personal data of 500,000 of its customers. Marriott International got slapped with a fine of just over £99 million ($124 million) for exposing a variety of personal data in 339 million guest records globally."[269]

In the United States, there is not one all-encompassing data privacy law. Instead, it is a patchwork of laws that contain privacy and data security provisions. These laws relate to specific business sectors and specific populations, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act (COPPA), and most recently the California Consumer Privacy Act (CCPA), which will enter into force on 1 January 2020. Common to all these laws is the utilization of enforcement for violations through either statutory fines from governmental agencies or through litigation by the State Attorneys-General.

Cyber insurance policies which cover statutory fines often include the following language:

> [A]ny civil fine or money penalty payable to a governmental entity that was imposed in a Regulatory Proceeding by the Federal Trade Commission, Federal Communications Commission, or any other federal, state, local or foreign governmental entity, in such entity's regulatory or official capacity; the insurability of Penalties shall be in accordance with the law in the applicable venue that most favors coverage for such Penalties.[270]

It is important to note that policies that provide cyber insurance for fines and penalties typically will also provide coverage for certain costs incurred in connection with a governmental investigation and pursuit of a claimed violation.

In May 2018, DLA Piper and Aon reviewed the insurability of GDPR fines across Europe and found that GDPR fines were only insurable in two countries (Finland and Norway). Most countries did not allow for the insurance (including France, Italy, and Spain), whereas in some countries there was significant ambiguity around such insurance.[271] The UK

---

[269] *Id.*

[270] Matthew Divelbiss & John Iole, *Understanding "Fines and Penalties Coverage" Under Cyber Insurance, Insurance Policyholder Advocate*, JONES DAY (Feb. 26, 2015), https://www.jonesday.com/Understanding-Fines-and-Penalties-Coverage-Under-Cyber-Insurance-iInsurance-Policyholder-Advocatei-02-26-2015/.

[271] *DLA Piper and Aon Review Insurability of GDPR Fines Across Europe,* DLA PIPER (May

Information Commissioner's Office (ICO) has for example come out as saying that there is "nothing in the GDPR which either permits or prohibits insurance coverage for regulatory fines."[272]

On 16 October 2018, the Financial Supervisory Authority in Finland published an interpretation of the Finnish Insurance Companies Act, according to which "it is contrary to good insurance practice to provide insurance against a risk where the insurance might encourage actors' indifference to regulatory compliance and compromise actors' obligation to comply with the respective regulations. Provision of insurance against such a risk is in conflict with generally accepted social values."[273]

Most recently, in January 2019, the Global Federation of Insurance Associations (GFIA) has written a letter to the OECD Insurance and Private Pensions Committee (IPPC) noting that "there is international confusion as to the insurability of fines and penalties. OECD work to clarify this issue would benefit consumer and insurer contract certainty."[274]

2. The Parallel to Punitive Damages Coverage

It is a basic principle of insurance law that insurance against intentional wrongdoing violates public policy as it incentivizes moral hazards.[275] For example, in *Massachusetts Mutual Life Insurance v. Woodall*, the Court concluded that the insured was denied coverage for lost income under his disability insurance policy for his depression resulting from the prospect of being disbarred from the practice of law after committing certain intentional misconduct.[276]

In examining the insurability of statutory fines for data protection violations, one can draw an analogy to the rich history and jurisprudence

---

16, 2018), https://www.dlapiper.com/en/mexico/news/2018/05/insurability-of-gdpr-fines-across-europe/.

[272] Carolyn Cohn, *Insurers cash in on new European data privacy rules*, REUTERS (May 21, 2018), https://www.reuters.com/article/insurance-cyber-gdpr/insurers-cash-in-on-new-european-data-privacy-rules-idUSL5N1SN6QY.

[273] *Finland: Insurance Against Administrative Fines Announced as Not Permitted*, DLA PIPER (Oct. 23, 2018), https://blogs.dlapiper.com/privacymatters/finland-insurance-against-administrative-fines-announced-as-not-permitted/.

[274] *GFIA comments on the OECD Insurance and Private Pensions Committee's (IPPC) next steps on cyber issues*, GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS (January 2019), http://www.gfiainsurance.org/en/upload/positionpapers/GFIA-19-02%20GFIA%20comments%20on%20OECD%20next%20steps%20on%20cyber.pdf.

[275] But *cf.* Christopher French, *Debunking The Myth that Insurance Coverage is Not Available or Allowed for Intentional Torts or Damages*, 8 HASTINGS BUS. L.J. 65 (2012) (underscoring the many different scenarios in which liability insurance is offered for intentional torts, and why public policy favors such insurance recoveries).

[276] Mass. Mut. Life Ins. Co. v. Woodall, 304 F. Supp. 2d 1364, 1366 (S.D. Ga. 2003).

around coverage for punitive damages. Both cases involve the question of whether insurance in these instances should be seen as a violation of public policy for indemnifying misconduct that is sufficiently blameworthy. The literature around insuring punitive damages[277] illustrates how courts have split on this issue.

In *Hartford Casualty Insurance Company v. Powell*, the District Court for the Northern District of Texas concluded that punitive exemplary damages are levied against a defendant to punish him for outrageous, malicious, or otherwise morally culpable conduct. "[R]equiring a wrongdoer to suffer the sting of a punitive damage award is synonymous with public good, with the consequence that necessarily a private contract that would tend to diminish the punishment effect of a punitive damage award would harm or injure the public good.*"*[278] The Court based on its decision on the findings of Circuit Judge John Wisdom of the Fifth Circuit in *Northwestern Nat'l Cas. Co. v. McNulty*, who found that:

> It is not disputed that insurance against criminal fines or penalties would be void as violative of public policy. The same public policy should invalidate any contract of insurance against the civil punishment that punitive damages represent. The policy considerations in a state where …. punitive damages are awarded for punishment and deterrence, would seem to require that the damages rest ultimately as well nominally on the party actually responsible for the wrong. If that person were permitted to shift the burden to an insurance company, punitive damages would serve no useful purpose. Such damages do not compensate the plaintiff for his injury, since compensatory damages already have made the plaintiff whole. And there is no point in punishing the insurance company; it has done no wrong. In actual fact, of course, and considering the extent to which the public is insured, the burden would ultimately come to rest not on the insurance companies but on the public, since the added liability to the insurance companies would be passed along to the premium payers. Society would then be punishing itself for the wrong committed by the insured.[279]

---

[277] *See, e.g.*, Kenneth Mann, *Between Civil Sanctions: The Middleground Between Criminal and Civil Law* 101 YALE L. J. 1795 (1992); *see also* ROBERT G. SCHLOERB ET. AL., PUNITIVE DAMAGES: A GUIDE TO THE INSURABILITY OF PUNITIVE DAMAGES IN THE UNITED STATES AND ITS TERRITORIES (3d ed., 2003).

[278] Hartford Cas. Ins. Co. v. Powell, 19 F. Supp. 2d 678, 694 (N.D. Tex. 1998).

[279] Northwestern Nat'l Cas. Co. v. McNulty, 307 F.2d 432, 440–41 (5th Cir. 1962). Additionally, Tom Baker has expounded on this concept:

> [T]he theoretical justifications for punitive damages are to prevent harm and to provide retribution for highly culpable harm. Insurance for punitive damages undercuts the prevention justification when it reduces the financial impact of those damages on defendants (and potential

Presenting an opposite view, in *First Bank (N.A.)* v. *Transamerica Insurance Company*,[280] the Supreme Court of Montana suggested that to adopt Judge Wisdom's deductive conclusions would be akin to leaning "upon a slender reed."[281] In particular, the Court reasoned that punitive damages are many times issued on the basis of the particular findings of a particular set of fact finders. To deny coverage is unsustainable from the perspective of the Court where a different set of fact finders might have reached a different conclusion as to punitive damages. Even more so, the Court argued that "a defendant may be subject to a punitive damage award for conduct not considered or known to be wrongful prior to the imposition of the award."[282]

To the Montana Supreme Court's arguments, Tom Baker adds a set of additional justifications for allowing insurance for punitive damages:

> (1) Insurance companies will have strong incentive to control moral hazard and adverse selection (thereby preserving the deterrence/prevention);[283]
> (2) "By encouraging victims to seek and collect punitive damages, insurance for punitive damages enhances tort law's capacity to project norms and to reassert publicly the value of those injured." The availability of the insurance will increase the likelihood that plaintiffs will file actions thereby enhancing tort law's ability to achieve its retributive ends; [284]
> (3) Applying an "intentional harm" exclusion could answer some of the retribution objections to insurance for punitive damages.[285]

3. Policy Reform

Baker's three justifications are difficult to apply in the context of indemnification for data protection violations for two reasons. First, even if

---

> defendants) who are unlikely to respond adequately to the norm projection aspects of tort law. Moreover, insurance for punitive damages undercuts the retribution justification when it allows a perpetrator to escape responsibility for the consequences of egregious action.

Tom Baker, *Reconsidering Insurance for Punitive Damages*, 1998 WIS. L. REV. 101, 113 (1998).

[280] First Bank (N.A.) v. Transamerica Ins. Co., 679 P.2d 1217, 1221 (Mont. 1984).

[281] *Id*.

[282] *Id*. at 1222.

[283] Baker, *supra* note 279, at 127–28.

[284] *Id*. at 113.

[285] *Id*. at 130.

insurance companies are incentivized to control moral hazards, as the discussion above has already shown, they might not be well suited to engage in the kind of cybersecurity and privacy assessments that are necessary to prevent the harm. Lacking sufficient expertise and historical data around cyber risks makes it so that we should be cautious about insurers' ability to preserve the deterrence/prevention effects that fines would otherwise introduce. Baker argues that "the twin problems of moral hazard and adverse selection provide insurance companies with adequate incentive to address the deterrence objection to punitive damages insurance and that the companies' control over underwriting and contracting places them in a better position than courts to address that objection."[286] In the data protection context, cyber insurers might not be at a better position than data protection authorities and federal regulators and enforcement agencies in providing the needed deterrence.

Moreover, indemnifying fines from data protection regulation might not enhance norms projection. This is because, unlike other fields of law, in cases of data breaches and privacy infringements, victims have a limited capacity to approach the Courts. Article III standing requirements prevent them from showing an "injury-in-fact" that is necessary to file cases so to achieve tort law's retributive ends.[287]

Thus, it would seem that we should be guided by Judge Wisdom's general approach and operate with a general assumption against indemnification as ultimately it stands against societal public policy interests. That said, we should avoid a binary overbroad *per se* rule against insurability. GDPR, HIPAA, COPPA, and CCPA fines are not categorically uninsurable. For example, where a fine is assessed vicariously against a policyholder (such as when a corporation is held liable for an unauthorized act of one of its employees), depending on the facts, we might not deem this situation as sufficiently blameworthy to prevent insurance coverage. Cases like the Uber and Equifax data breaches, on the other hand, where the companies' directors failed to be transparent about the ramifications of the attack and actively worked to hide the truth,[288] might trigger greater reprehensibility and should

---

[286] *Id*. at 101.

[287] *See, e.g.*, *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013); *In re* Google, Inc. Privacy Policy Litig., No. 5:12-cv-001382-PSG, 2015 U.S. Dist. LEXIS 92736 (N.D. Cal. Jul. 15, 2015); See also DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 812–19 (6th ed., 2017); Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 CARDOZO L. REV. DE-NOVO 119, 126 (2015).

[288] *See, e.g.*, Mike Isaac, Katie Benner & Sheera Frenkel, *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; Thomas Brewster, *How Equifax Kept Its Mega Breach Secret From Its Own Staff*, FORBES (Mar. 14, 2018),

prevent indemnification, even if not falling squarely under an "intentional harm" exclusion.

Another component that might go into our analysis of insurability pertains to the maturity of the law. Recall the finding of the Montana Supreme Court: we might be more lenient with insuring a punitive damage or statutory fine where the conduct was "not considered or known to be wrongful prior to the imposition" of the award or fine. If the GDPR or CCPA, which are two recent enactments, are insufficiently clear, especially in the way certain obligations are to be applied in specific circumstances, we might allow insurance to step in during the interim period and cover losses triggered by this ambiguity. Once the law matures and rules are more settled, we may revisit this determination.

V. CONCLUSION

In 2001, Bruce Schneier provided a premonition. In a short essay titled "*Insurance and the Computer Industry*,"[289] he foresaw the rise of the cyber insurance market. Schneier imagined a world wherein insurers sold "anti-hacking policies,"[290] and where it was "unthinkable not to have them," as a failure of an executive to acquire such a policy would be seen as recklessness worthy of class action suits.[291] In his ideal world, Schneier imagined a computer security industry "run by the insurance industry," with information security decisions being directly impacted by an insurer's checklist.[292] He believed that once we reach this world then we will "start seeing good security rewarded in the marketplace."[293]

Nearly twenty years have passed since Schneier's essay was published

---

https://www.forbes.com/sites/thomasbrewster/2018/03/14/how-equifax-kept-its-mega-breach-secret-from-its-own-staff/#178adf3d3ef1.

[289] Bruce Schneier, *Insurance and the Computer Industry*, SCHNEIER ON SECURITY (Mar. 2001), https://www.schneier.com/essays/archives/2001/03/insurance_and_the_co.html.

[290] In fact, in a different essay of the same period Schneier came up with more policy names:

> Concerned about denial-of-service attacks? Get bandwidth interruption insurance. (I'm making these policy names up here.) Concerned about data corruption? Get data integrity insurance. Concerned about negative publicity due to a widely publicized network attack? Get a rider on your good name insurance that covers that sort of event. The insurance industry isn't offering all of these policies yet, but they will before long.

Bruce Schneier, *The Insurance Takeover*, SCHNEIER ON SECURITY (Feb., 2001), https://www.schneier.com/essays/archives/2001/02/the_insurance_takeov.html.

[291] Schneier, *supra* note 289.

[292] *Id*.

[293] *Id*.

and we are still miles away from his wholesome vision. Perhaps Schneier's wondrous marketplace will never be fully attained. A constantly evolving cybersecurity threat landscape and an ever-changing technological reality is hindering the insurance market's ability to effectively mature. Information asymmetries and underwriting challenges are further limiting the ability of insurers to properly price stand-alone cyber policies and set appropriate premiums.[294] Lack of consensus around security standardization, ambiguous coverage schemes and policy questionnaires, and insufficient cybersecurity expertise are shaping a marketplace wherein good security is still not always rewarded. These challenges have been the focus of most of the literature to date.

But one may wish to pose an alternative question: should we even pursue Schneier's vision? Is a world where our public cybersecurity is set by private commercial insurers a desirable world? Should the insurer's checklist and checkbook replace agency regulation and augment public-policy discourse? Just like every other aspect of cybersecurity, public-private partnerships are both advisable and inevitable. This paper has attempted to highlight areas where legal intervention might be needed so as to nudge the market to pursue more societally favorable policies. Table 1 below offers a menu of such legal interventions. This menu is non-exhaustive, however. I hope the paper is seen as a call for action, to encourage future works interested not only in the economics of cybersecurity risk distribution, but with the philosophy and political science around such rearrangements.

---

[294] Writing in 2001, Schneier believed that these actuarial challenges "will be a snap," suggesting that an industry that is capable of offering coverage for "satellite launches and the palate of wine critic Robert Parker," would have no problem handling hacking. Schneier, *supra* note 290.

TABLE 1. SUMMARY OF PROPOSED LEGAL INTERVENTIONS

	Cyber Terrorism & State-Sponsored Cyberattacks	Extortion Payments in Ransomware Attacks	Statutory Fines for Data Protection Violations
Non-Cyber Insurance Parallels	Terrorism Insurance and Government Backstops	Kidnap and Ransom (K&R) Insurance	Coverage for Punitive Damages in General Liability
Existing Jurisprudence & Discourse	1. Narrow interpretation of the "War Exclusion" 2. Debates in Congress around extending the Terrorism Insurance Program (TRIP) in 2020	Historical and comparative debates around prohibitions for insurance indemnification of extortion payments	Inconsistent case law around the theoretical justifications for and against insurance indemnification of punitive damages
Cyber-Specific Public Policy Considerations	Move towards tailored "State-Sponsored" and "Cyber Terrorism" Exclusions trigger growing ambiguity and an increasing gap in coverage for potential mega-losses	The scale, volume, and impact of ransomware attacks to society calls for a re-adjustment of public policy around dealing with extortion payments in ransomware cases	As fines are the primary enforcement mechanism for data protection, there is further justification for adopting a cautious approach to insuring such fines
Proposals for Legal Intervention	1. Promoting uniform language around exclusions 2. Developing both domestic and international legal evidentiary standards for cyber attribution 3. Extending TRIP, providing explicit coverage for acts of cyber terrorism and certain state-sponsored cyber attacks and encouraging other foreign nations to adopt a similar policy	1. Demand notification to and collaboration with law enforcement and/or Computer Emergency Readiness Team (US-CERT) prior to any indemnification 2. Establish interagency guidelines for case-by-case determinations of insurability, *e.g.*, prohibiting indemnification for the extortion payment where risk to life and loss of property is limited	Avoid an overbroad *per-se* rule on insurability (*e.g.*, GDPR fines are insurable/ uninsurable). Instead, adopt a presumption against coverage, subjecting analysis to questions surrounding: (a) the maturity of the regulation violated; (b) the scope and degree of culpability of the fined entity

LETTING YOUR PHONE TESTIFY: WHY THE FIFTH AMENDMENT SHOULD BE AN ABSOLUTE BAR TO COMPULSORY UNLOCKING OF SECURED SMARTPHONES

John P. Mears*

TABLE OF CONTENTS

---

* Juris Doctor Candidate, California Western School of Law, 2021; B.A. Political Science, Public Law Emphasis, University of California San Diego, 2018. For invaluable assistance and feedback on this comment throughout its creation, I would like to thank California Western professors Tabrez Ebrahim and Liam Vavasour. Thank you to my family and friends for their incredible and unwavering support throughout the research and writing process. This comment was made possible only through the support of these individuals and I will be eternally grateful!.

I. INTRODUCTION

My phone is my life. How many of us have heard someone say that? Our favorite photos, our intimate messages, our work lives, and so much more concentrated in one handheld device. Now imagine you are wrongfully accused of possessing and distributing child pornography. Your entire life will now be subject to the immense investigative powers of the government being brought to bear in an effort to reveal your alleged secrets. The government serves you with a subpoena and a court order forcing you to provide them with your passcode to unlock your phone. You refuse, not out of any concern of your own guilt, but because you have an incredibly rich library of personal and private information on your phone, everything from text messages with your significant other to private medical records. Rather than seeking another method to gain access to your phone, perhaps from a company that specializes in doing so, the government takes you to court asking the judge to hold you in contempt and imprison you if you continue to refuse. What do you do?

This is precisely the situation this article seeks to address by arguing that forcing a defendant or witness to unlock their own smartphone falls squarely within the Fifth Amendment privilege against self-incrimination. This argument does not suggest that law enforcement should be unable to gain access to secured smartphones. Rather, it emphasizes that state actors should not be able to compel individuals to provide their own passcodes and must find other means to gain access to these devices. Rather than using legal gymnastics to try to make forced unlocking an exception to the Fifth Amendment, the burden of finding and paying for a resource[1] to gain access to these devices should fall squarely upon the entity in the best position to bear it: the government.

The Fifth Amendment to the United States Constitution secures the privilege against self-incrimination which protects individuals from being forced to be a witness against themselves.[2] While this is a federally secured right, the United States Supreme Court has extended the privilege to apply to the states as well.[3] However, the real-world application of the privilege has

---

[1] Numerous tools exist for the government to use in endeavoring to unlock an individual's smartphone, perhaps one of the most well-known is Cellebrite. *See Advanced Unlocking & Extraction Services*, CELLEBRITE, https://www.cellebrite.com/en/cas-sales-inquiry/ (last visited April 5, 2021).

[2] WAYNE R. LAFAVE, 1 SUBSTANTIVE CRIMINAL LAW § 3.5(f) (3d ed. 2020).

[3] *Id.; see also* Malloy v. Hogan, 378 U.S. 1, 6 (1964) ("We hold today that the Fifth Amendment's exception from compulsory self-incrimination is also protected by the Fourteenth Amendment against abridgement by the states").

introduced a range of issues as to how and when the privilege can be applied.[4] To address these issues as they relate to the argument in this article, it is necessary to first lay the foundation of the privacy interests at stake when granting access to these devices. Therefore, Part II provides an overview of smartphone encryption and details the issues related to smartphone encryption and the importance of digital privacy today. Part III explains the Fifth Amendment issue and provides a detailed outline of the substantive law in this area. Part IV introduces the varying approaches of the case law in several states while showing the different ways that courts have treated smartphones secured with biometric security versus those secured with passcodes. Finally, Part V takes this collective information and argues that the Fifth Amendment should be an absolute bar to forcing individuals to unlock their smartphones. Part VI concludes.

A. Brief Summary of the Issue and Argument

The world today certainly looks very different than it did decades ago. Twenty years ago, perhaps none of us could have foreseen the technological world that we now find ourselves in. Many were happy to simply make a cellular phone call without the connection dropping. However, the devices we hold today measure mere inches, yet are capable of processing dramatically more information at rates many times faster than the first Apollo spacecrafts.[5] Due to the dramatic growth in these devices' capability and use, the world now looks very different than it did just fifteen years ago.[6] We now wake up to use phones with ultra-high-definition screens to send emails, place phone calls, send encrypted messages, access confidential documents and health records, access our banking records, video conference with friends and colleagues, and so much more.[7] Many people use their cameras to record the events of our daily lives and share them on platforms, sometimes in encrypted formats on some services.[8] We even use our phones' digital assistants to help

---

[4] *See* WAYNE R. LAFAVE ET AL., 1 CRIMINAL PROCEDURE § 2.10(a) (4th ed. 2020) (enumerating self-incrimination issues that have been considered by the Supreme Court).

[5] Tibi Puiu, *Your smartphone is millions of times more powerful than the Apollo 11 guidance computers*, ZME SCIENCE (Feb. 11, 2020), https://www.zmescience.com/science/news-science/smartphone-power-compared-to-apollo-432/.

[6] *See id.* (describing the major advancements in computing ability in the decades following man being sent to the moon).

[7] *Smartphone*, COMPUTER HOPE (Feb. 1, 2021), https://www.computerhope.com/jargon/s/smartphone.htm.

[8] *See, e.g.*, *WhatsApp Security*, WHATSAPP, https://www.whatsapp.com/security/ (last visited Apr. 1, 2021) (explaining that the company has "built end-to-end encryption into the app").

us perform daily tasks, often allowing the device's microphones to remain always-on in order to activate these digital assistants by simply speaking a short word or phrase.[9] Indeed, our phones today "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[10]

However, these devices have increasingly reduced digital privacy in order to provide greater convenience. The basis of this ever-increasing intrusion is informed consent to access the types of data which companies seek. This is a subject being addressed by legislation in many states, including California.[11] This paper examines the extent to which law enforcement may force individuals to unlock their devices for investigative purposes. This subject has bred numerous conflicting court opinions across the several states[12] and scholarly articles discussing those approaches.[13] However, scholars have not considered whether the Fifth Amendment privilege against self-incrimination should be an absolute bar to the forced unlocking of smartphones. As a result, this article argues that we must consider the role of the Fifth Amendment in police investigations due to the limitations of the law, the law's failure to maintain pace with changes in technology, and as a matter of public policy.

---

[9] *See* Lisa Eadicicco, *Siri is always listening. Are you OK with that?*, BUSINESS INSIDER (Sept. 9, 2015), https://www.businessinsider.com/siri-new-always-on-feature-has-privacy-implications-2015-9 (discussing how Apple has introduced passive listening technology as "a standard feature for Siri and the iPhone"); *see also Google Assistant*, GOOGLE, https://assistant.google.com (last visited Mar. 18, 2021) (advertising how Google Assistant may be operated within Google products by a user merely saying "Hey Google . . .").

[10] Riley v. California, 573 U.S. 373, 393 (2014). *See also* United States v. Dijbo, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015) (indicating that a modern smartphone can contain the "combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually, and sometimes even sexually, in the owner's life").

[11] *2020 Consumer Privacy Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

[12] *See generally*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012) (holding decryption of the device would trigger Fifth Amendment protection"). *But see, e.g.*, State v. Andrews, 243 N.J. 447, 234 A.3d 1254 (2020) (holding that neither federal nor state protections against compelled disclosure apply to decryption of devices).

[13] *See, e.g.,* Orin S. Kerr*, Essay, Compelled Decryption and the Privilege Against Self-Incrimination,* 97 TEX. L. REV. 767 (2019) (arguing that the Fifth Amendment does not bar the government from compelling decryption when the suspect knows the passcode to the device). *But see, e.g.*, Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEXAS L. REV. ONLINE 63 (2019) (arguing that the government can only compel decryption when it knows the suspect already possesses the files and can identify them).

II. SMARTPHONES AND DIGITAL ENCRYPTION

To begin this discussion, it is important to set a foundation of the current security and privacy protections that exist with respect to consumer smartphones. In its most basic form, encryption can be defined as the "cryptographic transformation of data ('plaintext') into a form ('ciphertext') that conceals the data's original meaning to prevent it from being known or used."[14] Furthermore, it is important to clarify that "data" as used in the context of this article is broadly defined as "information in digital form that can be transmitted or processed."[15] While it is helpful to have knowledge of this basic information moving forward, a full discussion of encryption and all its intricacies is beyond the scope of this article.

Importantly, since late 2014, both Apple's iPhone operating system and Google's Android operating system have included default options to enable full disk encryption.[16] Full disk encryption technology is used to protect all the data stored on a device, including the device's operating system as well as any other user data.[17] Access to this data requires the user's password, passcode, or other authentication instrument in order to gain access to the device.[18] Therefore, once the encryption is enabled, the information on the device is inaccessible without specialized decryption tools or the user's authentication.[19] This process is known as decryption.[20]

---

[14] Computer Security Resource Center, *Encryption*, U.S. DEP'T OF COMMERCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, INFORMATION TECHNOLOGY LABORATORY, https://csrc.nist.gov/glossary/term/encryption (last visited February 12, 2021).

[15] *Data*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/data.

[16] Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com /news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/; Joe Miller, *Google and Apple to introduce default encryption*, BBC NEWS (Sept. 19, 2014), https://www.bbc.com/news/technology-29276955.

[17] *Guide to Storage Encryption Technologies for End User Devices: Recommendations of The National Institute of Standards and Technology*, U.S. DEP'T OF COMMERCE, § 3.1.1 (2007); Antwanye Ford & LaTia Hutchinson, *Full disk encryption: do we need it?*, CSO (Jan. 16, 2018), https://www.csoonline.com/article/3247707/full-disk-encryption-do-we-need-it.html.

[18] U.S. Dep't of Commerce, *supra* note 17; Ford & Hutchinson, *supra* note 17.

[19] Alison Grace Johansen, *What is encryption and how does it protect your data?,* NORTON (July 24, 2020), https://us.norton.com/internetsecurity-privacy-what-is-encryption.html (explaining that "Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key.").

[20] Isha Upadhyay, *What is Decryption, An Important Guide in 5 Points*, JIGSAW ACADEMY (Jan. 23, 2021), https://www.jigsawacademy.com/blogs/cyber-security/decryption/.

A. The Apple-FBI Conflict

The issues surrounding the government's ability to gain access to encrypted smartphones were thrust into public view when Apple publicly resisted a subpoena seeking to gain access to the iPhone owned by Syed Rizwan Farook in early 2016.[21] Farook and his wife were being investigated as part of a San Bernardino, California, shooting spree that killed 14 people on December 2, 2015.[22] Both were killed in a shootout with police,[23] meaning that Farook could not consent to unlock his phone. Accordingly, the issue became whether Apple could be forced to provide the FBI access to the passcode-protected iPhone by altering its operating system to create a "backdoor" into the device.[24]

The United States District Court for the Central District of California ordered Apple to assist the FBI in gaining access to the device on February 16, 2016.[25] This order was followed by over a month of heated public exchanges between Apple, the FBI, and the Justice Department with each entity trying to win over the public in their fight over privacy and government access.[26] Ultimately, the FBI withdrew its case to compel Apple to provide access to Farook's iPhone.[27] In a subsequent filing, the FBI claimed that it had found an alternate third party to assist them in gaining access to the iPhone.[28] The FBI, however, refused to disclose that third party.[29]

---

[21] *Breaking Down Apple's iPhone Fight with the U.S. Government*, N.Y. TIMES (Mar. 21, 2016), https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html.

[22] Adam Nagourney, Ian Lovett & Richard Pérez-Peña, *San Bernardino Shooting Kills at Least 14; Two Suspects are Dead*, N.Y. TIMES (Dec. 2, 2015), https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html.

[23] *Id.*

[24] Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[25] *Matter of Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016).

[26] Katie Benner & Matt Apuzzo, *U.S. Says It May Not Need Apple's Help to Unlock iPhone*, N.Y. TIMES (Mar. 21, 2016), https://www.nytimes.com/2016/03/22/technology/apple-fbi-hearing-unlock-iphone.html. *Filing to Drop Case Against Apple*, N.Y. TIMES (Mar. 28, 2016), https://www.nytimes.com/interactive/2016/03/28/technology/document-us-filing-dropping-apple-case.html.

[27] Benner & Apuzzo, *supra* note 26.

[28] *Filing to Drop Case Against Apple*, *supra* note 26.

[29] Eric Lichtblau & Katie Benner, *With Finality, F.B.I. Opts Not to Share iPhone-Unlocking*

Nevertheless, Apple's fight with the FBI and the Justice Department resulted in extensive coverage and public attention.[30] More importantly, this coverage exposed many Americans to the conflict between Apple and the government over access to secured smartphones for the first time.

B. The Importance of Digital Privacy

This discussion has become more important today, as many of us spend a significant portion of our lives in front of our smartphones. In fact, a 2019 study from market research company eMarketer found that Americans spent more time on their phones than they did watching television.[31] Smartphone usage accounted for an overwhelming majority of that time, with the average smartphone user spending nearly three hours a day on their device.[32] Since the start of the shutdowns caused by the COVID-19 pandemic in March 2020, some studies have shown an even greater increase in smartphone usage due to social distancing efforts.[33] Perhaps not surprisingly, these studies have shown many spend significantly more time with their devices to communicate via video calls, send text messages, and engage on social media.[34] However, in understanding the importance of digital privacy when it comes to smartphone usage, it's important to also understand what users are doing with their devices.

A 2015 study by the Pew Research Center revealed data on the usage

---

Method, N.Y. TIMES (Apr. 27, 2016), https://www.nytimes.com/2016/04/28/technology/with-finality-fbi-opts-not-to-share-iphone-unlocking-method.html.

[30] *Id*.

[31] Yoram Wurmser, *US Time Spent with Mobile 2019: Smartphones Gain Minutes, but New Challenges Emerge*, EMARKETER (May 30, 2019), https://www.emarketer.com/content/us-time-spent-with-mobile-2019.

[32] *Id.* (finding that the average US adult spent 2 hours, 55 minutes per day on a smartphone in 2019, which was a nine-minute increase from 2018.)

[33] *See* Travis Andrews, *Our iPhone weekly screen time reports are through the roof, and people are 'horrified,'* WASH. POST (Mar. 24, 2020), https://www.washingtonpost.com/technology/2020/03/24/screen-time-iphone-coronavirus-quarantine-covid/ (detailing increased smartphone usage brought on by quarantining and related measures during the COVID-19 pandemic); s*ee also Survey Says: Cell Phone Usage Impacted During COVID-19*, TWIGBY (Jun. 17, 2020), https://www.twigby.com/blog/survey-says-cell-phone-usage-impacted-during-covid-19/?utm_source=pr%20newswire&utm_medium=release&utm_campaign=may_2020_survey (finding that nearly forty percent of those surveyed reported increased cell phone usage during the COVID-19 pandemic).

[34] *See* Andrews, *supra* note 33; *see also Survey Says: Cell Phone Usage Impacted During COVID-19*, *supra* note 33.

behaviors of smartphone users.[35] Specifically, it found that 62 percent of users had used their phone to look up health-related information, 57 percent accessed their banking information, and 40 percent looked up government services or information.[36] Other uses included accessing news and educational content, getting directions, submitting job applications, and more.[37] Nearly six years have passed since the release of this study and behaviors certainly may have changed with the advent of new devices and services. For example, the Health app on iPhone allows users to take data from a multitude of different sources, including data collected from their Apple Watch, and create a complete picture of their health.[38] Users can even incorporate health records from their participating medical provider into the application to see such records alongside their other data. Users can also create a "Medical ID" containing pertinent health information to be used in emergencies.[39]

The amount of information collected on our devices doesn't even begin to address the private information contained within our messages located across the multitude of messaging apps and services in existence.[40] Nor does it address those who use their devices for business purposes and store confidential business information. Finally, it doesn't address those in legal, educational, or health institutions who may have legally privileged and protected data of others on their devices.[41] Unlocking a smartphone today is essentially kicking the door wide open to a massive trove of information, much of which is personal, private, and potentially privileged.

Encryption serves to protect the security of this information,[42] much like a lock on the door to a home protects the documents, items, and information located inside. However, unlike the door to a home, a phone can't simply be

---

[35] Aaron Smith, *Chapter Two: Usage and Attitudes Toward Smartphones*, PEW RSCH. CTR. (Apr. 1, 2015), https://www.pewresearch.org/internet/2015/04/01/chapter-two-usage-and-attitudes-toward-smartphones/.

[36] *Id.*

[37] *Id*.

[38] *Your health, from head to toe.* APPLE, INC. https://www.apple.com/ios/health/ (last visited March 12, 2021).

[39] *Id.*

[40] *See* H. Tankovska, *Most popular global mobile messenger apps as of January 2021, based on number of monthly active users*, STATISTA (last visited Feb. 10, 2021), https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (detailing number of monthly active users for six popular messaging apps).

[41] *See, e.g.*, *Healthcare*, APPLE, INC., https://www.apple.com/healthcare/ (last visited March 26, 2021) (detailing how Apple products and apps are being used by healthcare providers to provide treatment and conduct research).

[42] Comput. Sec. Res. Ctr., *supra* note 14.

broken into with a battering ram. Instead, it is protected with a passcode (or password) or biometric authentication methods. For example, on compatible devices, Apple's iPhone gives users the option to use fingerprint authentication with their Touch ID system[43] or facial authentication using their Face ID system.[44] Touch ID does not save an image of the user's fingerprint but instead converts the image to data, collected by the device's sensor, which is then used to match against future unlock attempts.[45] Similarly, the Face ID system does not save a simple image of the user's face but instead creates a three-dimensional geometric model of the user's face using a variety of different cameras and sensors. The model is then matched against future unlock attempts.[46]

III. THE FIFTH AMENDMENT ISSUES

The Fifth Amendment to the United States Constitution provides, in pertinent part, that "[n]o person shall be . . . compelled in any criminal case to be a witness against himself." The essential foundation of the privilege was laid down in an opinion authored by Chief Justice John Marshall in the historic trial of Aaron Burr, a former Vice President of the United States, for treason.[47] Under Justice Marshall's rule, a person can only be compelled to answer a request where "it is clear that no possible answer could be incriminating."[48] Furthermore, "[a]n incriminating answer does not mean a complete confession to the crime; the admission of any facts linking the witness to criminal activity is sufficiently incriminating."[49] Perhaps most importantly, after a witness asserts the privilege, a judge is prohibited from continuing to inquire about the witness's assertion "if there is some chance that the answer will supply some proof or link in the evidence against the witness."[50]

Due to the potential and unacceptable risk of disclosing privileged information, it is entirely the decision of the witness as to whether "the answer is incriminating and the court must respect the witness' decision."[51]

---

[43] *About Touch ID advanced security technology*, APPLE, INC., (Sept. 11, 2017), https://support.apple.com/en-us/HT204587.

[44] *About Face ID advanced technology*, APPLE, INC., (Sept. 14, 2021), https://support.apple.com/en-us/HT208108.

[45] *About Touch ID advanced security technology*, *supra* note 43.

[46] *About Face ID advanced technology*, *supra* note 44.

[47] DAVID M. NISSMAN & ED HAGEN, *LAW OF CONFESSIONS* § 3:4 (2d ed. 2020).

[48] *Id*.

[49] *Id*.

[50] *Id*.

[51] *Id*.

In accordance with this rule, many courts across the country have noted that, "the trial judge should not speculate about or predict the likelihood of prosecution in relation to an assertion of the constitutional privilege against self-incrimination."[52] However, the witness asserting the privilege "must be confronted with 'substantial and "real," and not merely trifling or imaginary, hazards of incrimination.'"[53] Therefore, compelling a person to give their name to an officer during a stop where no real threat of prosecution exists does not violate the Fifth Amendment privilege.[54]

The phrase "privilege against self-incrimination" is frequently used to describe the Fifth Amendment privilege. However, as the Supreme Court has made clear, "the term 'privilege against self-incrimination' is not an entirely accurate description of a person's constitutional protection against being 'compelled in any criminal case to be a witness against himself.'"[55] Additionally, "[t]he word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character."[56]

Generally, a person seeking to invoke the benefit of Fifth Amendment protections must establish three main elements: (1) compulsion, (2) incrimination, and (3) a testimonial communication or act.[57] First, while no universally accepted definition for compulsion is available in the context of the Fifth Amendment,[58] one proposed clear meaning is "[a]n official undertaking to induce a witness to provide evidence by threat of punitive sanctions."[59] Second, incrimination may be broadly defined as a situation where "an individual is asked to produce something or give an answer which could then support a conviction of that individual, or even lead to a chain of evidence that could be used to prosecute that individual for a crime."[60] However, a precise definition or meaning for what made a particular

---

[52] Carter v. United States, 684 A.2d 331, 336 (D.C. 1996).

[53] *The trial of Aaron Burr*, *supra* note 47 (citing United States v. Apfelbaum, 445 U.S. 115, 128 (1980)).

[54] *See* Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt County, 542 U.S. 177, 190–91 (2004) (holding that identifying oneself during a police stop does not violate the Fifth Amendment unless there is a reasonable belief of self-incrimination).

[55] United States v. Hubbell, 530 U.S. 27, 34 (2000).

[56] *Id*.

[57] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–47 (11th Cir. 2012).

[58] Lawrence Rosenthal, *Compulsion*, 19 U. PA. J. CONST. L. 889, 893 (2017).

[59] *Id.* at 908.

[60] Adam Herrera, Comment, *Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free From Self-Incrimination*, 66 UCLA L. REV. 778, 789 (2019) (citing Hoffman v. United States, 341 U.S. 479, 486 (1951)).

communication or act "testimonial" was more elusive until the U.S. Supreme Court heard *Doe v. United States*.[61]

A. The "Testimonial" Limitation

In *Doe*, the United States government had begun a grand jury investigation into the target, named only as John Doe, on charges of fraudulent manipulation of oil cargoes and receipt of unreported income.[62] Doe was served with a subpoena asking him to produce bank records relating to transactions at three different off-shore accounts located in the Cayman Islands and Bermuda.[63] Doe produced some of the bank records when asked to appear before the grand jury, but he refused to answer whether he had others by asserting his Fifth Amendment privilege.[64]

The United States, had also served the foreign banks with subpoenas, with which the banks refused to comply, citing the need for the customer's consent under their governments' laws.[65] So, the United States then sought to have Doe ordered to sign disclosure forms.[66] The district court denied the motion finding that signing the disclosure would violate Doe's Fifth Amendment privilege.[67] However, the Fifth Circuit reversed and remanded, noting that signing the disclosures "did not have testimonial significance."[68, 69]

At the U.S. Supreme Court, the main question became whether the act of executing these disclosure forms would be "testimonial" and therefore protected under the Fifth Amendment.[70] Doe argued that the testimonial requirement would be met in any case where the information disclosed could

---

[61] Herrera, *supra* note 60, at 789–92.

[62] Doe v. United States, 487 U.S. 201, 202 (1988).

[63] *Id.*

[64] *Id.* at 203.

[65] *Id.*

[66] *Id.*

[67] *Id.* at 205–06.

[68] *Id.* at 205.

[69] The Court in *Doe* also made clear that the foreign bank records the government sought and the foreign bank's disclosure of them would not be protected under the Fifth Amendment privilege. *Id.* at 206; *see* Fisher v. United States, 425 U.S. 391, 396–98 (1976) (articulating that "Fifth Amendment privilege is [] not violated by summonses" that are directed to artificial entities). Similarly, here, discovery of the underlying information located on the smartphone would not be protected by the Fifth Amendment privilege. Therefore, nothing is preventing the government from gaining access to a person's smartphone by means other than the forced disclosure of their passcode or biometric information to unlock the device.

[70] *Doe*, 487 U.S. at 207.

be used to further a criminal investigation of the witness.[71] However, the Court recognized that this test would essentially lead to all statements which have any sort of content significance to be barred by the Fifth Amendment privilege.[72] In rejecting Doe's proposed definition, the Court held that "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[73]

This rule was in line with previous case law finding that some acts, though they may be incriminating, fall outside the scope of the privilege.[74, 75] Importantly, the Court said, "it is the 'extortion of information from the accused;' the attempt to force him 'to disclose the contents of his own mind,' that implicated the Self-Incrimination Clause."[76] Additionally, the Court rejected Doe's arguments that this definition of "testimonial" would result in the Government having power to essentially force people to assist in their own prosecution.[77] Oral and written statements would very rarely *not* convey information or otherwise assert facts, and would thus often be protected by the privilege.[78] Additionally, the Court noted, there are other provisions which, in addition to the privilege against self-incrimination, should continue to ward off any abusive investigative techniques by the government.[79]

Using this rule, the Court found that the disclosure form was not "testimonial" because it did not identify the relevant banks themselves or even identify a specific account.[80] Therefore, the government was still forced to locate the banks and accounts themselves, with no assistance from Doe.[81] The disclosure form was only one wherein Doe consented to disclosure of

---

[71] *Id.* at 207–08.

[72] *Id.* at 208.

[73] *Id.* at 210.

[74] *Id.*

[75] The Supreme Court noted several examples of potentially incriminating acts that were testimonial but would not be protected by the privilege. Specifically, "a suspect may be compelled to furnish a blood sample; to provide a handwriting exemplar, or a voice exemplar; to stand in a lineup; and to wear particular clothing." *Id.* (internal citations omitted). The Court noted that "in each of those cases, . . . the suspect was not required to 'disclose any knowledge he might have,' or 'to speak his guilt.'" *Id.* at 211.

[76] *Id.* (internal citations omitted).

[77] *Id.* at 213.

[78] *Id.* at 213–14.

[79] *Id.* at 214 n.13 (internal citations omitted) (noting that these additional provisions included the Fourth Amendment's protection against unreasonable searches (particularly of the home), the attorney-client privilege, as well as the Due Process Clause's "limitations on the government's ability to coerce individuals into participating in criminal prosecution.").

[80] *Id.* at 219.

[81] *Id*. at 215.

potentially existent accounts in his control, under which the *bank* had to determine whether Doe had the right to withdraw.[82] This consent form, thus, did not "relate a factual assertion or disclose information."[83] The government, working with the bank, was still forced to find the accounts, identify them as Doe's, and ensure that Doe could exercise the right to withdraw.[84]

This is an important distinction moving forward. The government cannot simply force suspects to provide them with information that would aid in the suspects' prosecution. They must locate the information by their own efforts and only if a communication does not "relate a factual assertion or disclose information" can the government overcome an assertion of the Fifth Amendment privilege related to gaining access to the information sought.[85]

B. The Foregone Conclusion Exception

Even if a communication is found to be testimonial, it still may not be protected by the Fifth Amendment privilege if the government can establish the so-called foregone conclusion exception.[86] Under this exception,

> an act of production is not testimonial—even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials—if the Government can show with "reasonable particularity" that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a "foregone conclusion."[87]

It is important to emphasize that this applies to the act of production itself, and not the discovery of the underlying information.[88] In essence, the exception applies when the testimonial act itself "adds little or nothing to the sum total of the Government's information."[89] In those cases, the foregone conclusion exception will apply and the Fifth Amendment privilege will not

---

[82] *Id.* at 216–18.

[83] *Id.* at 210–19.

[84] *See id.* at 215–16.

[85] *See id.* at 210–19.

[86] *See* Fisher v. U.S., 425 U.S. 391, 411–14 (1976).

[87] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012).

[88] *See id.* at 1342.

[89] *Fisher*, 425 U.S. at 411.

protect against the compelled act.[90] In order to meet this exception, the government must be able to (1) independently prove the documents they are seeking exist and are within the person's possession; (2) "independently verify that the documents are what the government claims that they are; and (3) must be prepared to authenticate the documents without resort to the target's testimony."[91] Currently, the approaches to handling assertions of the foregone conclusion exception with respect to unlocking secured smartphones have differed.[92]

The Eleventh Circuit Court of Appeals addressed the issue in a 2012 child pornography case involving a grand jury subpoena forcing a person to deliver the unencrypted contents of computer hard drives.[93] Doe, the defendant, refused to deliver the decrypted hard drives by asserting his Fifth Amendment privilege, and the district court held him in contempt.[94] The Court of Appeals reversed, finding that the government failed to produce sufficient evidence that they knew the files existed, that they were located on the drives, or that Doe was capable of accessing them.[95] The court noted that it is insufficient for the government to simply argue that something is *capable* of storing massive amounts of information, and therefore *may* also contain incriminating information.[96] "Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all."[97]

These elements, applied to secured smartphones, place a substantial hurdle in the path of the government when seeking to overcome a person's assertion of the Fifth Amendment privilege. Without the cooperation of the person asserting the privilege, it is difficult to see under what circumstances the government will be able to prove, with *particularity*, that they know the files they seek exist; that the files are located on the smartphone; and that the person is capable of accessing the files. This difficulty is an essential part of the argument to this article, which will be expanded upon in more detail below.

---

[90] *See id.* at 411–14. *See also* Orin S. Kerr*, Essay, Compelled Decryption and the Privilege Against Self-Incrimination,* 97 TEXAS L. REV. 767, 773 (2019).

[91] NISSMAN, *supra* note 47, § 3:19 (discussing the "foregone conclusion" exception and compelling the production of computer or "smart phone" passwords).

[92] *Id.*

[93] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012).

[94] *Id.* at 1338.

[95] *Id.* at 1346–47.

[96] *Id.* at 1347.

[97] *Id.*

IV. CURRENT APPROACHES TO THE ISSUE OF FIFTH AMENDMENT PROTECTION OF SECURED SMARTPHONES

Lastly, it is helpful to understand the current case law and arguments on the issue. Since 2016 and particularly since the highly publicized Apple–FBI case discussed previously, a substantial split has arisen among case law in different jurisdictions.[98] Courts and legal scholars across the country have debated whether and under what circumstances people can be compelled to unlock their devices.[99] Due to this extensive library of case law and arguments, a survey of it is beyond the scope of this article.[100] Therefore, each section below will provide a brief sample of existing approaches that case law and legal scholars have taken.

A. Passcode Authentication Cases

Most recently, the Court of Appeals of Utah addressed this issue in *State v. Valdez*.[101] In that case, the defendant was convicted by a jury on charges of kidnapping, robbery, and aggravated assault.[102] However, his conviction came only after the trial court allowed guilt to be implied from the defendant's refusal to unlock his phone after asserting his Fifth Amendment privilege.[103] The Court of Appeals addressed the question of whether this adverse inference against Valdez was a violation of his Fifth Amendment rights.[104]

First, the Utah court found that Valdez's statement was testimonial, particularly after having first been asked by the police to provide his passcode. The court noted that "the government was asking Valdez to provide the equivalent of 'the combination to [his] wall safe,' a request that asked Valdez to reveal to the government the 'contents of his own mind.'"[105] Importantly, however, the court noted that this situation of communicating a passcode to an officer was a different situation from a suspect being asked to

---

[98] STEVE C. POSNER, MODERN PRIVACY & SURVEILLANCE LAW § 2.22 (2020).

[99] *Id.*

[100] *See, e.g.*, Jesse Coulon, Comment, *Annual Survey of Federal En Banc and Other Significant Cases: Privacy, Screened Out: Analyzing The Threat To Individual Privacy Rights And Fifth Amendment Protections In State V. Stahl*, 59 B.C. L. REV. E. SUPP. 225 (2018).

[101] State v. Valdez, 482 P.3d 861, 865 (UT App. 2021).

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.* at 873 (quoting Doe v. United States, 487 U.S. 201, 219 (Stevens, J., dissenting)).

hand over an unlocked smartphone.[106]

Next, the court found that the foregone conclusion exception did not apply, primarily because the court noted it was unclear how or even whether it should be applied in the context of smartphones.[107] Additionally, the court noted that the U.S. Supreme Court opinion which created the exception, *Fisher v. U.S.*, was issued decades before the advent of modern smartphones. Furthermore, the opinion cited the multitude of other cases emphasizing the limitations of the foregone conclusion exception.[108]

The court proceeded to find that the adverse inference imposed upon Valdez here was a Fifth Amendment violation and was not harmless error.[109] Accordingly, the court reversed Valdez's conviction.[110] Most importantly, however, *Valdez* is not an isolated case; multiple cases from other states have reached similar conclusions.[111]

In contrast to Valdez, other cases have found that the Fifth Amendment privilege does not extend to the disclosure of smartphone passcodes.[112] One of the most recent and on-point cases reaching this conclusion comes from the Supreme Court of New Jersey in *State v. Andrews*.[113] There, the defendant, Andrews, was a former county sheriff's officer who allegedly helped the subject of a state narcotics investigation avoid prosecution.[114] Andrews was indicted for official misconduct, hindering the apprehension or prosecution of another person, and obstructing the administration of the law or other government function.[115]

---

[106] *Id.* at 872.

[107] *Id.* at 875–76.

[108] *Id.* at 874.

[109] *Id.* at 878.

[110] *Id.*

[111] *See* Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (finding that the Fifth Amendment protected disclosure of a passcode but not a fingerprint); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1349 (11th Cir. 2012) (holding decryption of the device would trigger Fifth Amendment protection); Garcia v. State, 302 So. 3d 1051, 1057 (Fla. Dist. Ct. App. 2020), *rev. granted*, No. SC20-1419, 2020 WL 7230441 (Fla. Dec. 8, 2020) (holding that oral disclosure of a passcode is protected under the Fifth Amendment); Seo v. State, 148 N.E.3d 952, 953 (Ind. 2020) (holding that forced smartphone unlocking violates Fifth Amendment rights).

[112] *See* United States v. Apple Mac Pro Comput., 851 F.3d 238, 247–48 (3d Cir. 2017) (finding the foregone conclusion exception applied to allow for the disclosure of a computer password); Commonwealth v. Jones, 117 N.E.3d 702, 717–18 (Mass. 2019) (finding the foregone conclusion exception applied to force the production of a passcode to defendant's smartphone).

[113] State v. Andrews, 234 A.3d 1254, 1259 (N.J. 2020).

[114] *Id.*

[115] *Id.* at 1261.

In its analysis of the Fifth Amendment issue, the court emphasized the finding of *Doe*[116] that the Fifth Amendment did not serve as "an absolute bar to a defendant's forced assistance of the defendant's own criminal prosecution."[117] However, the court also detailed the significant splits in jurisprudence across states as to the Fifth Amendment issues of compulsory unlocking of smartphones.[118] Ultimately, the court found that while disclosure of the passcodes would be testimonial, its testimonial value would be minimal,[119] allowing for a clear application of the foregone conclusion exception. The court found that the mere fact that the state established that the passcodes existed and that several phones were in Andrews's possession at the time of seizure were sufficient to establish the applicability of the foregone conclusion exception. This is a narrow reading of the exception and it is a dangerous proposition when the compelled act involves giving access to the massive amount of information a smartphone may hold about a person's life.

Importantly, however, the court also stated their concern as to a distinction drawn by some courts to protect the disclosure of passcodes but not to protect against compelled unlocking by biometric authentication.[120] Additionally, the court also recognized that this distinction makes even less sense where most phones require a passcode before biometric authentication can be used.[121]

B. Biometric Authentication Cases

In *Commonwealth v. Baust*, the defendant Baust was indicted on charges of strangulation causing wound or injury wherein the state sought to compel production of his passcode or fingerprint to gain access to his smartphone.[122] The court addressed and utilized a distinction drawn between compelled unlocking of a device by passcode versus doing so by biometric authentication.[123] The court acknowledged the passcode should be protected as testimonial, and that the foregone conclusion exception should not apply "because it is not known outside of [the] Defendant's mind."[124] However,

---

[116] Doe v. United States, 487 U.S. 201, 213 (1988).
[117] State v. Andrews, 234 A.3d at 1266.
[118] *Id.* at 1269–73.
[119] *Id.* at 1274.
[120] *Id.*
[121] *Id.*
[122] Commonwealth v. Baust, 89 Va. Cir. 267, 267–68 (Va. Cir. Ct. 2014).
[123] *Id.* at 2–4.
[124] *Id.* at 9.

likening the unlock of a phone by fingerprint to other simple physical characteristics, the court found that Baust's use of his fingerprint would not be testimonial and therefore would not be protected under the Fifth Amendment.[125] The court focused on the fact that the use of the fingerprint does not involve the defendant's mental processes and also "does not require [the] defendant to 'communicate any knowledge' at all."[126]

On the other hand, in a case from just last year, the court in *U.S. v. Wright* found that the unlocking of a defendant's smartphone with their face was a testimonial act and was protected by the Fifth Amendment privilege.[127] This case involved a prosecution for possession of child pornography.[128] The court ultimately concluded that because there is no functional difference between unlocking a device using a biometric method rather than a passcode, the two should be similarly treated as testimonial and therefore protected.[129] The court also emphasized that a crucial difference exists between using your face to unlock your phone and allowing your fingerprint DNA to be taken, particularly in the case of a prosecution for possession of child pornography.[130] Unlocking the device indicates that the person owns or at least has some control over the phone, which would therefore satisfy the element of possession in proving that the defendant committed the crime.[131]

These cases are not isolated. Courts across the country have grappled with the same issue regarding biometric authentication, most of them adopting similar arguments in reaching one conclusion or the other.[132]

---

[125] *Id* at 9.

[126] *Id.* at 9–10.

[127] United States v. Wright, 431 F. Supp. 3d 1175, 1188 (D. Nev. 2020).

[128] *Id.* at 1179.

[129] *Id.* at 1187.

[130] *Id.* at 1187–88.

[131] *Id.* at 1188.

[132] *Compare In re* Search of a Residence in Oakland, California, Case No. 19MJ70053KAW1JD, 2019 WL 6716356, at *2–3 (N.D. Cal. Dec. 10, 2019) (finding that the compelled production of biometric information was testimonial under the Fifth Amendment privilege in response to a warrant seeking to compel an individual to unlock the device by means of facial recognition or fingerprint authentication); *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073–74 (N.D. Ill. 2017) (finding the compelled unlocking by fingerprint testimonial and therefore protected); United States v. Maffei, Case No. 18-CR-00174-YGR-1, 2019 WL 1864712, at *6 (N.D. Cal. Apr. 25, 2019) (finding that forcing the defendant to provide a passcode was testimonial, but ultimately that it did not violate the Fifth Amendment because it was not compelled, though the district court still suppressed the defendant's statement of her passcode for violating her Fourth and Sixth Amendment rights), *with* Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793–94 (D. Idaho 2019) (finding that a forced application of a fingerprint to unlock a device was not testimonial for Fifth Amendment purposes); United

C. Recent Arguments to Address the Issue

One approach to assessing the Fifth Amendment privilege with passcode-protected devices comes from Professor Orin Kerr who has written on the subject in order to establish a universal rule that may be applied to passcode-protected devices.[133] Professor Kerr argues that the privilege should apply unless the government can establish the foregone conclusion exception by showing that the person knows the passcode to the device.[134] Furthermore, Professor Kerr emphasizes that providing too much protection for individuals asserting the privilege may "shift the balance of power too much against the public interest in investigating crime."[135] Others have similarly argued that courts that protect and uphold the Fifth Amendment rights of individuals in these cases are having a chilling effect on law enforcement.[136] However, Professor Kerr acknowledges that several other options allow for the government to gain access to a suspect's encrypted smartphone, even if they may not be the most convenient.[137] Professor Kerr's argument does not stand in isolation, as legal scholars have taken several positions on the issue.[138]

For instance, Adam Herrera argues that the security method a person chooses should not determine whether or not they can assert the privilege.[139] Rather, biometric authentication methods, like those used on Apple's iPhone X and later versions, should receive the same level of protection.[140] Notably,

---

States v. Anthony Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019) (finding "that any implicit inference that can be drawn from a biometric unlock procedure is not of testimonial significance.").

[133] Kerr, *supra* note 13.

[134] *Id.* at 783.

[135] *Id.* at 770.

[136] *See, e.g.*, Kristen M. Jacobsen, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement*, 85 Geo. Wash. L. Rev. 566 (2017).

[137] Kerr, *supra* note 13, at 795.

[138] *See* Laurent Sacharoff, *supra* note 13. *See generally,* Note*, "Your Device Is Disabled": How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected By The Fifth Amendment Privilege*, 53 VAL. U.L. REV. 427 (2019); Madeline Leamon, Note, *Unlocking The Right Against Self-Incrimination: A Predictive Analysis of 21st Century Fifth Amendment Jurisprudence*, 64 WAYNE L. REV. 583 (2019); Parya Mahmoudi, *Face ID, Touch ID, And Biometric Passwords: A Fifth Amendment Privilege*, 97 DENV. L. REV. ONLINE 15 (2019); Richard G. Cole III, Comment, *The Constitutional Insecurity of Secured Smartphones: "Unlocking" The Current Fourth and Fifth Amendment Safeguards Protecting Secured Smartphones From Law Enforcement Searches*, 39 U. LA VERNE L. REV. 173 (2018).

[139] Herrera, *supra* note 60, at 807–08.

[140] *Id.*; *see also About Face ID advanced technology, supra* note 44.

as adoption of these biometric technologies continues to grow, it will become even more important to provide clarity on the level of Fifth Amendment protection offered for those who choose to use those methods.[141] In contrast, this article asserts that any distinction between biometric or passcode methods is not only unnecessary but also irrelevant, as a person should never be compelled to unlock their device after asserting the Fifth Amendment privilege against self-incrimination.

V. ARGUMENT: THE FIFTH AMENDMENT PRIVILEGE AS AN ABSOLUTE BAR TO COMPULSORY UNLOCKING

With this extensive legal history and framework in mind, the underpinnings of this article's argument should be clear. As noted at the outset, this article does not advocate that the government should never be able to access a secured smartphone to secure evidence for prosecution. Such an argument would be contrary to a system of law and justice that recognizes the need for a strong investigative process in criminal cases. However, in recognition of our system of law and justice, this article emphasizes the need to focus on the constitutional safeguards guaranteed to citizens who are subject to invasive investigative procedures.

This article focuses on the importance of placing the burden of unlocking a device on the government rather than on the constitutionally-protected defendant. The government is in the best position to find a company or entity that can assist it in unlocking a person's device. This may be a longer and more expensive process. Consequently, it may simply be easier and cheaper to have the defendant unlock their device. However, the primary focus of our criminal justice system is not and should not be reduced to simplicity and cost. The constitution demands more.

There is a substantial risk that this rule would impact criminal investigations. Will prosecutors never be able to gain access to a person's digitally stored information? Of course not. In addition to the government using hardware or software solutions to gain access to a device without the suspect's assistance, this rule does not limit the government's ability to obtain any digital information retained in cloud storage services or as part of device backups by third parties like Apple or Google.[142] Many people back up their devices to cloud services to avoid losing their information,[143] and nothing in

---

[141] Herrera, *supra* note 60, at 782.

[142] *How to back up your iPhone, iPad, or iPod touch*, APPLE, INC., https://support.apple.com/en-us/HT203977 (last visited Apr. 8, 2021); *Backup or restore data on your android device*, GOOGLE, https://support.google.com/android/answer/2819582?hl=en (last visited Apr. 8, 2021).

[143] Tom Coughlin, *Where do you backup data?*, FORBES (July 24, 2019, 2:33 PM),

this rule prevents the government from issuing a subpoena to obtain that information from a third-party service.

In situations where defendants are found innocent, public proceedings often result in defendants' personal lives being put on display for all to see. As discussed throughout this article, a person's secured smartphone can be the greatest source of information. For many people, a smartphone may contain a digital footprint of their entire life. Public disclosure of that information, or its use in evidence, could be potentially career-ending or life-altering.

In certain instances, this disclosure is unavoidable. However, constitutional safeguards are in place to protect that disclosure in as many circumstances as possible. The Fifth Amendment is no exception to that principle.

A. The Issue of Technological Change

Smartphones today contain more information than our founding fathers likely ever could have imagined. Therefore, they pose a significantly greater danger to the public disclosure of our private lives than even searches of our homes. The United States Supreme Court has recognized as much in *Riley v. California*, and the relevant portion of their opinion doing so is worth quoting in full.

> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." (citation omitted). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[144]

Today, the extent of the information that a phone potentially contains does not necessarily stop with that information actually stored on the device. For example, users may use other applications which utilize cloud storage to

---

https://www.forbes.com/sites/tomcoughlin/2019/07/24/where-do-you-backup-data/?sh=56b57e0442f0.

[144] *Riley*, 573 U.S. at 396–97.

save files, such as Dropbox, Google Drive, or iCloud.[145] Many devices allow these apps to automatically log in when the app is opened, or save the login information for it to be auto-filled when logging in.[146] This potentially limitless access to information presents several new issues.[147] Will separate motions to compel be needed to access the information stored in these apps and services if the login information is not saved? If the login information is saved, can the government legally access that information? If not, what is to stop them from doing so anyway? If the government gains access to a cloud service containing thousands of files accessible from the device, how can the foregone conclusion exception apply if the government didn't already know that information existed? With so many difficult, unanswered questions, a clear rule that respects the fundamental rights of citizens is crucial.

An additional issue presents itself if courts continue to treat biometric and passcode authentication methods differently. Both Apple's Face ID and Touch ID biometric authentication methods require a passcode.[148] Additionally, with these technologies, the device will require a passcode any time the device has been restarted, any time the device hasn't been unlocked for 48 hours, or if Face ID couldn't find a match five times in a row.[149] In a jurisdiction allowing only unlocking by biometric means, the government would have only 48 hours from the last time the individual unlocked the device to obtain an order compelling the person to unlock the device. If the battery dies or the device restarts in that time, the government will not be able to use the biometric method and will be right back where they started. Obtaining an order to compel within these technological limitations would be very unlikely, if not impossible.

Additionally, a key issue contributing to the challenges in this area is the continual evolution of technology. Each year, new smartphones are being released with newer, more advanced features. New 5G cellular networks are unlocking new realms of technological possibility.[150] Many of us probably could not have foreseen the massive technological progress that occurred over the past decade, and certainly the evolution does not appear to be

---

[145] *See* Michael Muchmore & Jill Duffy, *The Best Cloud Storage and File Sharing Services for 2021*, PC MAG, https://www.pcmag.com/picks/the-best-cloud-storage-and-file-sharing-services (last visited July 7, 2020).

[146] *See, e.g.*, *Set up iCloud Keychain*, APPLE, INC., https://support.apple.com/en-us/HT204085 (last visited Apr. 8, 2021).

[147] Seo v. State, 148 N.E.3d 952, 960–61 (Ind. 2020).

[148] *About Face ID advanced technology, supra* note 44; *About Touch ID advanced security technology*, *supra* note 43.

[149] *Id.*

[150] *See What is 5G?*, QUALCOMM, https://www.qualcomm.com/5g/what-is-5g (last visited Apr. 5, 2021).

slowing. Who knows what the world might look like in ten years? What information will be stored in our smartphones then? Will we even have smartphones, or will they simply be microchips embedded underneath our skin?[151] This article does not purport to be able to read the future, and chances are, neither do you.

This reinforces the need to develop a strict rule that protects the rights of defendants and other witnesses. By ensuring that we secure their rights to be free from forceful unlocking of the devices containing the most personal and private details of their lives, we will ensure that we protect a future where individuals can continue to feel safe in using technology for these ever-evolving uses.

VI. CONCLUSION

The smartphones many of us own today store significant parts of our lives, some of it deeply personal. From photos of our family, to medical records, to our text messages and much more, many of us probably have information on our phones we do not want the world to see. By proposing that the Fifth Amendment serve as an absolute bar to the compulsory unlocking of secured smartphones, we better respect the deeply personal nature of these devices.

Additionally, this rule provides a simple method to resolve a difficult question that has caused jurisdictions across the United States to reach several different conclusions. The rule will not be susceptible to still more varied conclusions as new technologies and security methods are released and adopted by consumers. Importantly, this rule does not eliminate the government's ability to obtain the information stored on smartphones by other means, many of which have been discussed within this article. Still newer ways to bypass encryption will surely be released as technology progresses.

The United States Supreme Court should address compelled unlocking of secured smartphones where the Fifth Amendment privilege is asserted and should adopt this simple yet effective rule. Technology will not stand still, and it will not backtrack to allow the law to keep up. Instead, the law must grow with technology if our constitutional liberties are to be meaningfully protected.

---

[151] Loren Savini, *Human Microchipping Is Here, and It's About to Rock Your Skin's World*, ALLURE, https://www.allure.com/story/rfdi-microchip-implant-in-skin (last visited Mar. 26, 2018).

SILENCING SPEECH IS BAD FOR DEMOCRACY: INCORPORATING VIEWPOINT-NEUTRAL OBLIGATIONS INTO SECTION 230

Roya L. Butler*

TABLE OF CONTENTS

---

* Juris Doctor, Georgetown Law. Baccalaureate, The Wharton School of the University of Pennsylvania. This work benefited from an invaluable fellowship at the Federalist Society's Freedom of Thought Project, Alida Kass for her initial guidance and input that led to my research, and Jordan Garsson and the other editors of the Journal of Law and Technology at Texas for all their efforts in bringing this Article to print.

I. INTRODUCTION

From time immemorial, parks and town squares have been considered public forums where people would come to express their ideas. The Founders created the First Amendment to protect the freedom of speech, understanding expression as integral to the functioning of a democratic society. Today, those public physical forums of parks and town squares have largely been replaced by the private virtual forums of social media. The free exchange of ideas on such virtual platforms must be likewise protected.

The First Amendment protects American citizens from government interference. Its protections usually do not extend to limitations on free speech imposed by private companies, like Facebook and Twitter. Yet, in today's information sharing environment, social media giants have the power to control public discourse on the same, if not a greater scale, than the government. For example, if two or more social media companies work in concert to ban a user, what comparable outlet would the user have for his speech? To be sure, individuals and groups have communicated without phone lines throughout much of American history and, similarly, individuals and "groups could communicate…without Facebook or Twitter[—]and historically ha[ve]" done so.[1] But "denying a group a vastly important means of public communication is a serious burden."[2]

---

[1] Eugene Volokh, *Treating Social Media Platforms as Common Carriers?,* 1 UCLA J. OF FREE SPEECH L. 377, 398 (2021)

[2] *Id. "*By way of analogy, Adam Smith wrote against taxing necessary commodities, but noted that necessity needs to be measured based on the realities of current life, not of the past." *Id.* (internal quotes omitted). "By necessaries I understand not only the commodities which are indispensably necessary for the support of life, but whatever the custom of the country renders it indecent for creditable people, even of the lowest order, to be without." ADAM SMITH, THE WEALTH OF NATIONS 368 (1843). "So it is with social media: More than just the Greeks and Romans lived very comfortably without them, but in our society access to the major social media platforms is a necessity—especially in a competitive political environment—for political groups." Volokh, *supra* note 1.

Social media giants have frequently taken actions to censor speech, often appearing to act in concert. For example, when Twitter suspended many accounts, including that of Former President Trump, in January of 2021, Facebook and other platforms followed suit.[3] Such actions raised the concerns of even organizations like the ACLU, which was by no means a supporter of President Trump. [4] And when users attempted to express those censored views on another social networking platform, Parler, that network was quickly shut down: Apple and Google removed the app from their stores and Amazon revoked its web-hosting services.[5]

The strong-arm control that private social media companies have over individuals is due to "Section 230" liability immunity. Usually, when the government grants immunity to private companies that immunity is conditioned upon compliance with required actions.[6] However, Section 230 of the 1996 Communications Decency Act was not written with such teeth. Consequently, Section 230 allows these social media companies free reign in

---

[3] Krista Kafer, *Social media giants may have the right to cancel speech, but that doesn't make it right,* DENVER POST (Jan. 25, 2021, 12:35 PM), https://www.denverpost.com/2021/01/25/twitter-blocking-first-amendment-free-speech-social-media/; *see also* Sarah Rumpf, *Newt Gingrich Fires Back at Twitter After His Account Gets Suspended for 'Hateful Conduct'*, MEDIAITE (Mar. 5, 2021) https://perma.cc/JST7-AE72.

[4] Kate Ruane, Vera Eidelrman & Jennifer Stisa Granick, *The Oversight Board's Trump Decision Highlights Problems with Facebook's Practices*, ACLU (May 6, 2021), https://www.aclu.org/news/free-speech/the-oversight-boards-trump-decision-highlights-problems-with-facebooks-practices/ (explaining that "the decisions by Facebook and other social media companies to remove Trump from their platforms highlight the immense power these corporations wield over our collective ability to speak online.").

[5] Kafer, *supra* note 3. Due to concerns that Parler's users were encouraging violence, Google and Apple removed Parler, the politically conservative social media site, from their App Stores; and Amazon Web Services also blocked hosting the site from its servers. This is due to "merely refusing to forbid certain speech, much of which is constitutionally protected—thus voluntarily acting in a way close to how the post office and phone companies are required by law to act." Volokh, *supra* note 1 (citing Alex Fitzpatrick, *Why Amazon's Move to Drop Parler is a Big Deal for the Future of the Internet*, TIME (Jan. 21, 2021)); Jay Peters, *Google Pulls Parler from Play Store for Fostering Calls to Violence*, VERGE (Jan. 8, 2021), https://perma.cc/2GVY-N6PE; Shirin Ghaffary, *Parler Is Back on Apple's App Store, With a Promise to Crack Down on Hate Speech*, VOX: RECODE (May 17, 2021, 6:50 PM), https://perma.cc/94JU-263X).

[6] *See, e.g.,* Warner Bros. Ent., Inc. v. Jones, 611 S.W.3d 1, 10 (Tex. 2020) (citing TEX. CIV. PRAC. & REM. CODE § 73.055(a)) ("[The DMA uses] sticks and carrots to induce plaintiffs and defendants to take prompt action to rectify defamatory publications so any ensuing damages are ameliorated."); BRV, Inc. v. Superior Court, 143 Cal. App. 4th 742, 743 (2006) (citing (20 U.S.C. § 1232g(b)(1)) ("The statute takes a carrot-and-stick approach: the carrot is federal funding; the stick is the termination of such funding to any educational institution which has a policy or practice of permitting the release of educational records (or personally identifiable information contained therein) of students without the written consent of their parents").

stifling freedom of speech. In order to reclaim the balance that has been lost, the government should therefore require viewpoint-neutral content moderation policies.[7]

This Article begins by discussing First Amendment protections and the public forum doctrine. Second, it argues that internet publishers, as a policy matter, should respect the First Amendment's protection of freedom of speech. Third, it discusses the history of Section 230. Fourth, it explains how de-platforming harms users and discusses the constitutionality of Section 230. Fifth, it proposes solutions: arguing that social media companies should be considered as providing public goods and proposing that Section 230 should require social media companies to maintain viewpoint-neutral moderation in exchange for liability protection.

II. FIRST AMENDMENT FREE SPEECH PROTECTION APPLIES TO PUBLIC FORUMS

The First Amendment protects speech from government censorship.[8] This broad category includes the federal government as well as state and local government actors such as lawmakers, elected officials, public schools and universities, courts, and police officers through the Fourteenth Amendment's Due Process Clause.[9] Courts employ the public forum doctrine as an analytical framework in First Amendment jurisprudence to determine the legality of restrictions on speech in the context of constitutionally protected public property.[10]

The Supreme Court has protected the right to assembly, including the right to assemble without a permit. In *Hague v. Committee for Industrial Organization*, the Supreme Court held that "banning a group of citizens from holding political meetings in a public place violated the group's freedom of speech and assembly under the First Amendment."[11] In *Hague*, a group

---

[7] Viewpoint discrimination occurs when the government regulates "based on 'the specific motivating ideology or perspective of the speaker.'" Reed v. Town of Gilbert, 135 S. Ct. 2218, 2230 (2015) (quoting Rosenberger v. Rector & Visitors of Univ. of Va., 515 U.S. 819, 829 (1995)); *see also* Moss v. U.S. Secret Serv., 572 F.3d 962, 970 (9th Cir. 2009) ("[V]iewpoint discrimination occurs when the government prohibits speech by particular speakers, thereby suppressing a particular view about a subject.") (internal citations and quotation marks omitted).

[8] U.S. CONST. amend. I.

[9] Lata Nott, *Is your Speech Protected by the First Amendment*?, FREEDOM FORUM INSTITUTE (Aug. 2018), https://www.freedomforuminstitute.org/first-amendment-center/primers/basics/.

[10] David L. Hudson Jr., *The First Amendment Encyclopedia*, MTSU (Jan. 8, 2020), https://mtsu.edu/first-amendment/article/824/public-forum-doctrine.

[11] Hague v. Committee for Indus. Org., 307 U.S. 496, 501 (1939) **(**ruling that banning a group of citizens from holding political meetings in a public place violated the group's freedom to

assembled in a public place to discuss and distribute literature relating to the National Labor Relations Act.[12] Mayor Hague "referred to the group as 'communist' and a danger to the city."[13] The issue was whether a Jersey City ordinance prohibiting assembly without a permit violated the First and Fourteenth Amendments.[14] The Committee for Industrial Organization (CIO), with support from the American Civil Liberties Union, sought an injunction based on denial of First Amendment rights.[15] "The lower federal courts ruled in favor of the CIO," and the Court upheld the decision.[16]

Writing for the Court, Justice Owen Roberts explained that streets and parks "have immemorially been held in trust for the use of the public and . . . have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions."[17] He reasoned that "[s]uch use of the streets and public places has, from ancient times, been a part of the privileges, immunities, rights, and liberties of citizens,[18] [and therefore] belong to citizens and must be protected as public forums."[19] Although expression can be regulated without discrimination in these public forums, it must not be prohibited.[20] He further explained that:

> [t]he privilege of a citizen of the United States to use the streets and parks for communication of views on national questions may be regulated in the interest of all; it is not absolute, but relative, and must be exercised in subordination to the general comfort and convenience, and in consonance with peace and good order; but it must not, in the guise of regulation, be abridged or denied. [21]

Recent decisions have similarly shown the Court's conviction to upholding free speech rights.[22] In *Mahanoy Area Sch. Dist. v. B.L.,* a cheerleader challenged her suspension from the squad based on social media

---

assemble under the First Amendment).

[12] *Id.* at 505–08.

[13] Lynne Chandler Garcia, *Hague v. Committee for Industrial Organization*, MTSU (2009), https://mtsu.edu/first-amendment/article/619/hague-v-committee-for-industrial-organization.

[14] *Hague*, 307 U.S. at 501; *see also* Garcia, *supra* note 13.

[15] Garcia, *supra* note 13.

[16] *Id.*

[17] *Hague*, 307 U.S. at 515.

[18] *Id.*

[19] Garcia, *supra* note 13.

[20] *Id.*

[21] *Hague*, 307 U.S. at 515–16.

[22] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046–47 (2021) (internal citations omitted).

posts that some considered vulgar.[23] The School District contended that "vulgar language [i]s low-value speech that c[an] be restricted to a greater extent than would otherwise be permissible." [24] The Court found that "while B. L. used vulgarity, her speech was not obscene . . . [and] [t]o the contrary, B.L. uttered the kind of . . . speech to which . . . the First Amendment would provide strong protection."[25] The Court reasoned that "[i]t might be tempting to dismiss B.L.'s words as unworthy of the robust First Amendment protections discussed herein. But sometimes it is necessary to protect the superfluous in order to preserve the necessary."[26] The Court concluded that "[w]e cannot lose sight of the fact that, in what otherwise might seem a trifling and annoying instance of individual distasteful abuse of a privilege, these fundamental societal values are truly implicated."[27]

These cases illustrate that, "[a]t the heart of the First Amendment is the recognition of the fundamental importance of the free flow of ideas and opinions on matters of public interest and concern."[28] "The fundamental purpose of the First Amendment was to guarantee the maintenance of an effective system of free expression," which is necessary to "protect the marketplace of free ideas." [29] Free expression affirms human dignity and man's "capacity as an individual."[30] The Constitution protects free expression as a natural right because "expression is an integral part of the development of ideas, of mental exploration and of the affirmation of self," [31] while restraint over expression has been criticized as an "indignity to a free and knowing spirit."[32] Although these principles only apply to the government under the Constitution, similar justifications exist for extending First Amendment-like protection to users of social media.

---

[23] *Id.*

[24] B.L. v. Mahanoy Area Sch. Dist., 964 F.3d 170, 191 (3d Cir. 2020).

[25] *Mahanoy*, 141 S. Ct. at 2047; *see* Cohen v. California, 403 U.S. 15, 19–24 (1971); *cf.* Snyder v. Phelps, 562 U.S. 443, 461 (2011) (holding that the First Amendment protects "even hurtful speech on public issues to ensure that we do not stifle public debate"); Rankin v. McPherson, 483 U.S. 378, 387 (1987) ("The inappropriate . . . character of a statement is irrelevant to the question whether it deals with a matter of public concern").

[26] *Mahanoy*, 141 S. Ct. at 2048; *see* Tyson & Brother v. Banton, 273 U.S. 418, 447 (1927) (Holmes, J., dissenting).

[27] *Mahanoy*, 141 S. Ct. at 2048 (quoting Cohen v. California, 403 U.S. 15, 25 (1971)).

[28] *Id.* at 2055 (quoting Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 50 (1988)).

[29] Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 880 (1963).

[30] *Id.*; *Free Speech in the Modern Age*, 31 FORDHAM INTEL. PROP. MEDIA & ENT. L.J. 978, 989 (2021).

[31] *Id.*

[32] JOHN MILTON, AEROPAGITICA 21 (Everyman's Library ed. 1927).

III. INTERNET CONTENT PROVIDERS SHOULD PROTECT FREEDOM OF SPEECH

Internet content providers such as Facebook and Twitter have largely succeeded the constitutionally protected town squares of the Founding. These social media platforms are forums where community groups chat and share information, headlines, and other discourse. Tweets, for instance, are akin to the early pamphlet distributors of the Founding era.[33] Like the parks and town squares, the barrier to entry on social media is de minimis, allowing for accessibility, ease, and convenience of posting and sharing ideas. The COVID-19 pandemic further enhanced the importance of online internet content providers, as various governments used the force of law to severely restrict in-person meetings.[34] Such quarantine mandates and indoor confinement only fortified the upsurge of user-created social media content.

This section proceeds by asserting, first, internet content providers should voluntarily, as a policy matter, protect free speech. Second, internet content providers' removal of social media profiles undermines free speech principles that are vital to a democratic society. Third, these providers should adopt content moderation policies consistent with First Amendment jurisprudence for incitement, or at least clarify and consistently apply their own incitement standards.[35] Fourth, when internet content providers effectively override the support of democratic voters it harms everyone, regardless of one's place on the political spectrum. Fifth, internet content providers' current lack of protection for free speech will harm vulnerable users. And finally, free speech is necessary to promote a stable economy.

A. Policy Reasons for Social Media Free Speech Protection

The First Amendment doesn't prevent a private company from filtering online speech. Nevertheless, these internet content providers' role as a modern replacement for historical public forums counsels that they should respect similar protections for speech as those enshrined in the First

---

[33] *See generally* JANE N. GARRETT, PAMPHLETS OF THE AMERICAN REVOLUTION (Harvard Univ. Press 1965) (describing the distribution of pamphlet literature including Thomas Paine's *Common Sense* during the Founding Era).

[34] Statistica Research Department, *Social media use during COVID-19 worldwide - statistics & facts*, STATISTICA (May 19, 2021), https://www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/.

[35] Facebook Community Standards, *Violence and Criminal Behavior: Violence and Incitement,* FACEBOOK, https://www.facebook.com/communitystandards/violence_criminal_behavior.

Amendment.[36] Therefore, the policy behind the First Amendment protecting public discourse should apply with equal force to internet content providers.

B. Social Media Profile Removal Undermines Free Speech

Facebook, for example, completely disregards the first *Brandenburg* prong, requiring consideration of whether the speaker directed his speech to cause this risk. Among other things, Facebook's content moderation policy removes "language that incites or facilitates serious violence," which is clarified to lead to the removal or disabling of accounts when there is a "genuine risk of physical harm or direct threats to public safety."[37] At first glance, this approach seems similar to the test in *Brandenburg v. Ohio*, used by courts to determine whether speech is unprotected incitement.[38]

This distinction is not immaterial. Under Facebook's policy, any speech that could lead to violence may be removed even if it is well-meaning. For example, posts regarding an extremely controversial topic or an unpopular opinion that are not otherwise a call to violence could be considered likely to create a "genuine risk of physical harm" by hecklers who will react violently to supporters of the poster. In this way, the poster, who is himself a victim of the violence, could end up being blocked. By focusing on the objective intent of the speaker rather than the reactions of the readers, Facebook can avoid this type of heckler's veto. And by considering the action that the speaker directed, Facebook can still remove speech calling for violent action but would not remove controversial speech that may incidentally be construed as a call to violent action when it was not intended as one. Internet content providers could consider the context in which statements are made, but the statements would truly have to be directed toward incitement.

C. Internet Content Providers Should Adopt Brandenberg

Facebook should consider following the Supreme Court's reasoning in *Brandenburg* and require that the meaning of the user's speech be directed toward causing this violence before removing it. For example, under such a

---

[36] Kate Ruane, Vera Eidelrman & Jennifer Stisa Granick, *The Oversight Board's Trump Decision Highlights Problems with Facebook's Practices*, ACLU (May 6, 2021), https://www.aclu.org/news/free-speech/the-oversight-boards-trump-decision-highlights-problems-with-facebooks-practices/ (although Facebook is a private entity and "not governed by the First Amendment . . . the broader issue . . . is how an extraordinarily powerful private corporation regulates access to one of the country's most important forums for discussion and debate . . . Facebook . . . must do more to ensure that it operates its platform consistent with principles of free expression and fair process for all.").

[37] Facebook Community Standards, *supra* note 35.

[38] Brandenburg v. Ohio, 395 U.S. 444, 447–48 (1969).

test, President Trump's video calling for protestors to go home would not be objectionable even if his repeated utterances of voter fraud allegations and expressions of love for the protestors could be construed to create a risk of physical harm.

Our Founding Fathers believed in the power of reason as applied through public discussion.[39] Indeed, they expressly recognized that:

> order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones.[40]

The Supreme Court has over time reinforced these views. In *Abrams v. United States*, Justice Holmes commented on the importance of both good and bad ideas in a marketplace of ideas.[41] Justice Holmes reasoned that "the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out."[42] Similarly, in *Texas v. Johnson*, Justice Brennan explained that we "may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[43] And in *Whitney v. California*, Justice Brandeis concurred that, "[i]f there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence."[44] He further noted that "the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government."[45]

The *Brandenburg* test shows the far reach of First Amendment protection against even odious speech. *Brandenburg* established when the government can restrict incitement, defined as inflammatory speech intending to incite illegal action.[46] In *Brandenburg*, the Court explained that speech is

---

[39] *Id.*
[40] *Id.* at 375–76.
[41] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting).
[42] *Id.*
[43] Texas v. Johnson, 491 U.S. 397, 414 (1989).
[44] Whitney v. California, 274 U.S. 357, 377 (1927).
[45] *Id.* at 375.
[46] Brandenburg v. Ohio, 395 U.S. 444, 444 (1969).

unprotected when it is reasonably calculated to imminently incite harm. [47] The facts of the case are revealing. The Court ruled that speech was protected when members of the Ku Klux Klan vowed vengeance against minority races and instructed listeners to march on Washington against elected officials who they claimed suppressed the white race.[48] The *Brandenburg* Court has held that even this repugnant speech was protected due to the fact that it was attenuated from any actual action and that there was not a direct call to violence. [49]

Critics contend that some ideas, like an incitement to violence, are simply not worth sharing. And, as discussed, courts have long recognized that such speech that presents a clear and present danger is not protected by the First Amendment. In these scenarios, courts reason that there will not be time for argument and debate to defeat bad ideas before violence occurs. Recognizing the importance of ensuring an open marketplace of ideas, however, has caused the court to adopt a very high standard for what constitutes actual incitement.

Returning to the example of the banning of President Trump, Facebook may argue that it was justified in its initial suspension of the former President's Facebook account in order to prevent the incitement of imminent violence at the capitol. Setting the merits of that contention to the side, however, Facebook is unquestionably not justified in permanently banning his account when no lingering danger exists and there is no evidence suggesting that the former President will make a call to arms.[50] Facebook could institute suspensions when necessary to prevent imminent violence, but a permanent speech suppression in the absence of any dangerous situation is abhorrent to the values protected by the First Amendment. Furthermore, the need for clear standards of general applicability becomes even more urgent when the consequence for violating those standards involves effectively silencing the leader of a political party representing a large segment of the country.[51]

---

[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Ruane, *supra* note 36 ("The ACLU believes that the speech of former President Trump should be presumed important to the functioning of our democratic system given his prior role in government. Most of what politicians and political leaders say is, by definition, newsworthy, and can at times have legal or political consequences. While their words may have greater capacity for harm, there is also a greater public interest in having access to their speech.").
[51] Prasad Krishnamurthy & Erwin Chemerinsky, *How Congress Can Prevent Big Tech from Becoming the Speech Police*, HILL (Feb. 18, 2021), https://perma.cc/645W-LMLP ("That private technology platforms exert unparalleled power over political discourse is deeply undemocratic."). Such censorship embodies the precise type of repression that the Founding

Subsequent cases have revealed that speech generally only constitutes incitement when there is a direct call to violence in a scenario where it can occur immediately or soon after.[52] Such a high bar ensures that only in the gravest situation of potential danger will the drastic remedy of suppressing speech be permitted. At a minimum, internet content providers should: (1) clearly outline what standard they use for incitement, and (2) apply a standard akin to *Brandenburg*. First, to avoid confusion, social media companies should clearly enunciate what constitutes incitement and apply their chosen standard evenly across the board.[53] Second, although social media companies are not currently obligated to apply the *Brandenburg* test, they should. The test affords the strongest protection of free speech while still balancing the interests in maintaining peace. Furthermore, social media companies should consider the arguments built upon over two centuries of First Amendment jurisprudence and ensure that only speech being suppressed is that which calls for—and is likely to actually result in—immediate violence.

Justices from all judicial philosophies over decades have understood that the only way to defeat bad speech is through countering it with good speech. A bad idea can only be defeated by a public argument in which a good idea triumphs over it through the power of reason and persuasion. Conversely, when ideas are censored from the public debate, they will never be subject to such a challenge. Instead, those beliefs will fester with no possible rebuttal from those who disagree with them. Believers in the bad idea would further only share those beliefs with other like-minded individuals out of fear that sharing them publicly would lead to their ostracism and cancellation. If left unchecked by debate and amplified through mutually confirmatory discussions with other believers, such bad ideas will only become more ingrained in the minds of followers. For example, imagine that the dominant thought was that the Earth was the center of the universe, and that anyone believing it was not, would be persecuted.[54] If unpopular ideas were censored,

---

Fathers warned of—likely to breed hate and menace any form of stable governance. *Id.*

[52] *Id.* (finding that the First Amendment lends no protection to speech when that speech urges listeners to commit violations of current law.); Rice v. Paladin Enters., Inc., 128 F.3d 233, 246 (4th Cir. 1997) (finding that First Amendment's protection of speech does not necessarily bar liability for aiding and abetting crime in the form of spoken or written speech.); United States v. Buttorff, 572 F.2d 619, 624 (8th Cir. 1978) (finding that aiding and abetting in tax fraud constituted incitement and thus was unprotected speech).

[53] Volokh, *supra* note 1 ("Facebook's and Twitter's rules lack . . . transparency, procedural protections and democratic pedigrees.") (citing Nick Clegg, *Facebook: Welcoming the Oversight Board,* FACEBOOK (May 6, 2020), https:// perma.cc/B5RF-JPAK.). "Facebook's failure to abide by basic principles of fairness and transparency are unacceptable given the influence they exert over our national debate. Facebook and similar platforms should err on the side of free expression, not censorship." Ruane, *supra* note 36 (explaining that "Facebook should publicly explain its rules for removing posts and accounts.").

[54] *See* Owen Gingerich, *Galileo, The Impact of the Telescope, and the Birth of Modern*

society would have no opportunity to hear the minority's argument and the false belief would persist.[55] To prevent such outcomes, Justice Holmes stated that "we should be eternally vigilant against attempts to check the expression of opinions that we loathe."[56]

Courts and the public have long understood the core rationale underlying the freedom of speech to be the protection of public discourse. Through the push and pull of debate, the public will eventually counter bad ideas and move together towards finding greater truth. Today, when individuals post their thoughts on social media, debate is facilitated through comments or replies. Adequate speech protections ensure that everyone is given an opportunity to engage.

D. Silencing Speech Has an Anti-Democratic Effect

When internet content providers effectively override the support of democratic voters, it affects us all. To specifically underscore why the potential effect is so bad, consider Facebook and Twitter banning former President Trump.[57] In this specific case, internet content providers' actions further create an acutely anti-democratic effect, silencing the spokesman of millions of American voters. Regardless of the former President's viewpoint, he represented 74 million people, and banning his social media presence effectively silenced those voters.[58] By unilaterally silencing the speech of a former elected official who had led a party representing roughly half of the country, Facebook and Twitter have effectively decided that the 74 million Americans who voted for the former President are not worthy of this significant form of representation on their platform.[59] The consequence of silencing the speech of voters by banning the voice of the person who speaks for them illustrates how the current policies of Facebook and Twitter have

---

Astronomy, 155 PROC. OF THE AM. PHIL. SOC'Y 134, 134 (2011) (explaining that "the inquisition forced Galileo under the threat of torture to recant his belief in Copernicus's heliocentric system.").

[55] *Id.*

[56] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting).

[57] Davey Alba, Ella Koeze & Jacob Silver, *What Happened When Trump Was Banned on Social Media*, N.Y. TIMES (Jun. 7, 2021), https://www.nytimes.com/interactive/2021/06/07/technology/trump-social-media-ban.html ("Facebook said the former president would not be allowed back on its service until at least January 2023, citing a risk to public safety.").

[58] See James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELATIONS (Dec. 15, 2020), https://www.cfr.org/blog/2020-election-numbers (stating that Former President Trump received 74,222,958 votes in the 2020 Presidential election.).

[59] Ruane, *supra* note 36 ("[I]t should concern everyone when companies like Facebook and Twitter wield the unchecked power to remove people from platforms that have become indispensable for the speech of billions.").

already led to an anti-democratic result and should be corrected. Although Facebook and Twitter should not accord special protections to elected officials, they should update their policies to apply a *Brandenburg* standard to all users. Facebook and Twitter might have defended their actions in banning President Trump as pro-democratic because they sought to challenge his allegedly anti-democratic rhetoric of questioning the election results. Those determinations, however, are not something that two private companies, who were not elected, should make.

Judge Silberman's dissent in *Tah v. Global Witness Publishing, Inc.,* expressed concern that "the first step taken by any potential authoritarian or dictatorial regime is to gain control of communications, particularly the delivery of news."[60] Judge Silberman goes on to explain that "one-party control of the press and media is a threat to a viable democracy," may "give rise to countervailing extremism," and that a biased press can distort the marketplace of ideas.[61] He points out that "Silicon Valley . . . has an enormous influence over the distribution of news, [a]nd it similarly filters news delivery in ways favorable to [only one] Party."[62] He states that "[i]t is well-accepted that viewpoint discrimination raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace."[63] He argues that "homogeneity in the media—or in the channels of information distribution—risks repressing certain ideas from the public consciousness just as surely as if access were restricted by the government."[64] Similarly, one-sided viewpoint discrimination in content moderation by social media companies presents an equal threat to the marketplace of ideas and the political system as it would if the speech was restricted by the government.

E. Vulnerable Users Are Harmed by Lack of Free Speech Protection

Internet content providers such as Facebook and Twitter should consider the broader effect of their current lack of free speech protection for all users and should apply their policies consistently across all people as a safeguard against viewpoint favoritism.[65] Some users, such as celebrities and

---

[60] Tah v. Global Witness Publ'g, Inc., 991 F.3d 231, 272 (D.C. Cir. 2021) (Silberman, J., dissenting) (quoting R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 387 (1992) (internal quotes omitted)).
[61] *Id.* at 271.
[62] *Id.* at 272.
[63] *Id.* (citing R.A.V. v. City of St Paul, Minn., 505 U.S. 377, 387 (1992).
[64] *Id.*
[65] *See* Katharine Trendacosta, *What the Facebook Whistleblower Tells Us About Big Tech*, EFF (Oct. 8, 2021), https://www.eff.org/deeplinks/2021/10/what-facebook-whistleblower-

politicians have a broad reach and therefore may not be as negatively affected if banned from social media. For example, President Trump, after he was banned, was able to reach his constituents through his personal website, campaign fund-raising site, and email.[66] Other popular social media accounts often picked up President Trump's messages and posted them themselves.[67] Many vulnerable groups, however, do not have as amplified a voice and have encountered situations where they have been shut out of speech with little or no other avenues.[68] Internet content providers should evaluate the

---

tells-us-about-big-tech (explaining, for example, that "[p]oliticians who make extreme statements get more engagement, and are therefore ranked higher by Facebook, and are therefore seen by more Facebook users."); Guardian Staff, *Facebook oversight board to review system that exempts elite users: The XCheck program allows some users to be 'whitelisted' or allowed to post material that violates the company's policies*, GUARDIAN (Sept. 21, 2021), https://www.theguardian.com/technology/2021/sep/21/facebook-xcheck-system-oversight-board-review (explaining that under Facebook's XCheck system, "some users are 'whitelisted', or not subject to enforcement action, while others are allowed to post material that violates Facebook rules pending content reviews that often do not take place"); Sam Biddle, *Revealed: Facebook's Secret Blacklist of "Dangerous Individuals and Organizations": Experts say the public deserves to see the list, a clear embodiment of U.S. foreign policy priorities that could disproportionately censor marginalized groups*, INTERCEPT (Oct. 12, 2021), https://theintercept.com/2021/10/12/facebook-secret-blacklist-dangerous/ ("The materials show Facebook offers 'an iron fist for some communities and more of a measured hand for others,' said Ángel Díaz, a lecturer at the UCLA School of Law who has researched and written on the impact of Facebook's moderation policies on marginalized communities.").

[66] Alba, *supra* note 57 (to reach his constituents, President Trump used his personal website, campaign fund-raising site, and email, and furthermore, other popular social media accounts often picked up his messages and posted them themselves). *See also* Natalie Colarossi, *ACLU Counsel Warns of 'Unchecked Power' of Twitter, Facebook After Trump Suspension*, NEWSWEEK (Jan. 9, 2021), https://www.newsweek.com/aclu-counsel-warns-unchecked-power-twitter-facebook-after-trump-suspension-1560248 (quoting ACLU Senior Legislative counsel Kate Ruane on the permanent suspension by Twitter of former President Trump, "President Trump can turn his press team or Fox News to communicate with the public, but others—like many Black, Brown, and LGTBQ activists who have been censored by social media companies—will not have that luxury.").

[67] Colarossi, *supra* note 66.

[68] *See e.g.,* Cindy Harper, *Mastectomy support groups constantly censored by Facebook despite not breaking rules the groups are battling with Facebook's censorship AI*, RECLAIMTHENET (Oct. 29, 2020), https://reclaimthenet.org/mastectomy-support-groups-constantly-censored-by-facebook/ ("The founder of a mastectomy support group on Facebook claims that the platform repeatedly censors its content despite their content not violating Facebook's community standards"); Biddle, *supra* note 65 (explaining that Facebook bans "Muslim regions and communities."); CJ Werleman, *How Facebook Threatens Vulnerable Muslim Communities*, ASTUTE NEWS (Sept. 5, 2020), https://astutenews.com/2020/09/how-facebook-threatens-vulnerable-muslim-communities/ ("Facebook has also been accused of showing favouritism to Israel by categorising vague or even commonly used Arabic terms or slogans as 'incitement to violence,' while simultaneously turning a blind eye to Israeli accounts that openly call for 'death to Arabs'");

consequences of this standard, not just as applied to the former President, but also to their vulnerable users.

F. Free Speech is Necessary to Promote a Stable Community

First Amendment Scholar Thomas I. Emerson reasoned that a system of free expression is necessary, amongst other things, to promote a stable community.[69] A healthy society adjusts to changing circumstances by developing new ideas through discussion and engaging with counterarguments, which diffuses prejudice and hostility.[70] Opposition, debate, and counter ideas function to stimulate the process of change, offsetting stagnation.[71] Conversely, "[s]uppression of ideas . . . festers and ultimately creates hostility."[72] As Emerson wrote, the suppression of free expression destroys a stable community:

> [S]uppression of expression conceals the real problems confronting a society and diverts public attention from the critical issues. It is likely to result in neglect of the grievances which are the actual basis of the unrest, and thus prevent their correction. For it both hides the extent of opposition and hardens the position of all sides, thus making a rational compromise difficult or impossible. Further, suppression drives opposition underground, leaving those suppressed either apathetic or desperate. It thus saps the vitality of the society or makes resort to force more likely. And finally it weakens and debilitates the majority whose support for the common decision is necessary. For it hinders an intelligent understanding of the reasons for adopting the decision and, as [John Stuart] Mill observed, "beliefs not grounded on conviction are likely to give way before the slightest

---

Marwa Fatafta, *Palestinian dissent is repressed online: Censorship of Palestinian content by Israel, the PA, and Hamas is escalating at an unprecedented and dangerous speed*, 972MAG (Dec. 4, 2019), https://www.972mag.com/censorship-online-palestinians/ ("WhatsApp, the messaging app now owned by Facebook, also blocked or shut down around one hundred accounts belonging to Palestinian journalists and activists, and banned them from sharing information and updates during Israel's military attacks on Gaza . . . .").

[69] Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 884 (1963).

[70] *Id.*

[71] *Id.*

[72] *Id.* ("[S]uppression of expression conceals the real problems confronting a society and diverts public attention from the critical issues." This diversion could likely "result in neglect of the grievances which are the actual basis of the unrest, and thus prevent their correction.")

> semblance of an argument."[73] In short, suppression of opposition may well mean that when change is finally forced on the community it will come in more violent and radical form.[74]

In fact, Emerson claimed that "prosecution of unpopular opinion is frequently an important avenue of political advancement, and hence has a special appeal for the politically ambitious."[75] He pointed out that "[f]requently prosecution of unpopular opinion is used as a screen for opposing necessary social change."[76]

The process of opening dialogs and sharing ideas allows for "greater cohesion [and] political legitimization," therefore promoting a stable community.[77] In other words, "allowing dissidents to expound their views enables them to 'let off steam'" and have their voices heard.[78] For example, when "any person is permitted to say anything he wishes to whatever audience he can assemble [in a public forum,] [it] results in a release of energy, a lessening of frustration, and a channeling of resistance into courses consistent with law and order."[79] This allows the person to feel heard, operating "as a catharsis throughout the body politic."[80]

IV. SECTION 230

Section 230's liability immunities present an issue to the extent they provide social media companies with legal and political cover for suppressing free expression. Section 230 states, in relevant part:

> **(c) Protection for "Good Samaritan" blocking and screening of offensive material.**
>
> **(1)** Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> **(2)** Civil liability. No provider or user of an interactive computer service shall be held liable on account of—
>
> **(A)** any action voluntarily taken in good faith to restrict

---

[73] *Id.* (citing John Stuart Mill, ON LIBERTY AND OTHER ESSAYS 20, 42 (Neff ed. 1926) (1859)).
[74] Emerson, *supra* note 69, at 885.
[75] *Id.* at 890.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*

> access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> **(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].[81]

Section 230(a)(3) explains that one purpose of the Bill was to ensure that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[82]

Ensuring that internet platforms cannot be treated as publishers or speakers of user-generated content precludes common law liability for such content. Absent Section 230, the common law made internet content providers potentially liable for what others posted if the providers engaged in content moderation.[83] Section 230(c)(1), by its text, prohibits "only one type of action: those where a plaintiff seeks to 'treat [an internet platform] as the publisher of independently posted content.'"[84] The text of Section 230(c)(1) does not suggest that it creates general immunity for internet content providers, but courts have read the statute to confer such general immunity under Section 230(c)(2).[85]

The purposes enumerated in Section 230 confirm that the Bill was intended "to promote the continued development of the Internet and other interactive computer services and other interactive media"[86] and "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who

---

[81] 47 U.S.C. § 230(c) (2012).

[82] 47 U.S.C. § 230(a)(3) (2012); *but see* The Pact Act and Section 230: The Impact of the Law that Helped Create the Internet and an Examination of Proposed Reforms for Today's Online World Before the S. Subcom. on Communications, Technology, Innovation, & the Internet, S. Comm. on Commerce, Science, & Transportation, 116th Cong. (2020) (statement of Jeff Kosseff, Assistant Professor, Cyber Science Department, United States Naval Academy).

[83] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1996).

[84] Adam Candeub, *Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230*, 22 YALE J. L. & TECH. 391, 398–403 (2020).

[85] *Id.*; Levitt v. Yelp! Inc., No. C 10-1321 MHP, 2011 U.S. Dist. LEXIS 99372, *23 (N.D. Cal. Mar. 22, 2011); Airbnb, Inc. v. City & Cty. of San Francisco, 217 F. Supp. 3d 1066, 1074 (N.D. Cal. 2016).

[86] 47 U.S.C. § 230(b)(1).

use the Internet and other interactive computer services."[87] Section 230 provided that these companies would not be liable for moderation decisions or third-party speech in order to ensure that online forums could flourish without such a daunting specter of liability.

This section examines Section 230 precedent and then analyzes how the actions it immunizes harms users. Next, it evaluates social media platforms as a public good and reviews the history of common carrier doctrine before arguing that common carrier and public accommodation doctrines should apply to social media platforms. Finally, it discusses amending Section 230 with obligations or "sticks," including a requirement to engage in viewpoint-neutral moderation that would include a safe harbor to promote small business.

A. History of Section 230

Understanding the legislative bargain underlying Section 230 requires understanding the Act's history and purpose. The seminal cases of *Cubby, Inc. v. CompuServe* and *Stratton Oakmont, Inc. v. Prodigy Services* led to the enactment of Section 230.[88]

In *Cubby*, the Southern District of New York considered a defamation claim against CompuServe, an online content provider.[89] The claim was based on an allegedly libelous statement posted in CompuServe's online journalism forum, which disparaged Cubby's competing journalism forum.[90] The court noted that CompuServe did not exercise editorial control over the forum contents because a third-party provider edited the forum content and analogized CompuServe to "an electronic, for profit library" with distributor liability.[91] Concerned with the free flow of information, the court found the "inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information."[92] The court noted that "an ISP, as a distributor, would generally

---

[87] 47 U.S.C. § 230(b)(3).

[88] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1996).

[89] *Cubby*, 776 F. Supp. at 140–41.

[90] *Id.* at 137.

[91] Restatement (Second) Of Torts § 581 (Am. Law Inst. 1977) ("(1) Except as stated in subsection (2), one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character. (2) One who broadcasts defamatory matter by means of radio or television is subject to the same liability as an original publisher.").

[92] *Id.*

not be liable for defamation if it did not know or did not have reason to know of the existence of defamatory statements."[93] The court considered CompuServe's lack of control over users' publications in the forums and reasoned that "it would be no more feasible for CompuServe to examine every publication it carried for potentially defamatory statements than it would be for any other distributor to do so."[94] Therefore, the *Cubby* court held that an online content provider that does not control moderation of a forum cannot be held liable for third-party posts.[95]

In *Stratton*, the New York Supreme Court considered a defamation claim against online content provider, Prodigy.[96] The *Stratton* court reached the opposite conclusion of *Cubby* and "held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements."[97] Here, plaintiff also brought suit on an allegedly libelous statement posted on its online bulletin board.[98] Like CompuServe, Prodigy contracted a third-party to monitor and edit the forum content.[99] Unlike CompuServe, however, Prodigy marketed itself as an online community with a "value system that reflects the culture of millions of American families," and "developed and implemented policies, guidelines, and a software-screening program and allowed its bulletin board leaders to delete offending messages."[100] Prodigy's actions led the court to conclude that, unlike CompuServe,, the online content provider acted more like an original publisher than a distributor.[101] The court reasoned that Prodigy (1) advertised that its service practiced control of user content and (2) actively monitored and edited posted bulletin board messages.[102] Therefore, Prodigy's receipt of the benefits of editorial control precluded it from claiming distributor immunity from liability.

Thus, the common law provided two potential liability frameworks for internet content providers. If an internet content provider did not itself dictate moderation policies, it would be examined under the *Cubby* framework and deemed a distributor that generally could not be held liable for that content.[103]

---

[93] *Id.*
[94] *Id.*
[95] *Id.* at 140.
[96] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1996).
[97] *Id.* at *1.
[98] *Id.*
[99] David P. Miranda, *Defamation in Cyberspace: Stratton Oakmont, Inc. v. Prodigy Services Co*., 5 ALB. L.J. SCI. & TECH. 229, 234 n.29 (1996).
[100] *Id.* at 234.
[101] *Id.*
[102] *Id.*
[103] *See, e.g.*, Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1996); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907

Conversely, if an internet content provider set policies to moderate user content, courts would consider the *Stratton* approach and deem them strictly liable as if they were the speaker of the content. Section 230 responded to this legal liability framework by providing a new avenue for internet content providers to moderate content without exposing themselves to potential liability.

Section 230(c)(1) states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[104] Just like bookstores that have no duty to review the books they are selling, "this provision grants a type of distributor liability to online platforms."[105] The text of Section 230(c)(2) precludes liability for an internet content provider that deletes posts that are "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[106] Section 230(b)(4) describes the Act's purpose stating Congress's desire to allow internet content providers the ability to moderate their platforms and delete these categories of inappropriate content in order to ensure that the platform can remain family-friendly.[107]

The volume of information communicated by millions of users via online content providers is staggering and growing.[108] When enacting Section 230, Congress considered that if service providers were faced with potential liability for republishing, it could ultimately lead to a severe restriction on the amount and type of speech posted, and moderation of millions of posts would be costly and time-consuming.[109] In light of this concern, legislators chose to "immunize service providers to avoid any such restrictive effect."[110] In enacting Section 230, Congress also intended to "encourage service providers to self-regulate the dissemination of offensive material over their services."[111]

Section 230 responded to a legitimate problem in the common law. The statute enabled the online landscape to flourish over the last thirty years, changing it fundamentally from the time of *Stratton* and *Cubby*. This boom

---

F. Supp. 1361, 1365 (N.D. Cal. 1995) (finding access provider not directly liable).

[104] 47 U.S.C. § 230(c)(1).

[105] Candeub, *supra* note 84, at 421.

[106] 47 U.S.C. § 230(c)(2).

[107] *See* 47 U.S.C. § 230(b)(4) (providing that one of § 230's policy goals is to empower parents to restrict children's access to objectionable online material).

[108] *See* Reno v. Am. C.L. Union, 117 S. Ct. 2329, 2334 (1997) (finding that the number of host computers increased from 300 in 1981 to 9,400,000 by 1996).

[109] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) ("The specter of tort liability in an area of such prolific speech would have an obvious chilling effect.").

[110] *Id.*

[111] *See* 47 U.S.C. § 230(b)(4) (providing that one of § 230's policy goals is to "remove disincentives to block" offensive material.

has caused social media to take a prominent, if not preeminent, place in how many Americans receive their information and engage in political discourse. Section 230's original justification may no longer be applicable today.

Section 230 allows internet content providers to de-platform their users with no regard for potential liability, which in turn harms users by preventing them from posting their views.[112] This may make sense in some cases; for example, it would be difficult for a small company to gain users if it could not systematically de-platform the harassing trolls[113] or bots.[114] As such, the lack of ability to moderate could impede the growth of small business. However, in cases involving dominant digital platforms, the de-platformed user who is precluded from expressing himself faces a massive harm.

V. SECTION 230 PRESENTS POLICY AND LEGAL ISSUES

Section 230 in its current form presents at least two significant problems. First, Section 230 allows social media companies to de-platform users with impunity. Second, Section 230 may unconstitutionally allow the government to coerce social media companies to suppress speech in ways that the government constitutionally cannot.

A. De-platforming Can Harm Users Through Discrimination

In *Biden v. Knight First Amendment Institute at Columbia University,* Justice Thomas expressed his concern that internet content providers suppress speech.[115] He noted that "if the aim is to ensure that speech is not smothered, then the more glaring concern must perforce be the dominant digital platforms themselves."[116] He explained that "Twitter made clear [that] the right to cut off speech lies most powerfully in the hands of private digital platforms."[117] This de-platforming is particularly harmful if it discriminates

---

[112] *See Deplatforming, Oxford English Dictionary*, https://www.lexico.com/en/definition/deplatforming?locale=en ("The action or practice of preventing someone holding views regarded as unacceptable or offensive from contributing to a forum or debate, especially by blocking them on a particular website."); 47 U.S.C. § 230(c)(2) (limiting the liability of internet companies for restricting access to content).

[113] *See Troll, Oxford English Dictionary*, https://www.lexico.com/en/definition/troll?locale=en ("A person who makes a deliberately offensive or provocative online post.").

[114] *See Bot, Oxford English Dictionary*, https://www.lexico.com/en/definition/bot?locale=en ("An autonomous program on the internet or another network that can interact with systems or users.").

[115] Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1222 (2021) (Thomas, J., concurring).

[116] *Id.* at 1227.

[117] *Id.*

against some user groups while allowing other groups to post content more permissively. Making matters even worse, Twitter and Facebook exercise viewpoint discrimination against the same general type of users, effectively shutting entire views out of the conversation on a national or global scale.[118] This could lead to an undue influence on the electorate.[119]

"Government enterprises . . . shouldn't decide which organizations or ideas should be favored and which ones handicapped in public debates."[120] Likewise, private social media companies should not "decid[e] what Americans can say in a particular medium of public communication."[121] Discrimination on social media platforms is a key concern because it disadvantages some to the advantage of others in terms of access to what purportedly is an open-access good.[122] Considering that at present there are few if any alternatives to Facebook and Twitter, anyone banned on both platforms is effectively shut out of the public discourse entirely.[123] Possible alternatives, such as Parler, have been swiftly shut down.[124] Considering the

---

[118] Biddle, *supra* note 65 ("The materials show Facebook offers 'an iron fist for some communities and more of a measured hand for others,' said Ángel Díaz, a lecturer at the UCLA School of Law who has researched and written on the impact of Facebook's moderation policies on marginalized communities."). Candeub, *supra* note 84; *see also* Biddle, *supra* note 65 ("The rules are 'a serious risk to political debate and free expression.'").

[119] Volokh, *supra* note 1, at 4. In fact, "[w]hen elections are closely divided, even small interference with various groups' ability to affect public opinion can make a big difference in outcomes." *Cf.* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335 (2014); *see also* Kyle Langvardt, *Will the First Amendment Scale?*, 1 UCLA J. OF FREE SPEECH L. 273, 277 (2021) (suggesting similar concerns if social media companies were to "selectively amplify[] and tamp[er] newspaper coverage get-out-the-vote messaging around competing candidates based on pure partisan preference.").

[120] Volokh, *supra* note 1, at 380.

[121] *Id.* at 385.

[122] Candeub, *supra* note 84, at 808.

[123] Although one could argue that Facebook and Twitter at least compete with each other, there is some evidence to indicate that they coordinate censorship decisions. *See* Audrey Conklin, *Hawley presses Zuckerberg on whistleblower complaint alleging Facebook coordination with Twitter, Google*, FOX BUSINESS (Nov. 17, 2020), https://www.foxbusiness.com/technology/hawley-presses-zuckerberg-on-whistleblower-complaint-alleging-facebook-coordination-with-twitter-google (describing Senator Holly's account of a whistleblower complaint). "Facebook . . . banned Trump from posting during the remainder of his term in office, and Snapchat banned him as well. YouTube suspended Trump's account, and Google took the next step of removing alternate social media website Parler from its store, with Apple threatening to do the same." Ashe Schow, *ACLU Worries About Social Media's 'Unchecked Power to Remove People From Platforms' After Twitter, Facebook Ban Trump*, DAILYWIRE (Jan. 9, 2021), https://www.dailywire.com/news/aclu-worries-about-social-medias-unchecked-power-to-remove-people-from-platforms-after-twitter-facebook-ban-trump.

[124] Jack Nicas & Davey Alba, *Amazon, Apple and Google Cut Off Parler, an App That Drew*

systemic censorship directed towards certain political views, readers no longer receive information spanning across the political spectrum, but rather only that information which unelected social media companies choose for them.[125]

Courts routinely enforce viewpoint-neutral requirements on speech regulations and therefore this requirement would be easy to administer. To prevent this harm, Section 230's liability protection should be tied to a requirement that content moderation is viewpoint-neutral. This requirement would prevent social media companies from targeting certain viewpoints for de-platforming.

B. Section 230 Might Be Unconstitutional

Section 230 also presents a constitutional conundrum. In *Norwood v. Harrison*, the Supreme Court held that it is "axiomatic" that the government "may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish."[126] Courts read Section 230 as an absolute grant of immunity to internet content providers for censorship decisions.[127] It "not only permits tech companies to censor constitutionally

---

Trump Supporters, N.Y. TIMES (Jan. 9, 2021), https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html.

[125] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2055 (2021) ("[A]dvocacy of a politically controversial viewpoint . . . is the essence of First Amendment expression") (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995)); *see also* Jeet Heer, *Tech Giants Can't Be Trusted to Police Speech,* THE NATION (Jan. 13, 2021), https://www.thenation.com/article/politics/trump-censorship-twitter-facebook/ (noting that "[t]he job of regulating incendiary discourse belongs to democratically elected governments, not powerful private interests."); E. Roaslie, *Censorship of Conservatives and the Part of the Story We're Missing: An examination of the social media purge following the Jan 6th attack on the Capitol*, MEDIUM (Jan. 15, 2021), https://medium.com/swlh/have-conservatives-been-censored-and-if-so-why-abd71bcee20c ("A healthy democracy requires tolerance of pluralism.");

[126] Norwood v. Harrison, 413 U.S. 455, 465 (1973) (quoting Lee v. Macon Cnty. Bd. of Ed., 267 F. Supp. 458, 475–76 (M.D. Ala. 1967).

[127] *See, e.g.*, Murphy v. Twitter, Inc., 274 Cal. Rptr. 3d 360, 375–76 (2021) (finding that immunizing internet content providers for deplatforing under section 230(c)(1) does not render § 230(c)(2) surplusage); Domen v. Vimeo, Inc., 433 F.Supp.3d 592, 602–603 (S.D.N.Y. 2020), *aff'd*, No. 20-616-cv, 2021 U.S. App. LEXIS 28995 (2d Cir. Sep. 24, 2021) (finding that the defendant was entitled to immunity under § 230(c)(1) because plaintiffs sought to treat defendant as a "publisher" for deleting plaintiffs' content on its website); Wilson v. Twitter, No. CV 3:20-00054, 2020 WL 3256820 (S.D. W. Va. June 16, 2020) (adopting magistrate's report and recommendation, finding that plaintiff's claims seeking to hold Twitter liable for deleting posts and suspending account based on a hateful conduct policy was barred by § 230(c)(1)); Fyk v. Facebook, Inc., 808 F. App'x 597 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1067 (2021) (holding that section 230(c)(1) immunized the

protected speech but immunizes them from liability if they do so."[128]

However, some commentators have observed that by "[u]sing a combination of statutory inducements and regulatory threats, Congress has co-opted Silicon Valley to do, through the back door, what the government cannot directly accomplish under the Constitution." [129] Internet content providers should not be free to regulate content in violation of the First Amendment when doing so at the behest of the government."[130]

The Supreme Court has "long held that the provision of such immunity can turn private action into state action."[131] In *Railway Employees' Department v. Hanson*, the Court considered a statute which immunized agreements forcing all employees to join a union from liability under state law.[132] The Court held that if private action could only occur with the power and authority of the government, then the Court would analyze that grant of power and authority as subject to the Constitution's restrictions of governmental power.[133] The Court found that "the federal statute [was] the source of the power and authority by which any private rights [were] lost or sacrificed."[134] The Court has previously analyzed preemption of state law under a First Amendment framework. The *Hanson* Court analyzed the union shop provision of the Railway Labor Act, which sought to strike down inconsistent laws in seventeen states.[135] The Court analyzed the Railway Labor Act's preemption of state law under the First Amendment because it infringed on protected interests in joining a union that the preempted state laws also sought to safeguard.[136] Although the Court ultimately found that this preemption did not violate the First Amendment in this case because individuals can be regulated once they choose to join an association, the analysis shows that parallel federal preemption of state laws that apply to private actors, such as online content providers, could run afoul of the First

---

interactive computer service based on its alleged "de-publishing" and "re-publishing" of user content); Mezey v. Twitter, Inc., No. 1:18-CV-21069-KMM, 2018 WL 5306769, at *1–2 (S.D. Fla. Jul. 19, 2018) (alleging Twitter "unlawfully suspended [plaintiff's] Twitter account" dismissed on grounds of § 230(c)(1) immunity).

[128] Vivek Ramaswamy & Jed Rubenfeld, *Save the Constitution from Big Tech*, WALL ST. J. (Jan. 11, 2021), https://www.wsj.com/articles/save-the-constitution-from-big-tech-11610387105.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] Ry. Emp. Dep't v. Hanson, 351 U.S. 225, 231 (1956).

[133] *Id.*; *cf.* Smith v. Allwright, 321 U.S. 649, 663 (1944).

[134] *Hanson*, 351 U.S. at 232 (citing Steele v. Louisville & N.R. Co., 323 U.S. 192, 198–99 (1944)); Brotherhood of R.R. Trainmen v. Howard, 343 U.S. 768, 772 (1952); Public Utils. Comm'n of District of Columbia v. Pollak, 343 U.S. 451, 462 (1952)).

[135] *Hanson*, 351 U.S. at 233.

[136] *Id.*

Amendment.[137]

Similarly, in *Skinner v. Railway Labor Executives Association*, the Court found state action in the conferral of immunity to conflicting state laws.[138] The *Skinner* Court found that when a private party acts as an instrument or agent of the government, actions they take may be subject to constitutional scrutiny.[139] The Court explained that a private actor could act as an instrument or agent of the government, even if the government did not compel those actions, if the government preempts state laws that would otherwise apply to the private actions.[140] The federal statutes at issue in *Skinner* and *Hanson*, similar to Section 230, "protected certain private parties from lawsuits if they engaged in the conduct Congress was promoting."[141] Thus, in a similar manner, Section 230's grant of immunity could unconstitutionally preempt state laws.

Section 230 may also unconstitutionally allow government coercion of private actors to suppress speech. "Congressional Democrats have repeatedly made explicit threats to social media giants if they failed to censor speech those lawmakers disfavored."[142] And the Democrats chairing the committees and subcommittees that held hearings on tech companies in recent years have made those threats as a matter of public record.[143] In fact, even a basic Google search yields results of politicians threatening "to take away a broad tech liability protection for online platforms that knowingly publish demonstrably false" information.[144] The term "false information" seems to be both broad and vague, leaving the government wide latitude to punish companies publishing information it deems "false." This confluence of government coercion and legally enacted liability protection constitutes state action.[145] It

---

[137] *Id.*

[138] Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989).

[139] *Id.*

[140] *Id.*

[141] Ramaswamy & Rubenfeld*, supra* note 129.

[142] *Id.*

[143] Glenn Greenwald, *Congress Escalates Pressure on Tech Giants to Censor More, Threatening the First Amendment*, GREENWALD (Feb. 20, 2021), https://greenwald.substack.com/p/congress-escalates-pressure-on-tech; *see also* Ramaswamy & Rubenfeld, *supra* note 128 **(**noting that Louisiana Rep. Cedric Richmond warned Facebook and Google that they had better restrict what he and his colleges saw as harmful content or face regulation) (internal quotations omitted).

[144] Sayta Marar, *Democrats' new bill targeting 'fake news' threatens free speech,* WASHINGTON EXAMINER (Mar. 6, 2020), https://www.washingtonexaminer.com/opinion/democrats-new-bill-targeting-fake-news-with-section-230-rollback-threatens-free-speech.

[145] Volokh, *supra* note 1. ("[P]latform-imposed restrictions that stem from behind-the-scenes governmental pressure can be especially dangerous") (citing Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51 (2015)).

is axiomatic that government coercion combined with a liability shield is state action. In turn, a state action of giving private online content providers Section 230 liability protection combined with government coercion leads to an unconstitutional result.

Section 230 makes these threats especially problematic, as courts have somehow read the statute to give digital platforms immunity even for bad-faith removal of third-party content.[146] Courts derive this immunity from Section 230(c)(1).[147] If courts instead derived immunity from Section 230(c)(2)(A), internet content providers would only have protection for removing content in good faith.[148] Courts' current reading of immunity under Section 230(c)(1), renders Section 230(c)(2)(A) superfluous and nullifies the threat of private lawsuits, which are a key deterrent to prevent platforms' acquiescence to unconstitutional government threats.[149] However, given that this reading seems to be the dominant interpretation, internet content providers can freely acquiesce to political demands for censorship and victims are left with no recourse.

The Whole Act Rule dictates that judges must avoid "interpreting a provision in a way that would render other provisions of the Act superfluous or unnecessary," as statutory interpretation is a holistic endeavor.[150] By

---

[146] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14–18 (2020) (Thomas, J., statement respecting denial of certiorari).

[147] *See*, *e.g.*, Murphy v. Twitter, Inc., 274 Cal. Rptr. 3d 360, 375–76 (2021) (finding that immunizing internet content providers for de-platforming under section 230(c)(1) does not render § 230(c)(2) surplusage); Domen v. Vimeo, Inc., 433 F.Supp.3d 592, 602–03 (S.D.N.Y. 2020), *aff'd,* 991 F.3d 66 (2d Cir. 2021) (finding that the defendant was entitled to immunity under § 230(c)(1) because plaintiffs sought to treat defendant as a "'publisher'" for deleting plaintiffs' content on its website); Wilson v. Twitter, No. 3:20-cv-00054, 2020 WL 3256820, at *1 (S.D. W. Va. June 16, 2020), (adopting magistrate's report and recommendation finding that plaintiff's claims seeking to hold Twitter liable for deleting posts and suspending account was based on a hateful conduct policy barred by § 230); Fyk v. Facebook, Inc., 808 F. App'x 597, 598 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1067 (2021) (holding that section 230(c)(1) immunized the interactive computer service based on its alleged "de-publishing" and "re-publishing" of user content); Mezey v. Twitter, Inc., No. 1:18-cv-21069-KMM, 2018 U.S. Dist. LEXIS 121775, at *1–2 (S.D. Fla. Jul. 19, 2018) (alleging Twitter "unlawfully suspended [plaintiff's] Twitter account" dismissed on grounds of § 230(c)(1) immunity).

[148] *Id.*

[149] Some courts, however, have instead rooted protection for deplatforming in section 230(c)(2). *See, e.g.,* Domen v. Vimeo, Inc., 991 F.3d 66, 73 (2d Cir. 2021) (finding that "Section 230(c)(2) immunizes from liability providers and users of interactive computer service who voluntarily make good faith efforts to restrict access to material they consider to be objectionable.") (quoting Green v. Am. Online (AOL), 318 F.3d 465, 472 (3d Cir. 2003)).

[150] Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or., 515 U.S. 687, 698 (1995) (applying cannon of interpretation disfavoring readings of statutes that render statutory language surplusage); Filler v. Hanvit Bank*,* 378 F.3d 213, 220 (2d Cir. 2004) (finding that

deriving immunity for internet content providers from only Section 230(c)(1), Section 230(c)(2)(A) is read out of the statute and the provision is nullified.[151] This reading makes Section 230(c)(2)(A) surplusage, which is against the canons of construction.[152] This broad-based grant of immunity can allow internet content providers to abuse their de-platforming power.

This abuse of de-platforming power has garnered global disdain and generated pressure from international governments, particularly in Europe.[153] This pressure is significant because EU laws generally allow for much more speech regulation than what the U.S. law allows.[154] In this case, even the EU saw social media policing as a step too far in banning speech.[155] "German Chancellor Angela Merkel called Twitter's decision to impose a permanent ban on a U.S. President problematic."[156] Chancellor Merkel's spokesperson, Steffen Seibert, added that "[t]his fundamental right can be intervened in, but according to the law and within the framework defined by legislators—not according to a decision by the management of social media platforms."[157]

---

a basic canon of statutory interpretation, which is equally applicable to interpreting treaties, is to avoid readings that 'render statutory language surplusage' or 'redundant.').

[151] *Id.*

[152] *Id.*

[153] Clara Hendrickson & William A. Galston, *Big tech threats: Making sense of the backlash against online platforms*, BROOKINGS (May 28, 2019), https://www.brookings.edu/research/big-tech-threats-making-sense-of-the-backlash-against-online-platforms/ (explaining that "[a] growing international consensus holds that the ways in which today's dominant online platforms are currently designed poses an inherent threat to democracy. Countries around the world have responded to this growing threat by launching investigations, passing new laws, and commissioning reports. Europe has responded forcefully to protect users' online privacy, bolstering its already robust set of privacy laws").

[154] Committee of Ministers, Hate Speech Recommendation No. R (97) 20 (1997).

[155] Recently, France cited hate speech laws to quash the speech of 12 pro-Palestinian activists who wore t-shirts that advocated a boycott of Israel. Benjamin Dodman, *France's criminalisation of Israel boycotts sparks free-speech debate*, FRANCE 24 (Jan. 21, 2016), https://www.france24.com/en/20160120-france-boycott-israel-bds-law-free-speech-antisemitism. Cases in Turkey are common where citizens have been prosecuted under hate speech laws for criticizing government officials or the military. *See, e.g.*, Sürek v. Turkey (No. 1) (Application no. 26682/95) (Eur. Ct. H.R. Jul. 8, 1999), https://hudoc.echr.coe.int/eng#%7B%22dmdocnumber%22:%5B%22696156%22%5D,%22itemid%22:%5B%22001-58279%22%5D%7D.

[156] AFP, *Twitter's 'problematic' Trump ban troubles Europe,* EURACTIV (Jan. 11, 2021), https://www.euractiv.com/section/global-europe/news/twitters-problematic-trump-ban-troubles-europe/.

[157] Jason Lemon, *Angela Merkel Calls Trump Twitter Ban Problematic as Freedom of Opinion Is Fundamental Right*, MSN (Jan. 11, 2021) https://www.msn.com/en-us/news/world/angela-merkel-calls-trump-twitter-ban-problematic-as-freedom-of-opinion-is-fundamental-right/ar-BB1cEQZa (quoting Steffen Seibert, a spokesperson for Chancellor Merkel).

"Contrary to the claim that these internet giants can be trusted to police themselves, they face continuous accusations of politicization and unfair censorship."[158] French Economy and Finance Minister Bruno Le Maire explained that, "[t]he regulation of digital giants cannot be done by the digital oligarchy itself."[159] "European commissioner Thierry Breton, who introduced two EU proposals that would place more restraints on internet content providers, saw Twitter's decision as a total break from the past, calling it 'the 9/11 moment of social media.'"[160] Although faced with such scrutiny and pressure, social media companies have failed to address these concerns.[161] Social media companies, therefore, "have become the free expression's weakest link."[162]

"[A]lthough a private entity is not ordinarily constrained by the First Amendment, it is if the government coerces or induces it to take action the government itself would not be permitted to do, such as censor expression of a lawful viewpoint."[163] Justice Thomas in his *Biden v. Knight* concurrence considered government threats: "[p]eople do not lightly disregard public officers' thinly veiled threats to institute criminal proceedings against them if they do not come around."[164] He noted that "[t]he government cannot accomplish through threats of adverse government action what the Constitution prohibits it from doing directly."[165] He suggested that "plaintiffs might have colorable claims against a digital platform if it took adverse action against them in response to government threats."[166]

Other commentators also argue that Section 230 could be unconstitutional

---

[158] Candeub, *supra* note 84, at 391; *cf* Cara J. Ottenweller, *Note, Cyberbullying: The Interactive Playground Cries for A Clarification of the Communications Decency Act*, 41 VAL. U. L. REV. 1285, 1300 (2007).

[159] *Twitter's "Problematic" Trump Ban Troubles Europe*, EURACTIV (Jan. 12, 2021), https://www.euractiv.com/section/global-europe/news/twitters-problematic-trump-ban-troubles-europe/.

[160] *Id.*

[161] Candeub, *supra* note 84 ("Seth Kreimer foresaw how '[r]ather than attacking speakers or listeners directly, governments [will] enlist private actors within the chain as proxy censors to control the flow of information' on the internet.") (citing Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 14 (2006)).

[162] Candeub, *supra* note 84 (citing Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018)).

[163] Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1221 (2021) (Thomas, J., concurring) (quoting Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921, 1944 (2019)).

[164] *Id.* (Thomas, J., concurring) (citing Bantam Books, Inc. v. Sullivan, 372 U. S. 58, 68 (1963)).

[165] *Id.* (citing Blum v. Yaretsky, 457 U. S. 991, 1004–05 (1982)).

[166] *Id.*

for a different reason.[167] Section 230 grants immunity to online content providers, which preempts state laws that may grant a cause of action to protect speech from private censorship.[168] These commentators argue that this preemption infringes on speech that the *Cubby* and *Stratton* framework intended to protect.[169] Under this view, *Cubby* and *Stratton* created a judicially cognizable speech right and recognized violations by internet content providers that breached that right.[170] Section 230, however, puts this speech at risk, as private companies can now censor that speech without fear of a private action. In the same way, the federal preemption of state tort law through Section 230 could be unconstitutional.[171]

VI. SOLUTIONS

Historically, the government has had wide latitude to regulate public goods.[172] This latitude could justify tying Section 230 immunity to a viewpoint moderation requirement. This section focuses on the concepts of public goods and common carriers as applied to social media.

A. Public Goods

Social media platform technologies are public goods and should be regulated as such. "Economists define a public good as (i) non-rivalrous, meaning that consumption of a good does not reduce availability to others and (ii) non-excludable, meaning that one cannot provide the good without others being able to enjoy it."[173] Typical examples include police protection, environmental protection, and flood protection. Most public services meet the economic definition of public good. One's enjoyment of police or fire

---

[167] *See e.g.,* Eugene Volokh, *Might Federal Preemption of Speech Protective State Laws Violate the First Amendment? The Volokh Conspiracy*, REASON (Jan. 23, 2021), https://reason.com/volokh/2021/01/23/might-federal-preemption-of-speech-protective-state-laws-violate-the-first-amendment/**;** Vivek Ramaswamy & Jed Rubenfeld, *Save the Constitution from Big Tech*, WALL ST. J. (Jan. 11, 2021), https://www.wsj.com/articles/save-the-constitution-from-big-tech-11610387105.

[168] Volokh, *supra* note 1.

[169] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1996).

[170] *Id.*

[171] Volokh, *supra* note 1.

[172] *See* German Alliance Ins. Co. v. Lewis, 233 U. S. 389, 411 (1914).

[173] *Id.* (citing James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 41–42 (2003); Richard A. Epstein, *The Disintegration of Intellectual Property? A Classical Liberal Response to a Premature Obituary*, 62 STAN. L. REV. 455, 457–58 (2010).

protection does not impinge upon another's enjoyment of the same, so these goods are non-rivalrous. Similarly, one cannot exclude another from receiving those services, which makes them non-excludable.

Universal communications platforms, such as social media, are public goods.[174] Unlike most private goods, communications platforms, like many other public goods, increase in value as more people use them.[175] Universal communications forums also create spaces for expression. Such forums are important as a means for the "government to explain itself to citizens—and citizens to express themselves to government and fellow citizens."[176] Those communications platforms are "therefore necessary for democracy and democratic institutions, which are themselves a public good."[177] Universal communications platforms provide a further benefit by lowering "search costs for finding suitable goods and services and their associated transaction costs."[178] Such rationale justified the Constitution's direction that the federal government create the post office as a public good.[179] It was also the rationale behind early Congresses to placing price controls on "newspapers so that citizens could learn about and participate in politics and national issues."[180] Congress may have felt comfortable enacting these price controls, notwithstanding the Founders' preference for free markets, due to the fact that it viewed newspapers as a public good necessary to educate the public.[181] Today, social media platforms serve many of the roles that newspapers served in keeping the public informed and are also a public good that may be subject to reasonable regulation as common carriers.

---

[174] *Id.*

[175] *Id.; see also Network Effects – definition and examples*, ECONOMICSHELP. https://www.economicshelp.org/blog/glossary/network-effects/ (last visited December 1, 2021); Caroline Banton, *Network Effect*, INVESTOPEDIA (Apr. 3, 2021), https://www.investopedia.com/terms/n/network-effect.asp (explaining that "the network effect occurs when a good or service becomes more valuable as more people use it").

[176] *Id.*

[177] *Id.* ("Above all, a universal communications platform allows for democratic self-government by promoting free speech. George Washington emphasized the value of 'political intelligence and information,' and James Madison argued that in democratic society the 'easy and prompt circulation of public proceedings is peculiarly essential.'") (citing RICHARD B. KIELBOWICZ, NEWS IN THE MAIL: THE PRESS, POST OFFICE, AND PUBLIC INFORMATION, 1700-1860S 34 (Greenwood, 1989)).

[178] *Id.*

[179] *Id.* (noting that the "United States Constitution, Article I, Section 8, Clause 7 empowers Congress [t]o establish Post Offices and Post Roads") (internal quotes omitted).

[180] *Id.* (citing C. Edwin Baker, *Turner Broadcasting: Content-Based Regulation of Persons and Presses*, 1994 S. CT. REV. 57, 98 (1994); David M. Rabbant, *The First Amendment in Its Forgotten Years*, 90 YALE L.J. 514, 528 (1981).

[181] Samuel Fleischacker, *Adam Smith's Reception among the American Founders, 1776-1790*, 59 THE WILLIAM AND MARY Q. 4, 897–924 (2002), https://www.jstor.org/stable/3491575.

B. Applying Common Carrier Doctrine to Social Media

Justice Thomas, in his *Biden v. Knight* concurrence, considered whether common carriers or public accommodation status could justify heavier regulation of digital platforms to prevent free speech violations.[182] He expressed that scholars differ on when a business should be treated as a common carrier. Some say "common-carrier regulations are justified only when a carrier possesses substantial market power."[183] "Others have said that no substantial market power is needed so long as the company holds itself out as open to the public."[184] In prior cases, the Court has clarified that even if historically an industry had not been considered a common carrier, it could be recognized as a common carrier if "by circumstances and its nature, [the industry can] rise from private to be of public concern."[185]

Justice Thomas further expressed that the solution to "private, concentrated control over online content and platforms available to the public . . . may be found in doctrines that limit the right of a private company to exclude."[186] Historically, common carrier and public accommodation doctrines have limited a company's right to exclude, subjecting it to special regulations, including a general requirement to serve all comers.[187]

Transportation and communications provide the prototypical examples of common carriers, and courts and legislators have deemed other industries as common carriers by analogy to these industries. For example, telegraphs have been deemed to be common carriers because they were similar to "railroad companies and other common carriers [that] were bound to serve all customers alike, without discrimination."[188]

Although private companies are not regulated by the First Amendment, "[i]n many ways, digital platforms that hold themselves out to the public resemble traditional common carriers," which have restrictions on their

---

[182] Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1221–27 (2021) (Thomas, J., concurring).
[183] *Id.* (citing Candeub, *supra* note 84).
[184] *Id.*; *see also* Ingate v. Christie, 3 Car. & K. 61, 63, 175 Eng. Rep. 463, 464 (N. P. 1850) ("[A] person [who] holds himself out to carry goods for everyone as a business . . . is a common carrier").
[185] *See* German Alliance Ins. Co. v. Lewis, 233 U. S. 389, 411 (1914) (affirming state regulation of fire insurance rates). At that point, a company's "property is but its instrument, the means of rendering the service which has become of public interest." *Id*. at 408.
[186] *Biden*, 141 S. Ct., at 1222 (Thomas, J., concurring).
[187] Candeub, *supra* note 84, at 398–403; *see also* CK Burdick, *The Origin of the Peculiar Duties of Public Service Companies, Pt. 1*, 11 COLUM L. REV. 514, 521–26 (1911).
[188] *See* Primrose v. Western Union Tel. Co., 154 U. S. 1, 14 (1894) (internal quotations omitted).

ability to exclude.[189] Justice Thomas noted that "[t]here is a fair argument that some digital platforms are sufficiently akin to common carriers or places of accommodation to be regulated in this manner."[190] He compared the modern day internet's information infrastructure to traditional phone wire networks, both connecting people in the same way.[191] There is no fundamental difference between digital and physical platforms because both are "communications networks . . . carry[ing] information from one user to another."[192]

Common carrier obligations are often accompanied with favored government treatment.[193] Governments, for example, "have tied restrictions on a carrier's ability to reject clients to immunity from certain types of suits or to regulations that make it more difficult for other companies to compete with the carrier (such as franchise licenses)."[194] Because these companies provide something akin to a government service, they therefore must also respect limitations on their ability to exclude. The dominant market share held by the major internet content providers in combination with the fact that they "derive much of their value from network size," further counsels treating these companies as common carriers as it is difficult if not impossible for competitors to enter and expand.[195]

Justice Thomas noted that "[t]he Facebook suite of apps is valuable largely because [three] billion people use it," while "Google search—at 90% of the market share—is valuable relative to other search engines because more people use it, creating data that Google's algorithm uses to refine and improve search results."[196] Justice Thomas observed that although the profit margin of these platforms are astronomically high—a condition which generally "would induce new entrants into the market"—"substantial barriers to entry" prohibit competition.[197] In considering network effects, Justice Thomas noted that dominant digital platforms are dramatically different because of the concentration of power that a small number of people wield,

---

[189] *Biden*, 141 S. Ct. at 1224 (Thomas, J., concurring) (citing United States v. Stevens, 559 U. S. 460, 468 (2010)). Interfering "with the author's communication to those who deliberately subscribe to the account" by removing an account or deleting a post "is similar to a phone company's decision to cancel a phone line[; i]t seems . . . reasonable to impose a common carrier requirement that prevents such decisions." Volokh, *supra* note 1, at 29.
[190] *Biden*, 141 S. Ct. at 1224 (Thomas, J., concurring).
[191] *Id.*
[192] *Id.*
[193] Candeub, *supra* note 84, at 402–07.
[194] *Biden*, 141 S.Ct. at 1223 (Thomas, J., concurring) (internal quotations omitted).
[195] *Id.* at 1224.
[196] *Id.*
[197] *Id.*

giving enormous control over speech.[198] He further noted that, unlike dominant digital platforms, ownership of other digital spheres, such as the email protocol, is much more decentralized."[199] This dominance is concerning as it gives these digital platforms great ability to censor users who would have no other recourse. Arguably, users can try workarounds to avoid these harms, as "these platforms are not the sole means for distributing speech or information."[200] For example, one can write a blog, but it would not have the reach of established social media platforms and is therefore not a comparable alternative. If no comparable alternatives exist, "a company exercises substantial market power."[201] And as Justice Thomas observed, there are no comparable alternatives currently in existence "[f]or many of today's digital platforms." [202]

Section 230's grant of immunity to social media companies does not come coupled with any obligations.[203] One of the enumerated purposes of Section 230 was "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services."[204] Social media companies have obstructed this purpose through one-sided content moderation.[205] Section 230, therefore, should be modified to require viewpoint-neutral moderation. Such a modification would be in line with historical sticks placed upon common carriers in exchange for their carrots of liability protection.

Internet content providers purport that they are taking down content that violates their policies. However, some commentators say that, in the aggregate, these platforms' high-profile de-platforming decisions lean against conservatives.[206] This may suggest that content moderation is being

---

[198] *Id.*
[199] *Id.*
[200] *Id.* at 1225.
[201] *Id.*
[202] *Id.*
[203] Adam Candeub, *The Common Carrier Privacy Model*, 51 U.C.D. L. REV. 805, 813 (2018).
[204] 47 U.S.C. § 230(b)(3).
[205] Abby Ohlheiser, *Just how offensive did Milo Yiannopoulos have to be to get banned from Twitter?*, WASH. POST (Jul. 21, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/07/21/what-it-takes-to-get-banned-from-twitter/; Editorial Board, *Facebook Keeps Banning Trump*, WALL ST. J. (May 5, 2021), https://www.wsj.com/articles/facebook-keeps-banning-trump-11620255813; Bret Molina, *Facebook ban on Trump upheld: Here's how everyone is reacting*, MSN (May 5, 2021), https://www.msn.com/en-us/news/politics/facebook-ban-on-trump-upheld-heres-how-everyone-is-reacting/ar-BB1go70a.
[206] Natalie Musumeci, *Twitter bans blogger Jim Hoft, conservative radio host Wayne Allyn Root*, N.Y. POST (Feb 8, 2021), https://nypost.com/2021/02/08/twitter-bans-conservatives-

conducted on the basis of viewpoint. Internet content providers may contend that they do not discriminate on the basis of viewpoint and that a viewpoint-neutral requirement would place a large burden on them. This pushback lacks credibility because social media companies that do not discriminate on the basis of viewpoint will continue to receive Section 230 protection.

C. A New Section 230 Deal

Section 230 should function as other grants of immunity do: by granting sticks and carrots. As it stands, Section 230 grants the massive carrot of liability immunity without a corresponding stick. If the concern is the systematic bias of tech companies in speech suppression, a simple solution would be to mandate tech companies to regulate in a viewpoint-neutral manner. Given that a social media company is a public good or a common carrier without any available alternative, additional regulation in this is more than warranted.

1. Section 230 Needs Sticks

Section 230 is straightforward in that internet platforms receive immunity for third-party content.[207] This liability relief encourages the posting of third-party, user-generated content and thus furthers the free flow of ideas.[208] Legislators intended to give companies complete immunity so that they could create family-friendly online environments.[209]

In the nineteenth century, courts adjusted common carriage liability in the same way that modern courts adjusted internet content provider liability with

---

jim-hoft-wayne-allyn-root/; Rose Bak, *Conservatives Are Being Banned From Twitter and There's Nothing They Can Do About It*, NEWS BREAK (Jan. 31, 2021), https://www.newsbreak.com/news/2144454173752/conservatives-are-being-banned-from-twitter-and-theres-nothing-they-can-do-about-it; Jacob Palmieri, *GOP Rep: Twitter Banned At Least 60K Conservative Accounts*, THE PALMIERI REPORT (Jan. 9, 2021), https://thepalmierireport.com/gop-rep-twitter-banned-at-least-60k-conservative-accounts/; *Twitter suspends more conservative and pro-Trump accounts prompting new accusations of censorship*, RT USA NEWS (May 7, 2019), https://www.rt.com/usa/458669-twitter-bans-conservative-accounts/; Jeff Dunetz, *Twitter Bans 10 Conservatives Accounts, Gives No Reason*, CONSERVATIVEFIRINGLINE (Oct. 4, 2018), https://conservativefiringline.com/twitter-bans-10-conservatives-accounts-gives-no-reason/.

[207] 47 U.S.C. § 230.

[208] *See* Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting Section 230 Immunity*, 30 BERKELEY TECH. L.J. 1505, 1519–23 (2015).

[209] *See* 47 U.S.C. § 230(b)(4) (providing that one of § 230's policy goals is to empower parents to restrict children's access to objectionable online material).

Section 230.[210] "Under the old, common carriage strict liability rule, telegraph companies were liable for all damages resulting from an undelivered or misdelivered telegraph."[211] The large potential damages for a mistyped telegraph message needed to be curtailed because it was so easy for someone sending the telegraph to make mistakes and blame it on the carrier.[212] For example, "a mistaken telegram that says buy 50,000 pork bellies rather than 5,000 pork bellies could be an enormous liability." Therefore, "the court lowered the liability standard, limiting normal misdelivery liability to the cost of the telegraph."[213]

"The internet transformed from the dial-up curiosity of bulletin boards, stock quotes and file sharing into the dominant engine of global communications."[214] As content service providers became fewer and gained power, it quickly became evident that Section 230's protections required restraints.[215] Unlike the telegraph and telephone companies, which not only enjoyed immunity but faced obligations such as "refrain[ing] from discrimination, carr[ying] all lawful messages, or provid[ing] public good[s]," modern day Internet content providers have "enjoyed special immunity against" publisher liability without those obligations.[216] The absurdity of that distinction is even more pronounced with the realization that "they function as the dominant communications of their time, just like telegraphs and telephones once did."[217] The government should therefore use sticks to ensure that these dominant companies cannot shut out one side of the debate.

2. Viewpoint-Neutral Moderation Tied to Section 230 Limited Liability

Section 230's liability protection initially made sense to ensure that online content providers would not take down content in order to limit liability. Today, however, online content providers regularly take down content.[218]

---

[210] Candeub, *supra* note 84, at 391 (stating that courts also eliminated liability for service outage in the twentieth century "because this liability protection was viewed as part of a deal that included reduced telephone rates and allowed universal service." (internal citations omitted)). It is also analogous to relaxation of liability for wire services and conduits. *Id.*

[211] *Id.* at 422 (citing *In re* Vehicle Carrier Servs. Antitrust Litig., 846 F.3d 71 (3d Cir. 2017) (holding that the Shipping Act immunizes certain ocean shippers from private antitrust suits based on the Shipping Act.)).

[212] *Id.*

[213] *Id.* (citing Candeub, *supra* note 203, at 813).

[214] *Id.*

[215] *Id.* at 422, 429.

[216] *Id.* at 422.

[217] *Id.* (noting that "the modern internet behemoths continue to enjoy a "liability freebie" granted to their pioneering predecessors")

[218] Isobel Asher Hamilton, *Facebook warns it can remove any content that might put it at*

What justifies a liability shield in this circumstance? For the reasons discussed in Part III, social media companies should not suppress unfavorable views. Tying the liability protection to viewpoint-neutral moderation would ensure that they do not.[219]

Supreme Court precedent explains that:

> [w]hen the government targets not subject matter, but particular views taken by speakers on a subject, [it is]…an egregious form of content discrimination. The government must abstain from regulating speech when the specific motivating ideology or the opinion or perspective of the speaker is the rationale for the restriction.[220]

Courts routinely apply clear tests to identify viewpoint and content discrimination.[221] Courts usually find content discrimination "whenever a government regulates 'particular speech because of the topic discussed or the idea or message expressed.'"[222] Courts find viewpoint discrimination when a government targets "particular views taken by speakers on a subject."[223] Viewpoint discrimination can be distinguished as "an egregious form of content discrimination."[224]

Viewpoint-neutral moderation would be easily administrable and enforceable by courts. At first glance, it may seem that viewpoint-neutral moderation would be difficult to administer, however courts regularly apply these rules in First Amendment jurisprudence and can therefore easily apply the same analysis to online content providers.[225] Whether an information

---

regulatory or legal risk, BUSINESS INSIDER (Sept. 1, 2020, 6:09 AM), https://www.businessinsider.com/facebook-remove-content-regulatory-legal-risk-2020-9?op=1; Ariana Tobin, Madeleine Varner & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, PROPUBLICA (Dec. 28, 2017, 5:53 PM EST), https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes.

[219] Curt Levey, *How Social Media Giants Can Solve Their Speech Problems with The First Amendment*, THE FEDERALIST (Feb. 1, 2021), https://thefederalist.com/2021/02/01/how-social-media-giants-can-solve-their-speech-problems-with-the-first-amendment/.

[220] Rosenberger v. Rector & Visitors of the Univ. of Va., 515 U.S. 819, 829 (1995) (internal citation omitted).

[221] Iancu v. Brunetti, 139 S. Ct. 2294, 2313 (2019) (Sotomayor, J., concurring in part).

[222] *Id.* (quoting Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015)).

[223] *Rosenberger*, 515 U.S. at 829.

[224] *Id.*

[225] Widmar v. Vincent, 454 U.S. 263, 280–81 (1981) (Stevens, J., concurring) (finding that a university engaged in viewpoint discrimination when allowing "a group of Republicans or Presbyterians to [speak on campus] while denying Democrats or Mormons the same privilege"); *see also* Good News Club v. Milford Cent. Sch., 533 U.S. 98, 121 (2001) (Scalia,

content provider has a viewpoint-neutral content moderation policy could be determined by federal courts on a case-by-case basis.

3. Viewpoint-Neutral Moderation Safe Harbor

Section 230's viewpoint-neutral moderation requirement should only apply to internet content providers large enough to be considered a public accommodation or common carrier. Larger companies presumably have the available resources to monitor and moderate content to comply with viewpoint moderation but such a change to the law could potentially discourage smaller entrants into the market. Smaller businesses trying to grow should not be burdened with potential costs of compliance, as those costs may stifle competition instead of promoting growth. Hiring firms or in-house counsel may be costly when starting up, and compliance costs could drive small businesses out of the market altogether. Therefore, any revision to Section 230 should include a safe harbor so that businesses that are too small to be common carriers or public goods could apply for Section 230 immunity regardless of their content moderation policies.

VII. CONCLUSION

"Diversity of opinion is the lifeblood of democracy."[226] If we "insist that everyone think the same way we think, our democratic way of life is in danger." [227] The First Amendment protects its citizens from government interference but does not generally apply its protections to limitations on free speech by private companies. Modern internet content providers now control

---

J., concurring) (holding that a school's denial of after-school meeting space to club that wanted to discuss permissible topics, like child rearing, from a religious perspective was not viewpoint- neutral); *Rosenberger*, 515 U.S. at 837 (finding that university's refusal to pay printing fees for student newspaper publishing on permissible topics from a religious perspective was viewpoint discriminatory); Lamb's Chapel v. Ctr. Moriches Union Free Sch. Dist., 508 U.S. 384, 384–85 (1993) (finding that school's denial of after-school meeting space to church to screen films with religious views on permissible topics, like family values, violated viewpoint neutrality).

[226] Joseph Choi, *New York Times dropping 'op-eds' for 'guest essays'*, MSN (Apr. 26, 2021) https://www.msn.com/en-us/news/politics/new-york-times-dropping-op-eds-for-guest-essays/ar-BB1g4HZY (quoting New York Times Opinion editor John B. Oakes); *see also* Daniel Greenfield, *Now That Everything is "Opinion", New York Times Drops Op-Ed Term*, FRONTPAGE MAG (Apr. 27, 2021), https://www.frontpagemag.com/point/2021/04/now-everything-opinion-new-york-times-drops-op-ed-daniel-greenfield/; Nancy Smith, *Letter: Two opposites can be true at the same time*, TUCSON (Apr. 29, 2021), https://tucson.com/opinion/letters/letter-two-opposites-can-be-true-at-the-same-time/article_1e36af9c-a7c0-11eb-9508-b3139bcafcea.html.

[227] Choi, *supra* note 226 (quoting New York Times Opinion editor John B. Oakes).

the most commonly used spaces of debate; spaces that our Founding Fathers no doubt would have intended to protect. As a policy matter, large internet content providers like Facebook, Twitter, and Google should follow First Amendment Free Speech doctrines. Additionally, the internal policies that these internet content providers employ should be transparent and applied evenhandedly.

Section 230's liability protections provided a beneficial and even necessary purpose of allowing the Internet to grow and thrive for much of its early existence. Today, however, this is no longer the case. Social media giants now censor entire viewpoints with impunity, resting in the comfort of knowing that their victims will have no recourse due to protections afforded by Section 230.

Legislators could apply a straight-forward solution. In exchange for the Section 230 liability immunity enjoyed by these internet content providers, the government should require companies to maintain viewpoint-neutral content-moderation policies but carve out a safe harbor for small businesses to encourage new growth.

THE USE OF GENETIC GENEALOGY IN SOLVING CRIMES: WHAT LIMITS FOR GENETIC PRIVACY?

Grant J. Tucek*

DNA technology has rapidly progressed to enable everything from catching criminals from crime scene evidence to identifying health conditions to which an individual may be predisposed and locating unknown blood relatives. In 2018, all three advancements crossed paths when law enforcement identified a serial killer by submitting a crime scene DNA sample to a public, commercial database intended for genealogy research.

The new industry of at-home DNA testing kits has resulted in private and public databases containing millions of genetic profiles. Until recently, private individuals used these services to analyze medical predispositions and find family members with traditional genealogical research. The arrest of the Golden State Killer, and dozens of other rapists and murderers in the following years, has demonstrated the utility in searching the larger population for matches to crime scene DNA rather than only known criminals in law enforcement databases.

This new methodology, however, presents issues of how the law adapts to technology and the balance between security and privacy. Catching criminals with scientifically proven evidence benefits the criminal justice system, victims, and society. But genetic genealogy is a powerful tool that involves the government searching genetic profiles and prying through people's private information.

This Comment proposes continued use of genetic genealogy, subject to statutory and judicial limitations. Genetic genealogy has only been used to solve violent felonies and to identify human remains. In the absence of regulation or legal precedent, the status quo relies on self-enforced limitations of law enforcement and private industry. The dangers of letting genetic genealogy go unchecked are twofold: government search of private DNA databases may expand too far into privacy interests, or courts may overturn cases using this method inappropriately and allow violent criminals to go free. Genetic genealogy should only be used to catch violent felons who cannot be identified through traditional law enforcement investigations, with databases that clearly inform users of law enforcement searches.

TABLE OF CONTENTS

*Grant J. Tucek is a commercial litigation associate at Husch Blackwell LLP.

I. INTRODUCTION

"You'll be silent forever, and I'll be gone in the dark."[1]

The man who told this to his victims committed over fifty rapes and at least thirteen murders between 1974 and 1986.[2] He was known by numerous names—the Visalia Ransacker, East Area Rapist, Original Night Stalker, and Golden State Killer—during different crime sprees, which were only

[1] MICHELLE MCNAMARA, I'LL BE GONE IN THE DARK: ONE WOMAN'S OBSESSIVE SEARCH FOR THE GOLDEN STATE KILLER 328 (2017).
[2] Megan Molteni, *The Creepy Genetics Behind The Golden State Killer Case*, WIRED, https://www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics (Apr. 2, 2018).

connected years later, as survivors continued to fear his return.[3] The Visalia Ransacker terrorized a small town in California from 1974 to 1975, committing over one hundred burglaries, killing the father of a teenage girl whom he attempted to kidnap,[4] and shooting out a pursuing police officer's flashlight.[5] The burglaries were unusual, to say the least—the burglar stole family photographs, wedding rings, and just one earring from a pair, leaving behind cash and items that would normally be of greater value to the typical burglar looking for money.[6] More distinctive were the meticulous precautions he took—he opened multiple windows in a house in case the residents returned while he was there, and he created makeshift alarms by placing breakable items on doorknobs.[7] Detectives and law enforcement agencies disagreed for decades whether the Visalia Ransacker went on to commit other crime sprees, but the Sacramento County District Attorney's Office formally announced in 2018 that the Visalia Ransacker had later committed the East Area Rapist and Original Night Stalker crimes.[8]

The East Area Rapist committed over fifty rapes in Sacramento between 1976 and 1978; during this time, he murdered a couple walking their dog whom he encountered while prowling.[9] The rapist planned attacks, making hang-up phone calls to the victims and neighbors, prowling and breaking into houses, stealing photographs and jewelry, bringing pre-cut ligatures to bind victims, and unloading victims' guns before the rapes.[10] He moved through neighborhoods using drainage ditches and canals,[11] parked his car outside of standard police perimeters,[12] and once escaped on a bicycle from a victim's

---

[3] *Golden State Killer*, CRIME MUSEUM, https://www.crimemuseum.org/crime-library/famous-murders/golden-state-killer (last visited November 4, 2020).
[4] *Id.*
[5] *Attempted Homicide: The McGowen Shooting*, THE VISALIA RANSACKER, https://visaliaransacker.com/mcgowen.php (last visited November 4, 2020).
[6] McNamara, *supra* note 1, at 85-86. For discussion of this type of burglar who offends for pleasure rather than monetary gain and the link to violent crimes, *see* LB Schlesinger and E Revitch, *Sexual Burglaries and Sexual Homicide: Clinical, Forensic, and Investigative Considerations*, 27 J. AM. ACAD. PSYCH. L. 227 (1999).
[7] McNamara, *supra* note 1, at 85–86.
[8] Eric Woomer, *Sacramento police: Former Exeter cop is Visalia Ransacker*, VISALIA TIMES DELTA (Apr. 25, 2018), https://www.visaliatimesdelta.com/story/news/2018/04/25/breaking-visalia-ransacker-aka-golden-state-killer-may-behind-bars/550310002.
[9] CRIME MUSEUM, *supra* note 3.
[10] McNamara, *supra* note 1, at 2, 58, 182; Jeva Lange, *Michelle McNamara's tantalizing roadmap for finding a long lost serial killer*, THE WEEK (Mar. 19, 2018), https://theweek.com/articles/761206/michelle-mcnamaras-tantalizing-roadmap-finding-long-lost-serial-killer.
[11] McNamara, *supra* note 1, at 182.
[12] *Id.* at 67–68.

FBI agent neighbor who chased him with a car.[13]

After attacking women alone in their houses, he began attacking heterosexual couples,[14] stacking dishes on bound male victims and threatening to kill them if he heard the dishes fall, then raping the female victims.[15] He turned off air conditioners and heaters during attacks to better hear threats from his bound victims or from outside.[16] He stayed in his victims' houses for hours, taking breaks to rummage through their kitchens, eat their food, and drink their beer.[17] The attacks did not end when he left—he continued making hang-up and threatening phone calls to victims decades after his attacks.[18]

In his next crime spree, the newly-named Original Night Stalker murdered at least ten people in or near Los Angeles, hundreds of miles from Sacramento, from 1979 to 1986 during attacks with modus operandi similar to that of the East Area Rapist.[19] Some of the same patterns appeared, such as prowling reported in the neighborhoods before the attacks and the attacker bringing precut ligatures to the scene.[20] Here, though, he lost control and shot victims in several attacks when they fought back.[21] In subsequent attacks, he bludgeoned bound victims to death with their own household objects, first covering their bodies with blankets to avoid getting blood on himself.[22] After killing his final known victim in 1986, no other crimes were linked to him.[23]

In 2001, crime scene DNA evidence connected the East Area Rapist and Original Night Stalker as the same offender, together named as the Golden State Killer by a book bringing attention to the massive series of unsolved crimes.[24] Despite the rise of law enforcement DNA databases in the decades

---

[13] *Id.* at 126.
[14] *Id.* at 65-66.
[15] *Id.* at 156.
[16] *Id.* at 68.
[17] *Id.* at 69, 210.
[18] Emily Shapiro, '*Going to kill you': Hear chilling phone call allegedly made by 'Golden State Killer'*, ABC 6 NEWS (May 5, 2018) https://6abc.com/going-to-kill-you-hear-chilling-phone-call-allegedly-made-by-golden-state-killer/3410937/. For the terrifying audio recording of one phone call, *see* FED. BUREAU OF INVESTIGATION, 1977 RECORDING OF SUSPECTED EAST AREA RAPIST, https://www.fbi.gov/video-repository/ear_phone_061516.mp4/view (last visited November 4, 2020).
[19] CRIME MUSEUM, *supra* note 3.
[20] *Id.*
[21] McNamara, *supra* note 1, at 122, 150.
[22] *Id.* at 25, 100.
[23] Jenny Espino & Gretchen Wenner, *At least a dozen men and women died because of the Golden State Killer. Her"s who they were*, USA TODAY (Apr. 28, 2018), https://www.usatoday.com/story/news/nation-now/2018/04/28/golden-state-killer-murder-victims/560657002/.
[24] CRIME MUSEUM, *supra* note 3; Eli Rosenberg, *She Stalked the Golden State Killer until she died. Some think her work led to the suspect's arrest*, WASHINGTON POST (Apr. 26, 2018,

following the crimes, the samples never revealed the man's identity;[25] he had not been arrested or convicted for any crimes in the 1990s or 2000s that would put him on a law enforcement DNA database.[26]

During the 2000s, however, the use of at-home DNA kits tested by private companies for people to learn about their ancestry—genetic genealogy—grew immensely. Paul Holes, an investigator in one jurisdiction where the Golden State Killer attacked, sent a crime scene DNA sample to a lab to process it in a format that genealogy websites could utilize for finding familial matches.[27] Then, he submitted it to GEDmatch, a database of approximately one million profiles of genetic information, and found several distant relatives.[28] After eliminating others, police zeroed in on Joseph James DeAngelo, a former police officer living near Sacramento, due to his age, description, and ties to the locations of the crimes.[29] Deputies collected DeAngelo's discarded DNA, and it matched the Golden State Killer crimes.[30] Finally, police arrested DeAngelo in April 2018, more than four decades after he began his crimes.[31] DeAngelo remained in custody for over two years as attorneys prepared for trial and negotiated a plea deal.[32] Finally, DeAngelo pleaded guilty in June 2020 to thirteen murders and admitted to the rapes, for

---

12:02 AM), https://www.washingtonpost.com/news/true-crime/wp/2018/04/26/she-stalked-the-golden-state-killer-until-she-died-some-think-her-work-led-to-the-suspects-arrest.

[25] Justin Jouvenal, *To find alleged Golden State Killer, investigators first found his great-great-great grandparents*, WASH. POST (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html.

[26] *See Report: Suspected Golden State Killer Joseph DeAngelo was arrested, then released by Sacramento police in 1996*, ABC 7 NEWS (Mar. 17, 2019), https://abc7news.com/report-golden-state-killer-suspect-arrested-let-go-in-96/5201262/ ("DeAngelo was a suspect in a gas station robbery, but the charges were ultimately dismissed").

[27] Jouvenal, *supra* note 25.

[28] *Id.* Investigators found common ancestors of these relatives in the early 1800s—the great-great-great grandparents of the killer. Then, they built family trees of their offspring to the present day, using historical documents and police databases. They identified descendants who matched the age and description of the attacker and who lived in the areas of the crime sprees. *Id.*

[29] *Id.*

[30] *Id.*

[31] Mark Berman, Avi Selk, & Justin Jouvenal, '*We found the needle in the haystack': Golden State Killer suspect arrested after sudden DNA match*, WASH. POST (Apr. 26, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/25/golden-state-killer-suspect-arrested-in-one-of-the-worst-unsolved-crime-sprees-in-u-s-history/.

[32] Giacomo Luc, *Judge orders May pretrial for Golden State Killer suspect Joseph DeAngelo*, ABC 10 NEWS (Jan. 22, 2020), https://www.abc10.com/article/news/local/sacramento/judge-orders-may-pretrial-for-golden-state-killer-suspect-joseph-deangelo/103-4cfc9ecd-614a-4c29-a4e6-8977e1bb4c53.

which the statute of limitations had passed.[33] In August 2020, the Sacramento Superior Court sentenced him to multiple life sentences without parole after three full days of victim impact statements from survivors and family members.[34] DeAngelo stood up in court, removing the mask he wore due to the COVID-19 pandemic—and symbolic of the masks he wore during attacks—and apologized to those he had hurt.[35]

DeAngelo's arrest as the Golden State Killer sparked discussion about the potential of using genetic genealogy in unsolved cases. Nationally, the number of cold cases is staggering. For example, roughly one-third of murder cases in America go unsolved.[36] Combined with legislation like John Doe warrants[37] or with California's removal of the statute of limitations on rape cases,[38] genetic genealogy could be an even more powerful tool for prosecutors. The government's increased ability to detect criminals through genetic genealogy comes at the cost of searching genetic profiles originally intended for ancestry research. As such, it represents a tradeoff between privacy and security and a challenge for law to appropriately adapt to new technology.

Genetic genealogy presents a new question for Fourth Amendment jurisprudence regulating the use of DNA databases and searches. The Supreme Court has upheld challenges to collection of DNA samples from violent felons for the purposes of identification and linking to other crimes.[39] In these instances, the privacy interest at issue has been solely that of the

---

[33] Elliot C. McLaughlin & Stella Chan, *Hearing details ghastly crimes of Golden State Killer as he pleads guilty to killings*, CNN (Jun. 29, 2020), https://www.cnn.com/2020/06/29/us/golden-state-killer-plea-expected/index.html.

[34] Michael Levenson, *Golden State Killer Sentenced to Life in Prison Without Parole*, THE NEW YORK TIMES (Aug. 21, 2020), https://www.nytimes.com/2020/08/21/us/golden-state-killer-sentenced.html.

[35] *Id.*

[36] *See* Martin Kaste, *Open Cases: Why One-Third of Murders in America Go Unresolved*, NATIONAL PUBLIC RADIO (Mar. 30, 2015), https://www.npr.org/2015/03/30/395069137/open-cases-why-one-third-of-murders-in-america-go-unresolved (explaining that murders are "unsolved" when police close the case without a corresponding conviction).

[37] *See* Kelly Lowenberg, *John Doe DNA Warrants and the Statute of Limitations*, STANFORD LAW SCHOOL LAW AND BIOSCIENCES BLOG (Feb. 7, 2010), https://law.stanford.edu/2010/02/07/john-doe-dna-warrants-and-the-statute-of-limitations/ (explaining how California prosecutors can file an arrest warrant identifying a suspect only by DNA, allowing identification and prosecution of a suspect after the statute of limitations would otherwise run out).

[38] Merrit Kennedy, *California Eliminates Statute of Limitations on Rape Cases*, NATIONAL PUBLIC RADIO (Sept. 28, 2016), https://www.npr.org/sections/thetwo-way/2016/09/28/495856974/california-eliminates-statute-of-limitations-on-rape-cases.

[39] Maryland v. King, 569 U.S. 435 (2013).

defendant.[40] With genetic genealogy, the privacy interests of people uploading DNA samples to commercial databases are also at risk. In addition, a suspect who has not been previously arrested or convicted of a crime would retain a reasonable privacy interest in his or her DNA.

Aside from Fourth Amendment privacy concerns, the most applicable legal theory to the issue is the third-party search doctrine. Under this doctrine, an individual traditionally loses any reasonable privacy interest in information upon disclosing it to a third-party, often a business. Recently, the doctrine was restricted for the first time when the Supreme Court held that a search of cell phone location history requires a warrant, absent exigent circumstances.[41] The Court emphasized the sensitivity of the data involved and the lack of user understanding of the data being disclosed. These concepts apply even more strongly to DNA and the limited understanding of privacy implications that most users have when merely trying to find relatives.

Despite the progress already made on these cold cases and potential for solving more, genetic genealogy remains legally in uncharted waters. Over two years after the arrest of DeAngelo, there are no statutes or substantial case law guiding law enforcement on using this technique.[42] One other man was convicted of a rape and double murder after law enforcement identified him with genetic genealogy, but the parties reached an agreement to treat the process as a tip during the trial.[43] Parabon NanoLabs, Inc., a private laboratory that converts crime scene DNA to profiles that can be used for familial matches, stated in May 2019 that it contributed to fifty-five criminal identifications in the preceding year.[44] Although DeAngelo apparently did not challenge his identification through genetic genealogy, it is a matter of time before other suspects litigate the matter in courts across the country. To maintain genetic privacy rights and simultaneously use genetic genealogy to solve crimes, federal and state governments should enact statutory regulation of the issue.

This Comment consists of four Parts. Part I analyzes the history of Fourth Amendment jurisprudence, including the third-party search doctrine. It also follows the legal history of using DNA as evidence in criminal cases, the

---

[40] *Id.*

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

[42] Molteni, *supra* note 2.

[43] *Id.*

[44] Parabon NanoLabs, *Parabon® Customers Net 55 Solved Cases in First Year of Snapshot® Genetic Genealogy Service* (May 8, 2019), https://parabon-nanolabs.com/news-events/2019/05/parabon-customers-net-55-solved-cases-in-first-year-of-snapshot-genetic-genealogy-service.html. Parabon is also known for creating digital portraits of peoples' faces constructed from DNA samples. Liz Stinson, *Creepy Ads Use Litterbugs' DNA to Shame Them Publicly*, WIRED (May 15, 2015), https://www.wired.com/2015/05/creepy-ads-use-litterbugs-dna-shame-publicly.

development of government DNA databases, and the commercial DNA testing industry. Familial matching, misidentification, and lack of standardization in DNA testing are necessary to understand the full scope of genetic genealogy. Part II explores the applicability of existing and proposed legal theories to the challenges presented by genetic genealogy. This includes the history of defining a search under the Fourth Amendment, issues with the third-party search doctrine, the concept of standing, abandoned property, and justifications for enhanced protection of genetic privacy.

Part III proposes three limitations on genetic genealogy to balance the privacy interests inherent in DNA and to chill the method to solve crimes. First, genetic genealogy websites should clearly inform users of policies for law enforcement access to genetic profiles and provide a method to opt-out of law enforcement searches. Second, genetic genealogy should only be used in cases of violent felonies. This has already been a standard for law enforcement databases,[45] and the commercial DNA testing industry has largely adopted it in its user terms for law enforcement following the arrest of the Golden State Killer.[46] Third, law enforcement should only use genetic genealogy when a case cannot be solved by other investigative methods.

Part IV presents potential ramifications for failure to protect genetic privacy. Before genetic genealogy crossed paths with criminal law, genetic privacy concerns existed in the healthcare and insurance domains. The government has sought to expand criminal DNA databases by including groups beyond convicted felons. Combined with familial matching and the explosive growth of the commercial DNA industry, it may soon become impossible for an individual to retain genetic privacy.

II. FOURTH AMENDMENT AND THE EXPANSION OF CRIMINAL IDENTIFICATION METHODS

New technology over the last century has bolstered law enforcement's ability to scientifically identify criminals. However, these advancements come with more prying into suspects' identities and personal lives, and courts have faced the challenge of balancing individuals' privacy rights under the Fourth Amendment with the public benefit of solving crimes. This Part provides a foundation for understanding the third-party search doctrine, the rise of DNA identification and corresponding law enforcement databases, commercial genetic genealogy databases that law enforcement has begun

---

[45] Maryland v. King, 569 U.S. 435 (2013).

[46] Richard P. Shafer, *Validity, Construction, and Application of DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C.A. §§ 14135 et seq. and 10 U.S.C.A. § 1565*, 187 A.L.R. FED. 373, 1a; GEDmatch, *Terms of Service and Privacy Policy*, https://www.gedmatch.com/tos.htm (last visited February 16, 2020).

using to identify criminals, familial matching, and standardization of DNA testing.

In *Katz v. United States*,[47] the Supreme Court began a shift in interpreting the Fourth Amendment from protecting property to protecting people.[48] The trial court upheld the government's use of evidence of the petitioner's conversations about illegal gambling made from a public telephone booth, which the FBI had wiretapped.[49] The Supreme Court held that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion" rather than merely safeguarding constitutionally protected areas.[50] Furthermore, the Court reframed Fourth Amendment protection from earlier focus on trespass of places to its protection of people.[51] Therefore, the Court held that the wiretap constituted a warrantless search and seizure, violating the Fourth Amendment.[52] The Court placed significant emphasis on the reasonableness of searches and seizures.[53] In his frequently quoted concurrence, Justice Harlan stated that a person must have a subjective expectation of privacy that society is prepared to recognize as reasonable to have Fourth Amendment protection.[54] The shifting view of the Fourth Amendment led to the development of the third-party search doctrine.

A. The Third-Party Search Doctrine

The third-party search doctrine, under which a person loses an expectation of privacy when he or she voluntarily gives information to a third party, first appeared in *United States v. Miller*.[55] The trial court admitted evidence of the defendant's checks and bank records to prove that he defrauded the government of tax revenue from an unregistered whiskey still.[56] The Supreme Court affirmed, holding that a respondent had no Fourth Amendment interest in subpoenaed bank records.[57] The Supreme Court found that an individual's bank records were not "private papers" which would give rise to Fourth Amendment protection.[58] Because the documents existed for the purpose of commercial transactions inherently involving other parties, the

---

[47] Katz v. United States, 389 U.S. 347 (1967).
[48] *Id.*
[49] *Id.* at 348.
[50] *Id.* at 350.
[51] *Id.* at 351.
[52] Katz v. United States, 389 U.S. 347, 358 (1967).
[53] *Id.* at 359.
[54] *Id.* at 361 (Harlan, J., concurring).
[55] United States v. Miller, 425 U.S. 435, 435 (1976).
[56] *Id.* at 436.
[57] *Id.* at 437.
[58] *Id.* at 440.

Court distinguished the records from other types of documents.[59] Here, the Court laid the groundwork for the third-party search doctrine, holding that revealing one's affairs to another carries the risk of that person conveying the information to the government.[60]

In *Carpenter v. United States*,[61] the Supreme Court limited the third-party search doctrine for the first time by recognizing the sensitivity of the data disclosed.[62] In this case, the FBI tracked the petitioner's cell-site location information (CSLI) for 127 days as part of a robbery investigation. The Court held that the government's acquisition of the petitioner's CSLI records constituted a Fourth Amendment search.[63] The Court began by defining a search as an invasion of a privacy interest "that society is prepared to recognize as reasonable."[64] This framework allows for adaptation when considering developments in surveillance tools.[65] The digital data in CSLI is a unique combination of expectation of privacy in physical location[66] and in information voluntarily given to a third party, as in *Miller*.[67] The Court distinguished the "exhaustive chronicle" of information in CSLI from business records with limited personal information discussed in *Miller*.[68] Further, it found that the voluntary exposure aspect of the third-party doctrine[69] does not apply to CSLI, which is not "shared' in the traditional sense.[70] Cell phones are an integral part of modern life, and they log CSLI without any affirmative action by users.[71] The Court held that the government

---

[59] *Id.*
[60] See United States v. Miller, 425 U.S. 435, 443 (1976).
[61] Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).
[62] *Id.*
[63] *Id. at 2208-09.*
[64] Id. at 2209; *See* Smith v. Maryland, 442 U.S. 735, 735 (1979) (The Court used a two-prong analysis to determine whether government action has invaded a person's justifiable, reasonable, or legitimate expectation of privacy. First, has the individual exhibited a subjective expectation of privacy by preserving something as private? Second, is society prepared to recognize that expectation as reasonable?).
[65] *Carpenter*, 138 S. Ct. at 2209.
[66] *See* United States v. Jones, 565 U.S. 400 (2012). Here, the police installed a GPS device on the defendant's vehicle to tracking it as part of a drug trafficking investigation. The Supreme Court affirmed the District of Columbia Circuit's reversal of the conviction for the warrantless use of the GPS device in violation of the Fourth Amendment. Justice Sotomayor's concurrence highlighted the fact that GPS monitoring allows the government to determine personal information such as political and religious beliefs and sexual habits. *Id.* at 417–18 (Sotomayor, S., concurring). *See also* Katz v. United States, 389 U.S. 347, 361 (1967).
[67] United States v. Miller, 425 U.S. 435 (1976). *See also Carpenter*, 138 S. Ct. at 2209.
[68] *Miller*, 425 U.S. at 435; *Carpenter*, 138 S. Ct. at 2210.
[69] *Miller*, 425 U.S. at 435.
[70] *Carpenter*, 138 S. Ct. at 2210.
[71] *Id.*

needs a warrant to access historical CSLI without exigent circumstances, and it noted that the decision did not disturb real-time CSLI tracking, conventional surveillance methods, or business records that might inadvertently reveal location information.[72] After decades of judicially-sanctioned expansion of government power to access information, the Court restricted the third-party search doctrine for the first time in *Carpenter*.[73]

The third-party search doctrine originally gave a clear distinction in privacy rights between information voluntarily disclosed to a third party and information kept private. With *Carpenter*, the Supreme Court has considered the nature of the data and evaluated the voluntariness and knowledge of disclosure.[74] As the modern world progresses with more information routinely disclosed through technology, often with limited information or chances to opt-out, the Court should continue acknowledging individuals' privacy interests in sensitive information, such as DNA. Before considering if or how to apply the third-party search doctrine to commercial DNA databases, it is important to analyze the progression of legal theory with technological advancements in DNA.

B. Development in Solving Crimes with DNA

DNA matching has become an important tool for law enforcement in recent decades. Statutes at the state and federal level, as well as courts, have permitted the expanding use of DNA technology to solve crimes. The first criminal conviction using DNA evidence in the United States occurred in 1987.[75] Since then, technology has advanced to enable extracting DNA from smaller and more degraded samples and finding partial matches with family members. The government has created a variety of databases to store DNA profiles of criminals and crime victims. In the private sector, genealogy research has incorporated DNA testing to match family members and identify ancestors. Most commercial databases belong to private companies with policies that limit law enforcement access. One public database allowed law enforcement access, leading to the identification of the Golden State Killer. Familial matching has greatly increased the utility of DNA databases, but misidentification of suspects can still occur. Errors with DNA testing stem in part from a lack of national standardization for defining a match.

---

[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] Michelle Hibbert, *State and Federal DNA Database Laws Examined*, PBS, https://www.pbs.org/wgbh/pages/frontline/shows/case/revolution/databases.html (last visited November 4, 2020).

1. Government DNA Databases

Congress passed the DNA Identification Act of 1994, authorizing the Federal Bureau of Investigation (FBI) to create a national DNA database of convicted criminals and samples recovered from crime scenes, among other categories.[76] The FBI launched the database, called the Combined DNA Index System (CODIS), in 1998 to link data between federal, state, and local agencies.[77] Today, all fifty states participate in CODIS.[78] Because many violent criminals become repeat or serial offenders, collection of DNA from one case often leads to matches from other crimes.[79] Linked databases help fill gaps in law enforcement communication and lead to arrests of offenders who commit crimes in different jurisdictions.[80] As of 2010, CODIS had over nine million DNA profiles with 668,000 arrestees.[81] CODIS can produce an offender hit when crime scene DNA matches a convicted offender or arrestee who has a DNA profile in the database.[82] In addition, it can produce forensic hits when multiple crimes are linked—indicating the presence of a serial offender.[83] In the Golden State Killer case, the East Area Rapist and Original Night Stalker were only linked as the same offender by DNA matching years after the crimes.[84]

Congress enacted the DNA Analysis Backlog Elimination Act of 2000 (Backlog Elimination Act) to strengthen state participation in CODIS.[85] This law authorized grants to states for analyzing DNA samples of individuals convicted of qualifying state offenses and including crime scene samples in CODIS.[86] In 2019, the section enumerates specific offenses for DNA collection in CODIS.[87] These offenses include any felonies, aggravated sexual abuse, any crimes of violence, and any attempt or conspiracy to commit those crimes.[88] Offenses which mandate DNA input to CODIS tend to involve crimes resulting in harm toward others. For example, misdemeanor bank larceny is not a qualifying federal offense triggering a required DNA

---

[76] 34 U.S.C. § 12592 (2012).
[77] John M. Butler, *Advanced Topics in Forensic DNA Typing: Methodology* 213 (2011).
[78] *Id*.
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] CRIME MUSEUM, *supra* note 3.
[85] Butler, *supra* note 74.
[86] Shafer, *supra* note 43.
[87] 34 U.S.C. § 40702 (2012).
[88] *Id.*

sample, but armed bank robbery and conspiracy to commit armed bank robbery are.[89]

Courts have generally held that the collection of samples under the Backlog Elimination Act does not constitute an unconstitutional search and seizure under the Fourth Amendment.[90] In a case challenging the Backlog Elimination Act, the First Circuit held that retaining and matching a defendant's DNA sample, obtained during probation, to another crime did not constitute a separate search under the Fourth Amendment.[91] In addition to an interest in proper identification of defendants and arrestees, the Ninth Circuit has held that the government has a compelling interest in the deterrent effect of DNA profiling of criminals and in the contribution of DNA collection to solving past crimes.[92] The Ninth Circuit noted the high recidivism rate among violent criminals as justification for keeping a DNA sample on file, especially when releasing said individuals for parole or probation.[93] The Court also noted that nonviolent offenders also have a high recidivism rate, and that the government has an interest in proper identification of this population to solve future investigations.[94] Finally, the Court noted that DNA profiling of qualified federal offenders can help bring closure to victims of unsolved crimes and their families, who might otherwise worry about their attackers being at large.[95]

Congress increased the number of individuals required to submit DNA samples to databases with the DNA Fingerprint Act of 2005[96] as part of the Violence Against Women Act.[97] Under the DNA Fingerprint Act of 2005, the government must collect a DNA sample from anyone convicted of a federal offense, without the earlier caveat of qualifying offenses.[98] The government's expansion of DNA databases signaled a shift in purpose from primarily identifying suspected offenders to becoming an investigative tool.[99]

The Supreme Court has upheld several methods of DNA collection that are instrumental to the success of these databases. In *Maryland v. King*,[100] the Court addressed the Fourth Amendment issue of collecting a buccal (cheek)

---

[89] *Id.*
[90] *Id.*
[91] Boroian v. Mueller, 616 F.3d 60, 71 (1st Cir. 2010).
[92] United States v. Kriesel, 508 F.3d 941, 949 (9th Cir. 2007).
[93] *Id.* at 949–50.
[94] *Id.* at 950.
[95] *Id.*
[96] 34 U.S.C. § 40702 (2012).
[97] Patrick Haines, *Embracing the DNA Fingerprint Act*, 5 J. TELECOMM. & HIGH TECH. L. 629, 631 (2007).
[98] *Id.*
[99] *Id.*
[100] Maryland v. King, 569 U.S. 435, 435 (2013).

swab from an arrestee and running it through CODIS.[101] Here, police arrested the respondent for assault and took his DNA sample during booking.[102] The sample matched an unsolved rape case from six years earlier and led to the respondent's conviction for that rape, which he appealed by alleging that taking the sample violated his Fourth Amendment rights.[103] The Court analyzed the reasonableness of the search, finding a reduced need for a warrant due to the arrestee already being in "valid police custody for a serious offense supported by probable cause."[104] Maryland's law in question[105] allowed police to collect DNA samples from arrestees accused of a crime of violence, including murder, rape, first-degree assault, kidnapping, arson, sexual assault, and burglary.[106] At the time of the case, all fifty states required the collection of DNA from felony convicts to be collected in CODIS.[107]

The collection of DNA by buccal swab after an arrest has become a routine part of police booking procedures, like fingerprinting, to ensure the identity and history of the arrestee, including prior crimes. Maryland did not allow testing for familial matches; an arrestee's DNA had to match an entry in CODIS exactly for identification.[108] The Court upheld the practice of collecting DNA samples from arrestees during booking as a reasonable search.[109] Although Maryland's law named specific violent felonies in the law, the Court simply affirmed the practice when applied to a "serious offense."[110] The Court accepted Maryland's classification of named violent felonies as serious offenses, but it left open the possibility of a wider range of "serious" offenses for which this practice would be appropriate. Criminal DNA databases, despite their rapid growth, can only identify previously arrested or convicted criminals and their family members. In contrast, private genealogy databases can detect criminals who have never been caught.

2. Private Genealogy Services

Government-established criminal DNA databases are no longer the only method of DNA collection. The at-home DNA testing industry has grown rapidly since its recent inception, with decreasing costs for customers.[111]

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.* at 436.
[105] Md. Public Safety § 2-504 (West).
[106] *King*, 569 U.S. at 444.
[107] *Id.* at 444–45.
[108] *Id.* at 444.
[109] *Id.*
[110] *Id.* at 465.
[111] Antonio Regalado, *2017 was the year consumer DNA testing blew up*, MIT

Users may purchase a test kit online or in stores, then mail a cheek swab or tube of saliva to a laboratory for genetic analysis.[112] These tests can provide information about ancestry and/or family secrets, such as unknown siblings.[113] As more people take these tests, genetic genealogy websites can link millions of Americans, including many who have never personally taken a DNA test.[114] Some of the most popular companies in the industry are 23andMe and Ancestry.com.[115]

In 2007, 23andMe launched its first direct-to-consumer DNA testing product at a cost of $999.[116] By 2011, the site had 100,000 customers and sold kits at $399 each.[117] As of April 2017, a year before law enforcement caught the Golden State Killer, 23andMe had over two million genotyped customers and offered an ancestry-only product for $99.[118] Yet, 23andMe is just one of many genetic ancestry services in the market; Ancestry.com boasts over fifteen million DNA tested people.[119] Others include MyHeritage with 1.4 million profiles and FamilyTreeDNA with 850,000.[120] Overall, the number of people who have used a direct-to-consumer genetic genealogy test increased twofold during 2017 alone,[121] with over twenty-six million people total tested by 2019.[122]

Each of these services creates its own private database, usually only sharing information between its own customers.[123] As a result, customers of

---

TECHNOLOGY REVIEW (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up.

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *23andMe History*, 23andMe, https://mediacenter.23andme.com/assets/timeline/index.html (last visited November 4, 2020).

[117] *Id.*

[118] *Id.*

[119] *Company Facts*, Ancestry, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited November 4, 2020).

[120] *Best DNA Test for Ancestry*, Smarter Hobby, https://www.smarterhobby.com/genealogy/best-dna-test/ (last visited November 3, 2020).

[121] Regalado, *supra* note 111.

[122] Jessica Bursztynsky, *More than 26 million people shared their DNA with ancestry firms, allowing researchers to trace relationships between virtually all Americans: MIT*, CNBC (Feb. 12, 2019), https://www.cnbc.com/2019/02/12/privacy-concerns-rise-as-26-million-share-dna-with-ancestry-firms.html.

[123] *Ancestry Guide for Law Enforcement*, Ancestry, https://www.ancestry.com/cs/legal/lawenforcement (last visited November 4, 2020); *FamilyTreeDNA Law Enforcement Guide*, FamilyTreeDNA, https://www.familytreedna.com/legal/law-enforcement-guide (last visited November 4, 2020).

a private genetic ancestry service can find familial matches only among users on the same website.[124] Additionally, these services only share user information with the government under certain circumstances. For example, 23andMe only shares user account information to government agencies with a valid legal request, such as a warrant or subpoena.[125] Ancestry.com and FamilyTreeDNA have nearly identical policies.[126]

For law enforcement to access more than user account details—namely, to obtain a user's DNA sample—these companies' policies generally require a warrant.[127] 23andMe informs customers that it may disclose customer information if it receives a judicial subpoena, warrant, or order and will notify the customer in such cases unless the order prevents it from doing so.[128] Ancestry.com requires a search warrant from a government agency with jurisdiction in order to release any DNA data from its customers, and it similarly notifies users of such requests unless prohibited.[129] Ancestry also has a provision for emergency requests in exigent emergencies involving the danger of death or serious physical injury to a person.[130] In general, the industry has reacted to the arrest of the Golden State Killer by clarifying terms and restricting clandestine law enforcement access to user information.

Surprisingly, one private genealogy site has changed its terms to be more permissive of law enforcement uploading crime scene DNA following the arrest of the Golden State Killer.[131] FamilyTreeDNA has explicitly given law enforcement permission to upload crime scene DNA to identify relatives of suspects.[132] The site does require law enforcement to request permission for such use and limits it to identification of a deceased individual or identifying a perpetrator of homicide, sexual assault, or abduction.[133] However, police cannot access individuals' raw genetic data through FamilyTreeDNA's profiles, and its database provides less genetic information than GEDmatch's

---

[124] *GEDmatch*, DNATestingAdvisor.com, https://www.dna-testing-adviser.com/GEDmatch.html (last visited November 4, 2020).
[125] *Law Enforcement Guide*, 23andMe, https://www.23andme.com/law-enforcement-guide/ (last visited November 4, 2020).
[126] Ancestry, *supra* note 123; FamilyTreeDNA, *supra* note 123.
[127] 23andMe, *supra* note 125; Ancestry, *supra* note 123; FamilyTreeDNA, *supra* note 123.
[128] *How 23andMe Responds To Law Enforcement Requests For Customer Information*, 23andMe, https://customercare.23andme.com/hc/en-us/articles/212271048-How-23andMe-responds-to-law-enforcement-requests-for-customer-information (last visited November 4, 2020).
[129] Ancestry, *supra* note 123.
[130] *Id.*
[131] Tina Hesman Saey, *What FamilyTreeDNA Sharing Genetic Data with Police Means for You*, SCIENCE NEWS (Feb. 6, 2019), https://www.sciencenews.org/article/family-tree-dna-sharing-genetic-data-police-privacy.
[132] *Id.*
[133] FamilyTreeDNA, *supra* note 123.

publicly available information.[134] Its terms now automatically opt in users in the United States to law enforcement searches of their profiles.[135] FamilyTreeDNA does still allow its customers to disable matching, but this affects all family matches, not just law enforcement searches.[136] The company says that only one percent of its customers opted out of matching several months after the new policy took effect.[137] This indicates that a portion of customers want to retain the core functions of the service—finding relatives and identifying health risks—while allowing law enforcement to detect criminals among those relatives. Although there may be future, unrecognized risks to the user, the immediate risk is to relatives who are violent criminals. Despite the growth of numerous commercial DNA databases, their utility is limited because users can only find matches within the same service.

3. A Public DNA Database

GEDmatch provides a public database for users of private DNA testing companies to upload their genetic profiles.[138] This allows users to find familial matches from other DNA testing services which would not otherwise be possible because each company maintains its own private database.[139] GEDmatch requires that uploaded DNA conforms to one of several categories, such as the user's own DNA or DNA from a person who has authorized the user to upload it.[140] For law enforcement use, the terms only allow DNA to identify remains of a deceased individual or to identify a perpetrator of a violent crime against another individual, defined as murder, non-negligent manslaughter, aggravated rape, robbery, or aggravated assault.[141]

After police identified the Golden State Killer and numerous other criminals using GEDmatch, the site changed its default terms to include opting out from allowing matches with law enforcement DNA samples.[142]

---

[134] Saey, *supra* note 131.
[135] Seth Augenstein, *GEDmatch Changes: 'Blow' to Forensic Genealogy?*, FORENSIC MAG. (May 20, 2019), https://www.forensicmag.com/news/2019/05/gedmatch-changes-blow-law-enforcement-and-forensic-genealogy?cmpid=horizontalcontent.
[136] Saey, *supra* note 131.
[137] Molteni, *supra* note 2.
[138]Tomohiro Takano, *GED match Review: What to Know Before You Start*, GENOMELINK BLOG (Sept. 1, 2020), https://blog.genomelink.io/posts/gedmatch-review-what-to-know-before-you-start.
[139] *Id.*
[140] GEDmatch, *supra* note 46.
[141] *Id.*
[142] Augenstein, *supra* note 135.

Existing users, who may have stopped using the site, would have to log in to their accounts and opt in to such searches.[143] New users, however, select one of four categories for their DNA: "private," "research," "public + opt-out," and "public + opt-in."[144] Users can later decide to change categories.[145] The "private" setting allows analysis of one's own DNA without any comparisons, while "research" allows one-on-one comparison to another sample.[146] The "public + opt-out" selection allows comparison to any other sample in the database, except for those uploaded for law enforcement purposes.[147] The "public + opt-in" setting allows comparison with any sample in the database, including those uploaded by law enforcement.[148] Although the change in privacy policy instantly reduced the database of over one million searchable profiles to zero, approximately 30,000 users opted back in within two weeks of the change.[149] As of October 2019, the numbers climbed to 163,000.[150] The number of users opting in to law enforcement searches indicates that a substantial number are willing to accept the privacy risks in return for identifying violent criminals, just as FamilyTreeDNA's statistics suggest.

The commercial DNA industry has grown to include millions of genetic profiles, but legal privacy doctrine has not found a way to govern it. Genetic privacy deserves protection beyond contractual user agreements between customers and DNA testing companies. With the development of genetic genealogy in law enforcement, the status quo for the DNA industry may no longer be sufficient.

4. Familial Matching and Standardization

Unlike bank records or CSLI, DNA belonging to one person always contains information about others. Familial matches via criminal DNA databases, even before genetic genealogy, drastically increased the likelihood of law enforcement identifying an offender.[151] With this technique, law enforcement searches a DNA database to identify close biological relatives

---

[143] *Id.*
[144] GEDmatch, *supra* note 46.
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] Augenstein, *supra* note 135.
[150] Sarah Zhang, *The Messy Consequences of the Golden State Killer Case*, THE ATLANTIC (Oct. 1, 2019), https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/.
[151] Samuel D. Hodge, Jr., *Current Controversies in the Use of DNA in Forensic Investigations*, 48 U. BALT. L. REV. 39, 49 (2018).

to the crime scene DNA sample, including siblings, children, and parents.[152] Police in the United Kingdom first used this method to identify a serial killer from the 1970s, who did not have a DNA sample in their databases.[153] However, the killer's son had been convicted of car theft and had a DNA sample in a law enforcement database, allowing British police to identify the killer via his child's DNA.[154] In the United States, at least twelve states allow law enforcement to conduct familial DNA searches through law enforcement databases as of 2019.[155] In 2016, law enforcement in California identified the Grim Sleeper, a notorious serial rapist and killer.[156] Although they had multiple crime scene DNA samples, they did not match any DNA in law enforcement databases.[157] Police then conducted a familial search and discovered a partial match between a convicted felon and his brother, the Grim Sleeper.[158]

While familial matching has solved high-profile cases, neither it nor genetic genealogy is entirely free from errors.[159] In Idaho, police working on the 1996 rape and murder of Angie Dodge identified a suspect through a partial DNA match in 2014, after failing to find an exact match in national criminal databases.[160] The suspect's father had provided a DNA sample to a nonprofit foundation later acquired by Ancestry.com.[161] Police obtained a warrant compelling Ancestry.com to produce the name of the partial match, the father.[162] Then, they mapped the family tree of the father.[163] Law enforcement identified one relative who they strongly suspected because of his ties to the location of the murder and because he was a filmmaker who had made some violent films.[164] Federal agents interrogated this suspect and obtained another warrant to collect his DNA.[165] After testing, law enforcement discovered that he was not the killer.[166] In 2019, however, a man who had been interviewed shortly after the homicide was identified through

---

[152] *Id.*
[153] *Id.* at 49–50.
[154] *Id.*
[155] *Id.* at 50.
[156] *Id.*
[157] *Id.* at 50–51.
[158] *Id*.
[159] *Id.* at 51.
[160] *Id.* at 51; Jim Mustian, *New Orleans filmmaker cleared in cold-case murder; false positive highlights limitations of familial DNA searching*, THE NEW ORLEANS ADVOCATE (Mar. 12, 2015), https://www.nola.com/article_d58a3d17-c89b-543f-8365-a2619719f6f0.html.
[161] Hodge, *supra* note 151, at 51.
[162] Mustian, *supra* note 160.
[163] *Id.*
[164] Hodge, *supra* note 151, at 51; Mustian, *supra* note 160.
[165] Hodge, *supra* note 151, at 51.
[166] *Id.*

genetic genealogy and subsequently confessed to the crime.[167] Notably, Parabon Labs, who processed the crime scene sample for use on genealogy websites, claimed that genetic genealogy had never before been done with such a degraded DNA sample.[168]

Cases like the murder of Angie Dodge demonstrate both the immense value in familial matching and genetic genealogy for solving cold cases and the danger in putting too much trust in a new methodology with varying standards across law enforcement agencies and private laboratories, administered by fallible humans. Further, there are privacy concerns specific to familial DNA matching.[169] Because racial minority groups are imprisoned at disproportionately high rates, familial matching through criminal DNA databases is more likely to identify minority suspects.[170] In addition, African-Americans specifically are more likely to be incorrectly targeted for investigation.[171] Combined with the possibility of false identification through familial matching, then, innocent minority family members are more likely to be subjected to searches, interrogations, and invasions of privacy.[172]

The issues with familial DNA are partially attributable to a lack of standardization.[173] There are no federal standards, guidance, or policies regulating the circumstances in which an agency may search a criminal DNA database for a familial, rather than exact, match.[174] Instead, it has fallen to individual agencies to enact policies that reflect privacy concerns.[175] For example, an agency may restrict searches for familial matches to cold cases or crimes impacting public safety, such as violent crimes.[176] California became the first state to regulate familial DNA searches in 2008.[177] Its policy requires that familial DNA searches may only be used when all other investigative methods have been exhausted for major crimes of violence.[178] Approximately ten other states have enacted similar regulations through legislation or agency policies.[179] The FBI prohibits using its National DNA Index System for familial matches, and Maryland prohibits such searches

---

[167] Shane Bishop, *Police arrest Idaho man in 23-year-old cold-case murder of Angie Dodge*, NBC NEWS (May 16, 2019), https://www.nbcnews.com/dateline/police-arrest-idaho-man-23-year-old-cold-case-murder-n1006726.
[168] *Id.*
[169] Hodge, *supra* note 151, at 52.
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.* at 53.
[177] *Id.*
[178] *Id.*
[179] *Id.*

altogether.[180]

DNA contains more sensitive information than any other type of data considered in legal precedent. Even if an individual understands the privacy risks involved in disclosing his or her DNA, there are troubling concerns that warrant additional protection. The DNA inherently provides information about relatives who cannot all possibly consent to disclosure. DNA may contain more information than is understood at the time of disclosure; it may be too late to protect one's privacy by the time risks are better appreciated.

III. CONSTITUTIONALITY OF IDENTIFYING CRIMINALS WITH GENETIC GENEALOGY

Existing legal doctrine does not clearly address genetic genealogy. Still, the Fourth Amendment framework provides a basis for analyzing circumstances in which law enforcement may access commercial DNA databases to identify criminals. When law enforcement submits a crime scene DNA sample to a database, it does conduct a search.[181] The traditional third-party doctrine provides insufficient protection of genetic privacy,[182] but the Supreme Court's current trend indicates a willingness to exempt sensitive data like DNA and retain the core functions of the doctrine.[183] DNA, like cell phone location information, deserves special protection beyond that of traditional commercial documents or transactions. In addition to the information revealed about the owner of the sample, DNA reveals information about relatives who have not disclosed the data to a database company, regardless of the applicability of the third-party search doctrine.[184] In light of these concerns, use of genetic genealogy should be limited to serious crimes that cannot be otherwise solved, using databases that clearly inform users of law enforcement access.

A. The Government Conducts a Search with Genetic Genealogy

The fundamental question in determining whether the government has

---

[180] *Id.*

[181] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (defining a search as an invasion of a privacy interest "that society is prepared to recognize as reasonable").

[182] Rebecca Gold, *From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges*, 55 CAL. W. L. REV. 491, 494-95 (2019).

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

[184] *Cf.* Christine Guest, *DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights*, 68 AM. U. L. REV. 1015 (2019) (arguing that law enforcement violates the privacy rights of both suspects and their families when uploading DNA to an open source database).

conducted a search is whether it has invaded a privacy interest "that society is prepared to recognize as reasonable."[185] Of the twenty-six million people who have taken direct-to-consumer DNA tests,[186] approximately one million have chosen to upload them to GEDmatch.[187] Unfortunately, there is no data explaining how many of the remaining users had privacy concerns about using a public site, were satisfied with the results from the particular private site they chose, or simply were not aware of GEDmatch. Within months of GEDmatch changing its million users' default setting to "opt-out" of law enforcement searches, 163,000 actively chose to opt in.[188] GEDmatch has not published statistics on how many users actively choose to opt out. Again, it is unclear how many users have privacy concerns about their profiles, are unaware of the change, or no longer access their accounts. Still, it seems reasonable to conclude that some users of GEDmatch and private sites have privacy interests in their genetic data despite being willing to use it for finding family members, ancestry information, or health risks.[189]

B. A Modified Third-Party Search Doctrine May Apply to Genetic Genealogy

Assuming some users of genetic genealogy services have privacy interests in their genetic data, is society prepared to recognize these interests as reasonable? The Supreme Court's holding in *Carpenter*[190] that the third-party search doctrine does not apply to CSLI indicates that the Fourth Amendment may similarly govern genetic genealogy. The aspects of CSLI that make the third-party search doctrine unworkable—quantity and unique nature of data[191]—apply to genetic profiles as well.

In *United States v. Jones*,[192] the Court reaffirmed that a search violating a reasonable expectation of privacy violates the Fourth Amendment protection of peoples' privacy.[193] Here, the government warrantlessly attached a GPS tracker to the defendant's vehicle and monitored it at his home

---

[185] Smith v. Maryland, 442 U.S. 735, 743 (1979); *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).
[186] Bursztynsky, *supra* note 122.
[187] Augenstein, *supra* note 132.
[188] Zhang, *supra* note 150.
[189] *See* Michael I. Selvin, *A Too Permeating Police Surveillance: Consumer Genetic Genealogy and the Fourth Amendment After Carpenter*, 53 LOY. L.A. L. REV. 1015 (2020) (citing two 2018 studies suggesting that the public supports law enforcement use of genetic genealogy to solve violent crimes).
[190] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[191] *Id.* at 2217.
[192] United States v. Jones, 565 U.S. 400 (2012).
[193] *Id.*

and on public streets.[194] Justice Sotomayor, in her concurrence, stated that not all information voluntarily disclosed to a third party should be stripped of Fourth Amendment protection, noting the massive amount of information revealed in the digital age.[195] DNA contains far more data than the physical locations tracked by cell phone location or a vehicle—it reveals information about health risks, ancestry, and family members other than the individual providing the DNA. Courts have held that arrestees and convicts do not have a reasonable expectation of privacy in their DNA to prevent proper identification or connections to other crimes.[196] However, courts faced with the issue of genetic genealogy should find that people who upload DNA samples to genealogy websites for purposes such as finding family members have an expectation of privacy that society recognizes as reasonable.

One solution proposed by Eunice Park, a professor at Western State College of Law, to the dilemma of analyzing genetic genealogy is additional modification of the third-party search doctrine to account for the uniqueness of DNA.[197] A new test, similar to the acknowledgement of the special circumstances in CSLI data, could be limited to searches involving genetic information.[198] The Court declined to apply the traditional third-party search doctrine to CSLI for two reasons.[199] First, it distinguished the nature of CSLI from the bank records and call logs in earlier cases.[200] Second, it noted that cell phone users reveal their CSLI through a technology that almost everyone in society now uses, and users do so without an affirmative consent.[201] In light of this holding, Eunice Park has suggested applying a retrospective test when new or modern technology is used to share data without an affirmative act to do so.[202] A court would first inquire whether the user knew that using technology would result in sharing data with a third party and then determine whether the user had an opportunity to opt out of sharing.[203] This test would partially shift the focus of the third-party search doctrine from a consumer's

---

[194] *Id.* at 402, 413.
[195] *Id.* at 417–18 (Sotomayor, S., concurring).
[196] Shafer, *supra* note 46, at 5; Maryland v. King, 569 U.S. 435 (2013).
[197] Eunice Park, *Objects, Places and Cyber-Spaces Post-Carpenter: Extending The Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J. L. & TECH. 1, 13 (2019) (citing Carpenter v. United States, 138 S. Ct. 2206 (2018) (already modifying the third-party search doctrine by accounting for sensitivity of data)).
[198] *Id.* (citing *Carpenter* 138 S. Ct. at 2206 (noting that the modification of the third-party search doctrine for searches of CSLI did not disturb doctrine surrounding conventional surveillance methods)).
[199] *Id.* (citing *Carpenter*, 138 S. Ct. at 2206 (stating that the traditional third-party search doctrine does not apply to CSLI)).
[200] *Id.*
[201] *Id.* at 14.
[202] *Id.*
[203] *Id.*

action to the third party's disclosure. If pervasiveness is part of the analysis, then commercial DNA will likely take years to reach this threshold.[204]

Regarding affirmative acts, many genetic genealogy sites have implemented controls that ensure users understand the ways in which a site will use their genetic material and have an opportunity to opt out of certain features.[205] Excitement about DNA testing and the large amount of potentially-confusing information presented to new users may prevent them from fully understanding the privacy rights they sign over or the ramifications of not opting out of features such as research use of their DNA.[206] Specifically, 23andMe notifies users that its contracted lab processes user DNA samples.[207] It also gives users the option to share data for scientific research, informing them that over eighty percent of customers do so.[208] Furthermore, it clarifies that it will only share information with another third party—law enforcement—with a warrant. Yet, a user may not be able to effectively opt out of research after initially allowing access to one's genetic profile.[209] Notably, 23andMe implemented all of these controls voluntarily; federal law and most state laws regulating genetic information apply to insurance, employers, and healthcare, not DNA testing companies.[210] While these policies effectively address many concerns about genetic privacy, they rely on the company's goodwill and could change in the future. In the absence of federal regulation, a judicially created test that emphasizes user knowledge and affirmative consent may be an appropriate solution to protect the privacy interests of individuals using modern and future technology such as commercial DNA testing.[211]

Another solution for modifying the third-party doctrine post-*Carpenter*,[212] proposed by Michael Gentithes, a professor at Chicago-Kent College of Law, is a two-step test to determine whether the government needs a warrant to obtain information from a third party.[213] First, a court would analyze the sensitivity of the information using a scaled approach. This idea departs from *Miller*, where the third-party doctrine analyzed the search of bank records,[214] with a binary classification of data as either disclosed or

---

[204] *Id.* (citing *Carpenter* 138 S. Ct. at 2206).
[205] *Id.* at 40–41.
[206] *Id.* at 50.
[207] *Id.* at 42.
[208] *Id.* at 41–42.
[209] *Id.* at 47.
[210] *Id.* at 41.
[211] *Id.* at 57–58 (citing Carpenter v. United States, 138 S. Ct. 2206 (2018)).
[212] *Carpenter*, 138 S. Ct. at 2206.
[213] Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After Carpenter,* 53 GA. L. REV. 1039, 1045 (2019).
[214] United States v. Miller, 425 U.S. 435 (1976).

undisclosed to third parties.[215] A scaled approach would result in a moderate degree of protection for many types of commonly disclosed data and prevent warrantless access to information such as financial records.[216] The Supreme Court in *Carpenter*[217] indicated a willingness to consider the sensitivity of disclosed information.[218] In fact, the American Bar Association's 2012 Proposed Standards for Law Enforcement Access to Third Party Records[219] suggested labeling information on a sliding scale as highly private, moderately private, minimally private, or not private.[220] Second, a court would decide whether the quantity of sensitive information collected constitutes a search.[221] This builds on Justice Sotomayor's concurrence in *Jones*,[222] in which she pointed to the mosaic of information about a person created by continuous tracking of his or her movements.[223] If the information is sensitive and creates a picture of a person's life, it violates a person's privacy interest and constitutes a search.[224] To conduct such a search, the government needs a warrant, absent special circumstances.[225] Under this approach, using genetic genealogy to identify criminals or government analysis of a person's DNA profile would undoubtedly constitute a search. DNA would likely fall under the most sensitive category of information; it is difficult to imagine data more sensitive to an individual. Given its use in solving crimes, ancestry, and healthcare through revealing a person's predisposed risks, it creates a mosaic of a person's identity as well. Accordingly, DNA would satisfy both steps of this approach, constituting a search and requiring a warrant for government access, notwithstanding any disclosure to a third party.

A scaled, rather than binary, approach to privacy of information disclosed to third parties may become necessary as modern technology continues to facilitate constant sharing of large volumes of information. Creating separate tests for different types of data could become burdensome to the judicial system and lead to uncertainty as to whether certain types of data may receive heightened protection. Still, DNA contains information revealing the core of

---

[215] Gentithes, *supra* note 208.
[216] *Id.*
[217] *Carpenter*, 138 S. Ct. at 2206.
[218] Gentithes, *supra* note 208.
[219] *Law Enforcmeent Access to Third Party Records Standards*, ABA, https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/ (last visited November 4, 2020).
[220] Gentithes, *supra* note 208, at 1064.
[221] *Id.* at 1046.
[222] United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring).
[223] Gentithes, *supra* note 208, at 1046.
[224] *Id.*
[225] *Id.*

a person's existence—if any type of data deserves its own test for privacy, it is DNA.

C. A Criminal Defendant Identified Via Genetic Genealogy May Lack Standing to Challenge a Search

Without statutory regulation, courts might not rule on the practice of genetic genealogy because the criminal defendants it identifies lack a clear showing of standing.[226] Essentially, a criminal defendant challenging evidence obtained through a genealogical site search needs to have a personal Fourth Amendment right violated.[227] In these cases, the actual material searched would be the DNA sample from the relative using the genealogy site, many of whom have consented to law enforcement searches.[228] This is functionally similar to a relative voluntarily tipping off law enforcement to the identity of the offender. In the intermediate steps of the search, law enforcement has used public census records, newspapers, and graves to identify relatives of the genealogy site match.[229] Finally, the match to the defendant comes from crime scene DNA, in which the owner has given up any privacy interest by abandonment.[230] Law enforcement has confirmed matches prior to arrests by using well-established constitutional methods of DNA collection, such as collection from a public place or trash left outside a suspect's home.[231]

The Supreme Court ruled on the issue of standing in criminal cases in *Rakas v. Garamond*.[232] In this case, a defendant passenger challenged police officers' search of a car, which revealed an illegal firearm and ammunition.[233] The Court held that challenging the legality of a search to suppress evidence requires a defendant to personally be the victim of the search.[234] The Court interpreted Fourth Amendment rights as personal rights that cannot be

---

[226] *See* Hillary L. Kody, *Standing to Challenge Familial Searches of Commercial DNA Databases*, 61 WM. & MARY L. REV. 287, 313 (2019) (arguing that suspects retain an expectation of privacy in familial DNA and should have standing to challenge a search of DNA in a third-party database).
[227] George M. Dery III, *Can a Distant Relative Allow the Government Access to Your DNA? The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations*, 10 HASTINGS SCI. & TECH. L.J. 103, 139 (2019).
[228] *Id.*
[229] *Id.* at 139–40.
[230] *Id.* at 139.
[231] Jouvenal, *supra* note 25.
[232] Rakas v. Illinois, 439 U.S. 128, 128-29 (1978).
[233] Dery, *supra* note 227, at 140.
[234] *Id. at 141.*

asserted on behalf of a third party.[235] Because the defendant was only a passenger in the car, he did not have a Fourth Amendment privacy interest in the car's contents and therefore lacked standing to challenge the search.[236]

Recently, the Court ruled again on standing to challenge the search of a car in *Byrd v. United States*.[237] Here, the Court held that a driver of a rental car had a privacy interest in the car's contents despite not being a party to the rental agreement.[238] The Court in *Byrd*[239] recognized both property law and privacy expectations recognized by society, concluding that the driver did have a reasonable expectation of privacy in the car.[240] In its analysis of the rental car under traditional property law concepts, the Court emphasized the ability to exclude others as an indication of an expectation of privacy.[241] The Court applied this concept to the rental car, finding that a driver had an ability to exclude others from the car regardless of his or her inclusion on the rental agreement.[242] A court applying this reasoning to genetic genealogy would likely find that a defendant challenging the search of a genealogy site amounts to claiming a right to exclude others from the site.[243] However, the entire purpose of these sites is to share genetic information, contrary to any expectation of excluding others.[244] The terms of GEDmatch claim that it only acknowledges a property interest in the DNA sample by the person who uploads it, not any relatives who may share a large portion of the DNA themselves.[245] Under *Byrd*, it seems unlikely that a criminal defendant could claim a property interest and right to exclude in the DNA sample of a relative who uploaded it to GEDmatch or another genealogy database.[246] Without the property interest, ability to exclude, and resulting expectation of privacy, then a defendant would not have standing to challenge the search.[247]

D. DNA as Abandoned Property

If DNA samples uploaded to a genetic genealogy site may be analyzed under the traditional view of privacy grounded in property law, it is worth

---

[235] *Id.*
[236] *Id.*
[237] Byrd v. United States, 138 S. Ct. 1518, 1518-20 (2018).
[238] Dery, *supra* note 227, at 142.
[239] *Byrd,* 138 S. Ct. at 1518.
[240] Dery, *supra* note 227, at 142.
[241] *Byrd,* 138 S. Ct. at 1528.
[242] *Id.*
[243] Dery, *supra* note 221, at 143.
[244] *Id.*
[245] *Id.* at 141.
[246] *Id.* at 143.
[247] *Id.*

evaluating crime scene DNA under this lens as well. Under the traditional lens, privacy protected property rather than individuals.[248] Abandoned DNA has a well-established legal history of being considered abandoned property, with the original owner giving up all property rights to it.[249] Without property rights to personal property, the former owner also loses any reasonable expectation of privacy under the Fourth Amendment.[250] In 1960, the Supreme Court in *Abel v. United States*[251] upheld a government search of items left in a trash can.[252] In this case, the FBI and Immigration and Naturalization Service (INS) questioned a man, arrested him, and allowed him to pack belongings before checking out from his hotel room.[253] The arrestee left some items on the windowsill and trash can.[254] FBI agents then searched the room with the hotel manager's permission, seized the items, and found a hollowed out pencil and pencil sharpener containing microfilm and a cipher pad.[255] The Court held that man had abandoned the items by checking out of the hotel, and that the government acted lawfully when it seized abandoned personal property.[256]

In 1986, the Supreme Court held in *California v. Greenwood*[257] that a person who places garbage out for collection has no reasonable expectation of privacy for the items inside it.[258] Here, a man put his trash, with drug paraphernalia inside, at the curbside for collection.[259] Police found the items in the trash, obtained a warrant to search his home, and found additional drugs there, leading to drug possession charges for the occupants of the home.[260] Regardless of the respondents' subjective expectations of privacy, the Court held that society as a whole does not have any reasonable expectation of privacy for garbage left for pickup on a public street.[261] Similarly, courts have used this reasoning to hold that people do not have reasonable expectations

---

[248] Katz v. United States, 389 U.S. 347.
[249] Thomas D. Holland, *Novel Features of Considerable Biologic Interest: The Fourth Amendment and the Admissibility of Abandoned DNA Evidence*, 20 COLUM. SCI. & TECH. L. REV. 271, 278 (2019). *See also* Hillary L. Kody, *Standing to Challenge Familial Searches of Commercial DNA Databases*, 61 WM. & MARY L. REV. 287, 314 (2019) (evaluating DNA shared between relatives as jointly held property).
[250] *Id.*
[251] Abel v. United States, 362 U.S. 217 (1960).
[252] Holland, *supra* note 243, at 273–74.
[253] *Id.*
[254] *Id.* at 274.
[255] *Id.*
[256] *Id.* at 274–75.
[257] California v. Greenwood, 486 U.S. 35 (1988).
[258] Holland, *supra* note 243, at 282–83.
[259] *Id.*
[260] *Id.*
[261] *Id.*

of privacy in abandoned bodily cells and fluids.[262] The emphasis in such cases relies on the owner's abandonment of the fluid or cell; courts have become reluctant to uphold forcible searches of bodily fluids, absent exigent circumstances, due to reasonable expectations of privacy.[263]

While viewing DNA as property may be problematic for privacy concerns, it does create an effective framework for abandoned DNA.[264] Case law provides analysis of various bodily substances abandoned in different manners, giving varying weight to privacy interests. The Washington Supreme Court upheld the admissibility of DNA evidence obtained when detectives tricked a defendant into mailing them an envelope and then tested it for his saliva.[265] Although the court found that a person does not have an inherent privacy interest in saliva, it held that a person loses any privacy interest when mailing an envelope, which becomes the property of the recipient.[266] The Massachusetts Appeals Court in *Commonwealth v. Cabral*[267] held that a defendant abandoned the Fourth Amendment protection of privacy in his saliva's DNA when he spit on the ground in public, because he assumed the risk of someone else taking possession of his bodily fluids.[268] Law enforcement may also take a person's hair cut in a jail barbershop if the person does not attempt to retain possession of the hair.[269]

In *Raynor v. State*, the Court of Appeals of Maryland even upheld collection of a defendant's skin cells for DNA from a chair in a police station after he was questioned.[270] Here, the court held that the defendant did not demonstrate a reasonable expectation of privacy in his genetic matter, even though he did not know that he had exposed it to the public.[271] In these cases, the bodily substance—whether saliva or blood—and circumstances of abandonment seem to matter less than the voluntariness of abandonment,

---

[262] *Id. See also* Moore v. Regents of Univ. of Cal., 51 Cal. 3d 120 (1990) (holding that plaintiff did not have ownership interest in cells used in medical research without permission after they left his body).

[263] Holland, *supra* note 243, at 282–83; *see* Missouri v. McNeely, 569 U.S. 141 (2013). Here, the Supreme Court held that the natural metabolization of alcohol in the bloodstream does not constitute a *per se* exigent circumstance for warrantless blood testing of a drunk driving suspect. Instead, reasonableness must be determined on a case-by-case basis from the totality of the circumstances. Government intrusion into the body is a significant and constitutionally protected privacy interest. *Id.*

[264] Holland, *supra* note 243, at 275.

[265] *Id.* at 294–95; *see* State v. Athan, 160 Wash. 2d 354 (2007) (holding that police do not need a warrant to collect DNA from saliva on an envelope).

[266] Holland, *supra* note 243, at 294–95.

[267] Commonwealth v. Cabral, 866 N.E.2d 429 (2007).

[268] Holland, *supra* note 243, at 295 (citing *Cabral*, 866 N.E.2d at 429).

[269] *Id.* at 297 (citing United States v. Cox, 428 F.2d 683 (7th Cir. 1970)).

[270] *Id.* at 297–98 (citing Raynor v. State, 99 A.3d 753 (2014)).

[271] *Id.*

which may even be a lack of affirmative intent to recover or retain the substance.[272] Yet, people leave DNA nearly everywhere they go, and ruling that failure to retrieve it constitutes abandonment makes it nearly impossible to have any real possessory interest.[273] In the era of "touch DNA," just a few skin cells can lead to analysis and a match.[274]

Collection of abandoned DNA is an integral element of genetic genealogy. In the Golden State Killer case, law enforcement collected discarded DNA from Joseph DeAngelo after identifying him through the genetic genealogy process and before obtaining an arrest warrant.[275] In fact, investigators both collected DNA from trash outside his home and obtained touch DNA by swabbing his car door handle after he parked at Hobby Lobby and went into the store.[276] Other law enforcement agencies have followed the same procedure in other high-profile cases in which offenders were identified through genetic genealogy.[277] This procedure is particularly necessary when law enforcement targets a suspect based on distant relatives who share a partial match to crime scene DNA.[278] Even if law enforcement obtained a close match, it would still be prudent to collect abandoned DNA to compare to crime scene DNA in order to obtain a search or arrest warrant.

Law enforcement conducts a search when uploading crime scene DNA to a commercial database to identify a criminal. Under the traditional third-party search doctrine, this search would likely be permissible because the user voluntarily disclosed the DNA to a business.[279] Following the Supreme Court's recent ruling on the third-party search doctrine,[280] however, the result is less clear. If the Court accounts for the sensitivity of data, a user likely does

---

[272] *Id.* at 298.

[273] *Id.* at 302; *See* United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004) (Kozinski, J., dissenting) (describing skin cells left behind by a person's ordinary movements as a breadcrumb trail of DNA).

[274] Mary Gray Leary, *Big Data, National Security, and the Fourth Amendment: Touch DNA and Chemical Analysis of Skin Trace Evidence: Protecting Privacy While Advancing Investigations*, 26 WM. & MARY BILL OF RTS. J. 251, 257 (2017).

[275] Jouvenal, *supra* note 25.

[276] Nicole Chavez, *DNA that led to Golden State Killer suspect's arrest was collected from his car while he shopped*, CNN (June 2, 2018), https://www.cnn.com/2018/06/02/us/golden-state-killer-unsealed-warrants/index.html.

[277] Sam Stanton, Benjy Egel, Darrell Smith & Cynthia Hubert, *NorCal Rapist suspect arrested. He's a 58-year-old safety specialist at UC Berkeley,* THE SACRAMENTO BEE (Sept. 22, 2018), https://www.sacbee.com/news/local/crime/article218793610.html; Emily Shapiro, *Former federal prisons worker Mark Manteuffel arrested in string of 'horrific' 1990s sex attacks in Sacramento: Police*, ABC NEWS (Jul. 2, 2019), https://abcnews.go.com/US/federal-prisons-worker-mark-manteuffel-busted-string-horrific/story?id=64082340.

[278] Jouvenal, *supra* note 25.

[279] United States v. Miller, 425 U.S. 435 (1976).

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

not lose a privacy interest in DNA by disclosing it due to the sensitivity of the data.

E. The Unique Nature and Quantity of Information in DNA Justifies Additional Safeguards for Individual Privacy

In addition to its modification of the third-party search doctrine, *Carpenter*[281] provides a starting point for analyzing the sensitivity of data in a search.[282] There are important distinctions between the CSLI in *Carpenter* and DNA obtained via genetic genealogy.[283] While both are private sources of information that warrant at least some degree of protection under the Fourth Amendment, the factors in the Court's holding in *Carpenter* do not necessarily apply to DNA.[284] Cell phone users automatically share their locations with their service providers.[285] Although it is technically a voluntary choice to use a cell phone, they are ubiquitous in modern society.[286] Cell phones are almost essential for daily life, and many users do not understand that providers continuously record their location history.[287] Further, most consumers do not read cell phone contracts and user agreements thoroughly enough to understand what data they give providers permission to collect.[288] Therefore, it is difficult to describe the choice to use a cell phone with a provider recording CSLI as truly voluntary.[289]

Genetic genealogy differs from CSLI both in terms of voluntariness and the nature of the data collected. Purchasing an at-home DNA kit is a voluntary decision in which the privacy risks, even if not fully understood by users, are not a hidden secondary effect as CSLI is to use of a cell phone.[290] While the Court directly considered the effect of long-term location tracking on privacy interests in *Carpenter*,[291] DNA does not inherently reveal information about a person's current location.[292] However, it has the potential to do just that in the near future.[293] Through DNA phenotyping, labs can create a sketch of a

---

[281] *Id.*
[282] *Id.* at 2262.
[283] Gold, *supra* note 179, at 510 (citing *Carpenter*, 138 S. Ct. at 2206); Natalie Ram, *Genetic Privacy after Carpenter*, 105 VA. L. REV. 1357, 1424 (2019).
[284] Gold, *supra* note 179, at 510–11 (citing *Carpenter*, 138 S. Ct. at 2206).
[285] *Id.* at 511.
[286] *Id.*
[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[292] Gold, *supra* note 179, at 511.
[293] *Id.*

person from his or her DNA.[294] Combined with increasing public surveillance footage and facial recognition software, a DNA sample actually could locate a person in real time.[295] The potential for future DNA advancements combined with other technology warrants caution in shaping genetic privacy doctrine.

Notwithstanding the use of particular data to track a person's location, DNA still contains sensitive genetic information deserving of protection.[296] It provides information about who a person physically is and his or her lineage—which is arguably more invasive than a person's current or recent physical movements.[297] As Justice Sotomayor stated in *Jones*,[298] the idea that an individual has no reasonable expectation of privacy in information voluntarily disclosed to a third party does not work in the modern digital age, where routine tasks involve disclosing large amounts of personal information.[299] In *Carpenter*,[300] the Court acknowledged the rapid development in cell phone technology that has increased the quantity of information about a person available to third parties and the government.[301] Similarly, DNA has rapidly increased in its usefulness for solving crimes.[302] Law enforcement previously needed a suspect to match to crime scene DNA; now, laboratories can create a sketch of a person from his or her DNA.[303] Prior to genetic genealogy, expansions of DNA use in law enforcement—such as the creation of criminal DNA databases and familial matching—have been subjected to statutory and judicial oversight. Genetic genealogy, however, has resulted in an expansion of law enforcement's ability to identify criminal suspects, presumably justified through the third-party search doctrine.[304]

Privacy doctrine for genetic profiles must consider the susceptibility of DNA databases to hacking and data breaches. Hackers have accessed millions of customers' personal and contact information, credit card numbers, and passwords from private companies such as Target, eBay, Home Depot, and Marriott.[305] Financial institutions, such as JP Morgan Chase and Equifax,

---

[294] Liz Stinson, *supra* note 41.
[295] Gold, *supra* note 179, at 511.
[296] *Id.*; Ram, *supra* note 282, at 1380.
[297] *Id.* at 511–12.
[298] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
[299] Gold, *supra* note 179, at 511–12.
[300] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[301] Gold, *supra* note 179, at 512.
[302] *Id.*
[303] *Id.*
[304] *Id.* at 513.
[305] Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Jan. 8, 2021), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

have also been breached with similar results.[306] Data breaches can even have direct physical consequences.[307] In 2010, the U.S. and Israeli governments (probably) created a virus to attack Iran's nuclear program.[308] Loaded on a USB flash drive, the virus caused centrifuges used in uranium enrichment to spin too quickly and destroy themselves.[309] Aside from the political issues, the crossover from hacking to physical destruction is concerning for the future.[310] The Department of Defense has issued a memorandum advising troops not to take at-home DNA test kits, citing national security concerns if foreign governments gained information about their health risks.[311]

American government entities have not fared better—hackers obtained twenty two million federal employees' information from the U.S. Office of Personnel Management, including fingerprint data and security clearance information.[312] The former director of the FBI, James Comey, expressed concern over the breach due to the type of information contained in these documents.[313] Security clearances include details about an employee's family members, such as information about siblings and children, and their addresses.[314] It can be difficult to imagine what a future hacker could do with information obtained from a DNA database, outside of the standard concerns over user contact information and payment details. However, DNA matching technology has rapidly expanded in the decades since it was discovered, and it is likely to continue doing so. Furthermore, policy and jurisprudence regarding DNA privacy should anticipate these advances and prepare for the worst-case scenario—someone with bad intentions obtaining millions of peoples' DNA samples illicitly. Policy for DNA privacy should not only consider people with good intentions having access to data, but also bad actors who obtain the data by hacking.

---

[306] *Id.*
[307] Josh Fruhlinger, *What Is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
[308] *Id.*
[309] *Id.*
[310] *Id.*
[311] Kyle Mizokami, *If You're in the Military, Maybe Don't Take That Home Genetic Test*, POPULAR MECH S. (Dec. 30, 2019), https://www.popularmechanics.com/military/a30362195/military-home-genetic-test.
[312] Swinhoe, *supra* note 305.
[313] *Id.*
[314] *Id.*

IV. GENETIC GENEALOGY SHOULD BE USED WITH THREE LIMITATIONS

This Comment proposes judicial or statutory limitations on law enforcement's use of genetic genealogy to solve serious crimes—specifically, violent felonies. This restriction acknowledges the potential for government abuse of databases and intrusion of the privacy of database users and family members. Still, it allows for use of this incredible tool for solving otherwise unsolvable crimes of the worst nature.

The Supreme Court in *Carpenter* demonstrated a willingness to consider the sensitivity of data disclosed to a third party by distinguishing CSLI from data collected in traditional surveillance methods.[315] When criminal suspects identified through genetic genealogy challenge the practice, assuming a court finds them to have standing in the matter, courts should recognize the privacy concerns inherent in this method.[316] However, courts should balance these concerns with the usefulness of genetic genealogy in solving the most egregious crimes in our society. Therefore, this Comment proposes a three-step test for warrantless searches of public and private DNA databases: (1) ensure users have informed consent of any warrantless law enforcement access; (2) only use genetic genealogy to solve serious crimes; and (3) only use genetic genealogy when the case cannot be solved using other investigative methods.[317]

A. Ensure Users Have Informed Consent

First, the database's terms allow for law enforcement access, or they

---

[315] Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).

[316] Rakas v. Illinois, 439 U.S. 128, 133 (1978).

[317] *See also* Shanni Davidowitz, *23andEveryone: Privacy Concerns with Law Enforcement's Use of Genealogy Databases to Implicate Relatives in Criminal Investigations*, 85 BROOK. L. REV. 185, 213 (2019) (proposing another multi-step process including verification that law enforcement has exhausted other investigative methods and use only in violent crimes, but failing to acknowledge the importance of database users giving informed consent to any law enforcement searches of their DNA profiles); Selvin, *supra* note 189, at 1065–68 (also advocating for statutory limitation of genetic genealogy to violent crimes left unsolved by traditional law enforcement methods, but again lacking user consent as an element); Emily M. Strak, *Genetic Standing: The Constitutionality of Familial DNA Searching on Genealogical Research Databases*, 1 CTS. & JUST. L.J. 44 (2019) (again advocating for statutory restriction of genetic genealogy to cold case violent crimes, given defendants' probable lack of standing to challenge a genealogical search). *Cf.* Jennie F. O'Hara, *23, Me, and the Police: The Fourth Amendment Implications of Familial DNA Searching*, 30 GEO. MASON U. C.R. L.J. 177, 198–99 (2020) (advocating that law enforcement exhaust investigative methods and consider the nature of the crime, in addition to various procedures for labs and prosecutors, before using genetic genealogy).

allow users an option to opt-out.[318] Before the arrest of the Golden State Killer, GEDmatch did not present users with any information about law enforcement's use of the site or opportunities to opt-out.[319] At that point, it was arguable whether users had a reasonable expectation of privacy from searches. After the Golden State Killer's arrest, genetic genealogy sites created policies for law enforcement access, informed users, and provided opportunities to opt-in or opt-out of searches.

When law enforcement uploads a DNA sample to a commercial database for comparison, it does not violate any reasonable expectation of privacy for the site's users, provided that the site's terms clearly inform users that law enforcement may access their data and gives them an option to opt-out. Traditional lenses of Fourth Amendment rights, such as property law concepts[320] or the third-party search doctrine,[321] do not adequately protect the privacy concerns of DNA, which may be voluntarily surrendered by an individual but reveal deeply personal information about his or her blood relatives. Aside from regulating law enforcement actions, greater oversight of direct-to-consumer DNA testing consent processes can safeguard consumers' genetic privacy.[322]

For private databases whose terms prohibit law enforcement access, the industry status quo should remain in effect: only a warrant justifies a search, because the individuals who have uploaded DNA to such a site maintain a reasonable expectation of privacy.[323]

B. Cases of Serious Offenses

Second, the case constitutes a "serious offense," generally a violent

---

[318] *See also* Christopher Slobogin & James W. Hazel, "A World of Difference"?: Law Enforcement, Genetic Data and the Fourth Amendment, 70 DUKE L.J. 705 (2021) (advocating for consideration of the public's privacy concerns in judicial determinations of law enforcement use of DNA); Jamie M. Zeevi, *DNA Is Different: An Exploration of the Current Inadequacies of Genetic Privacy Protection in Recreational DNA Databases*, 93 ST. JOHN'S L. REV. 767, 807 (2019) (listing a statutory requirement disclosing law enforcement activity on commercial genealogy databases as a possible solution).

[319] Augenstein, *supra* note 135.

[320] Byrd v. United States, 138 S. Ct. 1518 (2018).

[321] United States v. Miller, 425 U.S. 435, 437 (1976).

[322] Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers*, 21 COLUM. SCI. & TECH. L. REV. 118, 185 (2019).

[323] *But see* Najla Hasic, *An Invasion of Privacy: Genetic Testing in an Age of Unlimited Access*,
44 S. ILL. U. L.J. 519, 553 (2020) (arguing that Congress should mandate an automatic opt-out feature for direct-to-consumer ancestry services and only allow direct, rather than familial, matches to protect relatives' privacy).

felony.[324] This builds on Supreme Court precedent in *Maryland v. King*,[325] in which the majority tacitly approved of a state law requiring mandatory collection of DNA samples for arrestees of violent crimes.[326] Following the arrest of the Golden State Killer, numerous sites in the genealogy industry changed their terms to allow law enforcement to upload crime scene DNA from only violent felonies, which are typically specified as murder, rape, and sexual assault.[327] The new industry standard includes this provision, but it should be codified in law rather than website user terms. Infringing on a reasonable privacy interest should constitute a violation of Fourth Amendment rights rather than a mere violation of website user terms. The Supreme Court has already upheld this rationale for DNA collection in cases of serious crimes,[328] and it is a logical extension to use this distinction in genetic genealogy.

In *Maryland v. King*,[329] the Court referenced state law that provided for collection of DNA from arrestees of "serious crimes" to have genetic profiles uploaded to CODIS.[330] Connecting this practice with pretrial release, the Court reasoned that arrestees who have previously committed other serious crimes are incentivized to flee.[331] The Maryland law in question defined crimes of violence for this purpose as including murder, rape, manslaughter, first-degree assault, kidnapping, arson, sexual assault, carjacking, robbery, and others.[332]

Justice Scalia, in his dissent, critiqued the majority's similar limit to serious crimes.[333] He noted that the majority did not explain its reasoning for this limitation.[334] Further, he tied his criticism of the limitation to his disbelief of the majority's reasoning that DNA testing of arrestees will help identify them.[335] DNA testing would be equally capable of identifying a person arrested for a violent felony as it would a petty misdemeanor.[336] Ominously, the focus on identification of the arrestee will lead to more uses of

---

[324] *See* Zeevi, *supra* note 319, at 807–08 (listing statutory restriction of genetic genealogy to violent crimes as one possible solution to genetic privacy issues).
[325] Maryland v. King, 569 U.S. 435 (2013).
[326] *Id.* at 444.
[327] See GEDmatch, *supra* note 46 (revising terms of service and privacy policy to specify when law enforcement may access data).
[328] *King*, 569 U.S. at 435.
[329] *Id.*
[330] *Id.* at 436.
[331] *Id.* at 455.
[332] Md. Code Ann., Crim. Law § 14-101.
[333] *King*, 569 U.S. at 481-82.
[334] *Id.* at 481.
[335] *Id.*
[336] *Id.*

identification, such as airline security, and driver's licenses.[337] Instead, he argued, the majority should have simply ruled that the practice of requiring a DNA sample for felony convicts would have been permissible under the Fourth Amendment, with no burden on innocent arrestees.[338]

A limitation on DNA-related searches to serious crimes is proper given the power of DNA identification, and for reasons that neither the majority nor the dissent in *Maryland v. King*[339] contemplate. The majority discusses identification of suspects, and the dissent rejects any proper purpose for taking a DNA sample for identification before conviction.[340] Instead, limiting DNA collection and searches to serious crimes strikes a balance between individuals' privacy in their DNA and the need to bring serious offenders to justice.

C. Last Resort

Third, prior to using genetic genealogy, law enforcement has thoroughly investigated the crime over a sufficient period of time without successfully identifying the offender.[341] A bright-line rule for a waiting period would be an ineffective solution, considering the variances in each murder case. Such a rule might even incentivize homicide detectives with limited resources[342] to wait out the time period and then use genetic genealogy. Instead, a "sufficient" period of time means the point at which law enforcement has followed investigative procedures without identifying a suspect, and the case would otherwise become cold.[343] California has set a similar policy for its criminal databases; law enforcement must exhaust investigative methods before searching for familial, rather than exact, DNA matches.[344] Genetic genealogy will undoubtedly become an attractive method of solving crimes as more of the most notorious killers and rapists continue to be identified through this technique. As more people upload their DNA to genealogy

---

[337] *Id.*
[338] *Id.* at 481–82.
[339] *Id.* at 435.
[340] *Id*. at 466–67.
[341] *See* Zeevi, *supra* note 319, at 807–08 (listing statutory restriction of genetic genealogy to crimes where all other investigative methods have been exhausted as one possible solution to genetic privacy issues).
[342] *See generally* Kimbriell Kelly, Wesley Lowery & Steven Rich, *Buried under bodies*, WASH. POST (Sept. 13, 2018), https://www.washingtonpost.com/news/national/wp/2018/09/13/feature/even-with-murder-rates-falling-big-city-detectives-face-daunting-caseloads/ (explaining how homicide detectives in many city police departments are assigned more cases than they can solve, leading to lower arrest rates).
[343] FA Zeevi, supra note 319, at 807–08.
[344] Hodge, *supra* note 148, at 53.

websites each year, crime scene DNA will have closer matches. Accordingly, it will take fewer investigative resources to connect the relative "matched" on a database to the actual offender. When nearly everyone has a close relative with an accessible DNA profile, law enforcement—and the public—may see genetic genealogy as the first step toward solving a crime. However, thus far genetic genealogy has only been used to solve cold cases, and it should remain this way.[345] Genetic genealogy represents an expansion of government interference that should be reserved for otherwise-unsolvable cases of the worst nature. Law enforcement has used this tool with adequate judgment and discretion until now, and the genealogy industry has implemented policies to this effect.[346] This Comment proposes maintaining the status quo on this point through legislative or judicial means.

V. IMPLICATIONS OF UNRESTRICTED USE OF GENETIC GENEALOGY

Criminal prosecution is not the only potential for misuse of genetic genealogy. Before the arrest of the Golden State Killer, the expansion of commercial DNA collection had already presented concerns for abuse in healthcare and medical research.[347] If left unchecked, the aggregate effect of genetic profiles in growing government and commercial databases will remove any meaningful opportunity to retain genetic privacy.

One possible consequence of unchecked privacy policies on commercial DNA databases is abuse in the healthcare field.[348] DNA testing can reveal health conditions that a person may be predisposed to contracting.[349] This information can allow a person to get screening and avoid factors that would increase the likelihood of developing the condition.[350] Unfortunately, health insurance companies could also use this data for nefarious purposes.[351] They could potentially raise insurance rates based on genetic risk or deny coverage entirely.[352] Such actions would warp a positive aspect of DNA testing and negatively affect people's health by denying them affordable healthcare.

---

[345] FA See Zeevi, supra note 319, at 806. (describing law enforcement's use of familial searching in DNA databases as just beginning).
[346] GEDmatch, *supra* note 43.
[347] Sarah Washburn, *Controlling Your DNA: Privacy Concerns in Genomic Testing and the Uncertainty of Federal Regulation and Legislation*, 18 DEPAUL J. HEALTH CARE L. 1, 15 (2016).
[348] *Id.*
[349] *Id.*
[350] *Id.* at 15–16.
[351] *Id.* at 25. *See also* Jennifer Cacchio, *What You Don't Know Can Hurt You: The Legal Risk of Peering into the Gene Pool with Direct-to-Consumer Genetic Testing*, 87 UMKC L. REV. 219 (2018).
[352] *Id.*

Thus, the problem of genetic privacy in healthcare mirrors that of genetic genealogy. Potential for abuse of the technology in the future justifies preemptive safeguards.

In 2020, the federal government announced a plan to begin collecting DNA samples from citizens and permanent residents who are detained at the border.[353] This collection utilizes the Fourth Amendment exceptions for searches at the border to screen for potential terrorists or criminals entering the country with false identification.[354] Under this plan, the government would indefinitely store the DNA samples in CODIS alongside those of convicted felons.[355] The plan essentially conflates the permissible storage of felons' DNA[356] with the border search exception in a way not anticipated by either doctrine. The standard for detention at the border does not rise to the level of suspicion required for law enforcement to make an arrest for a felony charge, which does allow for DNA collection.[357] Accordingly, this plan could easily lead to a gradual decline in the judicial process necessary for the government to collect and indefinitely retain more peoples' DNA in a criminal database.

The gradual expansion of government DNA and commercial databases may eventually cause a complete lack of genetic privacy. Concerns over this lack of privacy could even result in fewer people taking DNA tests or opting-in to law enforcement searches, thus weakening the effectiveness of genetic genealogy.

VI. CONCLUSION

DNA has rapidly enhanced the criminal justice system by providing a reliable method for investigators to determine if a person was at the scene of a crime. With the collection of samples in state and federal databases and use of familial matching, law enforcement can find criminals without first

---

[353] Nomaan Merchant, *US to Start Collecting DNA From People Detained at Border,* DETROIT NEWS (Jan. 6, 2020), https://www.detroitnews.com/story/news/local/detroit-city/2020/01/06/dna-testing-bordeer-collection/40952247.

[354] *US Proposal to Collect DNA from Detained Immigrants Violates Privacy Rights*, HUMAN RIGHTS WATCH (Nov. 12, 2019), https://www.hrw.org/news/2019/11/12/us-proposal-collect-dna-detained-immigrants-violates-privacy-rights.

[355] *You need a good reason to curb privacy. None exists for collecting DNA at the border*, WASHINGTON POST (Jan. 11, 2020), https://www.washingtonpost.com/opinions/you-need-a-good-reason-to-curb-privacy-none-exists-for-collecting-dna-at-the-border/2020/01/11/9a206388-33df-11ea-9313-6cba89b1b9fb_story.html.

[356] Maryland v. King, 569 U.S. 435, 435 (2013).

[357] *See US Proposal to Collect DNA from Detained Immigrants Violates Privacy Rights*, *supra* note 335. (suggesting that the Court's limitation in Maryland v. King may make warrantless DNA collections violate the rights of the border detainees if they have only committed a civil violation).

connecting them to the crime via traditional investigative methods. Simultaneously, the genetic genealogy industry has provided health and family information to millions of people. The use of genetic genealogy in solving crimes brings into question the appropriate manner for law to adapt to technology and the right balance to strike between security and Fourth Amendment privacy rights.

Genetic genealogy presents unique issues to traditional legal principles of searches, the third-party search doctrine, and standing. When law enforcement uploads crime scene DNA to a commercial database, the sample will match to a relative rather than the offender.[358] Because the relative disclosed the sample, the suspect may not have standing to challenge the search.[359] Furthermore, another legal issue is that the offender did not choose to disclose the DNA to a database. Since the disclosure usually comes from the suspect in third-party search doctrine cases, this adds a new wrinkle when applying the doctrine.[360] Additionally, recent Supreme Court precedent shows a tendency to consider the sensitive nature of data in modern society.[361] DNA deserves at least as much privacy protection as cell phone location information receives.

Law enforcement should continue to use genetic genealogy responsibly, as it has in catching the Golden State Killer and numerous other serial rapists and murderers. Specifically, genetic genealogy should only be used to solve violent felonies which cannot be solved through traditional investigations, and commercial databases that allow such searches must inform users or give them an opportunity to opt-out. The DNA testing industry has largely adopted the practice of giving users an opportunity to opt-in or opt-out to law enforcement searches, but trust in user agreements is insufficient to safeguard genetic privacy. Congress and state legislatures should regulate this practice before it can grow beyond its current state and become a common tool for law enforcement. Genetic genealogy should remain reserved for solving only the most serious crimes, which inflict pain on victims, families, and society at large. Law enforcement has successfully used the method to arrest dozens of violent criminals[362] who would have evaded detection forever and left victims searching for the truth. Genetic genealogy can remain a valuable tool for solving crimes by codifying the restrictions already in place by law

---

[358] Jouvenal, *supra* note 25.
[359] Dery, *supra* note 227, at 143.
[360] Park, *supra* note 197. (citing Carpenter 138 S. Ct. at 2206) (stating that the traditional third-party search doctrine does not apply to CSLI).
[361] *Id.*
[362] Parabon NanoLabs, *supra* note 41; *See also* Portia Bruner, *Genetic Genealogy Helps Solve 1999 Rape Cases*, FOX 5 ATLANTA (Jan. 21, 2020), https://www.fox5atlanta.com/news/genetic-genealogy-helps-solve-1999-rape-cases; Stanton et al., *supra* note 271; Hodge, *supra* note 148, at 50.

enforcement and the DNA testing industry.