EDITOR'S NOTE

Welcome to the third Issue of Volume 73 of the *Federal Communications Law Journal* (*Journal*), official journal of the Federal Communications Bar Association (FCBA). This Issue contains topics spanning from deceptive media moderation to law enforcement use of private consumer surveillance data. Once again, this Issue exemplifies the increasingly wide scope of telecommunications and technology scholarship.

This Issue begins with an Article authored by Shannon Sylvester, a GW Law alumna, discussing the specific role of deepfakes as a method of spreading misinformation and their effect on a democratic society. Sylvester then provides social media platform-specific proposals to address the harm caused by deepfakes.

This Issue also features three student Notes. In the first Note, Christopher Frascella examines the relationship between law enforcement and companies that sell consumer surveillance equipment, like Amazon and the Amazon Ring. Frascella examines the ways in which consumer protection law could provide recourse for the privacy concerns arising from such relationships. In the second Note, Erin Seeton illustrates that victims of child pornography are further harmed by the current restitution scheme. Seeton proposes an amendment to the Copyright Act of 1976 and explains that such victims may be able to better recover under her proposal. In the third Note, Jasmine Arooni describes vulnerability disclosure programs and the U.S. Government's role in their governance. Arooni recommends a combination of federal government approaches for similar, private vulnerability disclosure programs.

This Issue also features our Annual Review about this year's noteworthy decisions with case briefs written by incoming Volume 74 Editorial Board members.

On behalf of the entire Volume 73 team, many thanks to the FCBA and The George Washington University Law School for their support. On my own behalf, many thanks to the Volume 73 Editorial Board, Associates, Members, and Authors who made this Volume possible. As our Volume 73 Editorial Board graduates this May, we leave the journal in the capable hands of the Volume 74 Editorial Board and wish you many successes.

The *Journal* is committed to providing its readership with rigorous academic scholarship and thought leadership in telecommunications and technology law. Please send submissions to be considered for publication to fcljarticles@law.gwu.edu. All other questions or comments may be directed to fclj@law.gwu.edu. This Issue and our archive are available at www.fclj.org.

Elissa C. Jeffers
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

VOLUME 73

Published by the GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
and the FEDERAL COMMUNICATIONS BAR ASSOCIATION

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association (FCBA) and The George Washington University Law School. The *Journal* publishes three issues per year and features articles, student notes, essays, and book reviews on issues in telecommunications, the First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, privacy, communications and information policymaking, and other related fields.

As the official journal of the FCBA, the *Journal* is distributed to over 2,000 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at www.fclj.org.

The *Journal* is managed by a student Editorial Board, in cooperation with the Editorial Advisory Board of the FCBA and two Faculty Advisors.

Federal Communications Bar Association

The FCBA (d/b/a FCBA – The Tech Bar) is a volunteer organization of attorneys, engineers, consultants, economists, government officials and law students involved in the study, development, interpretation and practice of communications and information technology law and policy. From broadband deployment to broadcast content, from emerging wireless technologies to emergency communications, from spectrum allocations to satellite broadcasting, the FCBA has something to offer nearly everyone involved in the technology, media, and telecommunications industries. That's why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

Through its many professional, social, and educational activities, the FCBA offers its members unique opportunities to interact with their peers and decision-makers in the communications and information technology field, and to keep abreast of significant developments relating to legal, engineering, and policy issues. Through its work with other specialized associations, the FCBA also affords its members opportunities to associate with a broad and diverse cross-section of other professionals in related fields. Although the majority of FCBA members practice in the metropolitan Washington, DC area, the FCBA has 11 active regional chapters, including: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Southern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the U.S., its territories, and several other countries.

The George Washington University Law School

Established in 1865, The George Washington University Law School (GW Law) is the oldest law school in Washington, DC. The Law School is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. GW Law has one of the largest curricula of any law school in the nation with more than 275 elective courses covering every aspect of legal study.

GW Law's home institution, The George Washington University is a private institution founded in 1821 by charter of Congress. The Law School is located on the University's campus in the downtown neighborhood familiarly known as Foggy Bottom.

The *Federal Communications Law Journal* is published by The George Washington University Law School and the FCBA three times per year. Offices are located at 2028 G Street NW, Suite LL-020, Washington, DC 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to FCBA, 1020 19th Street NW, Suite 325, Washington, DC 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in US dollars, and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at fclj@law.gwu.edu.

Single and Back Issues: Each issue of the current volume can be purchased for $15 (domestic, Canada and Mexico) or $20 (international), paid in U.S. dollars. Please send all requests for single or back issues to fclj@law.gwu.edu.

Manuscripts: The *Journal* invites the submission of unsolicited articles, comments, essays, and book reviews mailed to the office or emailed to fcljarticles@law.gwu.edu. Manuscripts cannot be returned unless a self-addressed, postage-paid envelope is submitted with the manuscript.

Production: The citations in the *Journal* conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia L. Rev. Ass'n et al. eds., 21st ed., 2020). Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Joe Christensen, Inc.

Citation: Please cite this issue as 73 FED. COMM. L.J. ___ (2021).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 73 ISSUE 3

APRIL 2021

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLE

Deceptive media can be dangerous in a democratic society, which values the pursuit of truth. Deceptive media, as the name suggests, deceives us by distorting the truth and reality. Deepfakes are a type of deceptive media, and they often deceive us by betraying our senses of sight and hearing. As misinformation and disinformation campaigns run rampant on social media sites, deepfakes threaten to add more confusion and uncertainty to the mix. To protect our democratic integrity, the threat of deepfakes needs to be addressed. This Article will show just how damaging deepfakes can be to a democratic society and why we need to take action now. Social media platforms can help mitigate the risks deepfakes pose to society by taking steps to curb the harm of deepfakes through independent fact-checking and stronger enforcement actions. This Article will provide solutions and best practices for social media sites to help them address the growing problem of deepfakes.

NOTES

Global technology companies are partnering with local police to secure buy-in from homeowner watchmen for a consumer-enhanced surveillance regime at the expense of the watched passers-by, with disproportionate impacts on people of color. As long as surveillance-based data collection continues to be profitable, companies like Amazon will continue to seek to grow these partnerships, absent friction that makes them inefficient. Although the most comprehensive solution would be a meaningful federal privacy law, a more immediate means of mitigation exists in consumer protection law. Consumer privacy laws do not adequately address the underlying privacy issues of these

Don't Let Them Fake You Out: How Artificially Mastered Videos Are Becoming the Newest Threat in the Disinformation War and What Social Media Platforms Should Do About It

Shannon Sylvester*

TABLE OF CONTENTS

* Shannon Sylvester received her J.D. from The George Washington University Law School in 2020. She would like to thank Professor Dawn Nunziato for the idea and for her support and encouragement while drafting this Article.

I. INTRODUCTION

It looked like former President Barack Obama. It sounded like former President Barack Obama. And without a second glance it fooled the best of us into thinking it *was* former President Barack Obama.[1] The "it" was a deepfake, an artificially generated video that used images and audio cloning technology to imitate the former President, making it appear as though he was saying things that he, in fact, never said.[2]

"This is a dangerous time," the fake Obama warned as he claimed, "[w]e need to be more vigilant with what we trust from the Internet."[3] While the video convincingly portrayed the former president addressing the nation, it was only because of a lack of eloquence that the video's creator Jordan Peele gave to Obama that people questioned the truth of the video.[4]

But what if Peele refused to admit that he created the video? The video, hosted on YouTube, has over 8.3 million views.[5] BuzzFeed's title of the video, "You Won't Believe What Obama Says In This Video!" followed by an emoji wink, is an obvious attempt to get people to click on the video.[6] Many people, intrigued by the title of the video, might be tempted to click on the link, and find themselves believing it was indeed former President Barack Obama saying obscenities, rather than a fake.

Believing that the former President used profanity while addressing the nation, could at a basic level, harm the President's reputation, but at a higher level, stands to do much more damage. Beyond the President's reputation, the nation's reputation could be harmed abroad. Critics of Obama could be further inflamed by the former President's offensive remarks in the video. Peele's deepfake Obama video sought to warn us of the real possibilities of disruption that could be caused by this manipulating technology. It further attempted to show that deepfakes can impair our understanding of the truth through deception, and in the hands of bad actors, can contribute to our already toxic and uncivil political discourse. The technology used to create deepfakes is advancing, and in the future, realistic deepfakes that might not be so easily debunked threaten to disrupt our already fragile democratic infrastructure.

This Article will explore the manipulative effects of deepfakes and how their truths can spread if left unchecked, significantly disrupting democracy.

---

1. *See* David Mack, *This PSA About Fake News From Barack Obama Is Not What It Appears*, BUZZFEED NEWS (April 17, 2018), https://www.buzzfeednews.com/article/davidmack/obama-fake-news-jordan-peele-psa-video-buzzfeed [https://perma.cc/6DRW-56BE].

2. *See id.*

3. *Id.*

4. *See id.* In the video, Peele, as Obama, calls President Trump a "dipshit" and argues the world is "fucked."

5. BuzzFeed Video, "You Won't Believe What Obama Says In This Video!", YOUTUBE (Apr. 17, 2018), https://www.youtube.com/watch?v=cQ54GDm1eL0 [https://perma.cc/8HNZ-KZ9E].

6. *See generally* Jessica Silbey & Woodrow Hartzog, *The Upside of Deep Fakes*, 78 MD. L. REV. 960, 964 (2019) (claiming that "eyeballs demand catchy headlines and lots of photographs").

Part I of this Article will introduce the origins of deepfakes and explain the technology and techniques that make up a deepfake. This section will also describe how deepfakes emerged on the consumer scene, and how this can have some beneficial uses—but like any technology, many negative implications as well. Part II will focus on deepfakes as catalysts to the disinformation war. As trust in the media has waned over the years, especially in the era of "fake news," public faith in the media to deliver accurate, credible news has become increasingly important. First Amendment constraints add difficultly to legislators seeking to regulate deepfakes, especially on social media sites where companies currently enjoy immunity through Section 230 of the Communications Decency Act (CDA). Social media sites are thus a prime market for deepfakes to thrive. Realizing this, some social media companies have adopted policies banning deepfakes, but they do not go far enough.

Part III of this paper will prescribe guidance on further steps social media companies should take to combat deepfakes. Social media companies should look towards helping policymakers and legislators define more clearly what deepfakes are and develop standards aimed at addressing the manipulation issues caused by deepfakes. In addition, companies should look towards adopting technological solutions. However, because social media sites are set up and run differently, there is no "one size fits all" approach when it comes to regulation and enforcement. Therefore, this paper attempts to show the problems deepfakes can cause and offer best practices that social media companies can adopt to help prevent the onslaught of damage deepfakes threaten to do if left unguarded.

II. DEEPFAKES DEFINED

Manipulated media encompasses a wide range of material, with deepfakes falling under that umbrella.[7] Deepfakes are a type of manipulated media created entirely through artificial intelligence (AI) processes.[8] "Deep" describes the "deep-learning" aspect of deepfakes, whereas "fake" refers to the fact that the video created often depicts people saying or doing things they never said or did.[9] Deepfakes should be distinguished from shallowfakes, which are also manipulated media, but manipulated through *human* intervention rather than artificial intelligence.[10]

---

7. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1759 (2019).

8. *See* Alex Engler, *Fighting Deepfakes when Detection Fails*, BROOKINGS (Nov. 14, 2019), https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/ [https://perma.cc/YZF6-BFFA].

9. *See* Mary Ann Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*, 78 MD. L. REV. 892, 893 (2019).

10. *See* Bobby Johnson, *Deepfakes Are Solvable—But Don't Forget That "Shallowfakes" Are Already Pervasive*, MIT TECH. REV. (Mar. 25, 2019); *see, e.g.*, Sarah Mervosh, *Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, Helped by Trump*, N.Y. TIMES (May 24, 2019), https://www.nytimes.com/2019/05/24/us/politics/pelosi-doctored-video.html [https://perma.cc/86JL-VEUR] (showing a shallowfake video that went viral, featuring House Speaker Nancy Pelosi appearing to slur her speech).

The technology that creates deepfakes is relatively simple to access and use.[11] But when that technology becomes more readily available on the consumer market, that raises concerns about the widespread use of deepfakes. As deepfakes enter the mainstream and grow in popularity, it is likely the technology used to create them will also become more advanced. If all it takes now is downloading an app to your phone to create a deepfake, imagine what a malicious actor could do with more sophisticated technology.[12] This section will explain the technology surrounding deepfakes and how its uses extend beyond its initial inception in Reddit threads.

A. Neural Networks and the GAN Approach

Deepfakes use deep learning, or neural network processes, known as "Generative Adversarial Networks" or GANs to function.[13] Deep learning dates back to the 1950s, when Frank Rosenblatt attempted to build a machine with a brain.[14] The idea of giving robots minds is why deep learning processes are often referred to as "neural networks."[15]

The GAN neural network process involves two networks that work against each other to produce the outcome.[16] The first network, the generator, uses a sample dataset of images to create a new image based on the sample set.[17] The second network, the discriminator, receives the new "fake" image from the generator and determines how successful the generator was at creating a plausible image.[18] If the discriminator determines the new image is inadequate and does not match up against the subject (e.g., if the mouth does not line up when the subject speaks), the discriminator sends the image back to the generator so the generator can churn out a new and improved image.[19]

The GAN method works with both images and audio clips.[20] Jose Sotelo of AI company Lyrebird, described his company's audio AI as pattern-matching.[21] The program runs by finding the uniqueness in a voice and then

11. *See* Chesney & Citron, *supra* note 7, at 1763.
12. *See, e.g.*, REFLECT, https://reflect.tech/faceswap/hot (last visited Mar. 29, 2021) [https://perma.cc/DS95-CCGV].
13. *See* Chesney & Citron, *supra* note 7, at 1761.
14. Gary Marcus, *Is "Deep Learning" a Revolution in Artificial Intelligence?*, NEW YORKER (Nov. 25, 2012), https://www.newyorker.com/news/news-desk/is-deep-learning-a-revolution-in-artificial-intelligence [https://perma.cc/GZ9Y-5GGT].
15. *Id*.
16. *Id.*
17. *See* Ian Sample, *What Are Deepfakes – And How Can You Spot Them?*, THE GUARDIAN (Jan. 13, 2020), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [https://perma.cc/WJL8-MN5X].
18. *Id.*
19. *See* Chesney & Citron, *supra* note 7, at 1760–61.
20. *Id.*
21. *Sleepwalkers, Truth to Power*, IHEARTRADIO (May 30, 2019), https://www.iheart.com/podcast/1119-sleepwalkers-30880104/episode/truth-to-power-45383294/ [https://perma.cc/GHU3-3436].

attempting to recreate that uniqueness.[22] While a fake audio message could be detrimental, a fake video is often times more damaging because it betrays both hearing and sight.[23]

Another way to think of the GAN approach is as a game of trickery.[24] The first machine tries to trick its adversary, the second machine, into believing the image or audio clip is legitimate.[25] If the second machine can easily spot the fake, it sends it back to the first machine to try again.[26] The first machine tries repeatedly until it can successfully trick the second machine into believing the image or audio clip is real.[27]

GANs have made their way into the consumer sphere.[28] Using the GAN approach, many companies work on their ability to create seamless deepfakes using just one video source or one photo source.[29] The results are impressive for the minimal effort it takes to create a convincing deepfake.[30] The ease of accessing and using deepfake technology for consumers has already resulted in a variety of entertaining purposes. Deepfakes have the potential to increase creative expression and even benefit the health industry, but they also have the potential to wreak havoc on individual liberty and democratic institutions.

B. From Hollywood to Handhelds

Deepfakes are relatively new to the consumer scene, but Hollywood's special effects teams have dabbled with the technology for years. The film *Forrest Gump* (1994) included an appearance by President John F. Kennedy, digitally recreated from archival video.[31] When Paul Walker died halfway through filming *Furious 7*, his brothers served as face templates to form a digital recreation of him used in the rest of the movie.[32] Even more recently, facial mapping and AI programming made actors look years younger in the

22. *See id.*; *see also* Andrew Mason, *How Imputations Work: The Research Behind Overdub*, DESCRIPT (Sept. 17, 2019), https://www.descript.com/post/how-imputations-work-the-research-behind-overdub [https://perma.cc/QF2Q-XPX7] (providing an overview of Descript company Lyrebird's audio cloning processes).

23. *Sleepwalkers*, *supra* note 21 (explaining how the host of the podcast's voice was used to create an artificial "robo" voice that was then used to prank call the host's aunt to ask for money).

24. *Id.* at 14:03.

25. *Id.*

26. *Id.* at 14:10–14:13.

27. *Id.*

28. *See generally* REFLECT, *supra* note 12.

29. *See* Colum Murphy & Zheping Huang, *Social Media Users Entranced, Concerned by Chinese Face-Swapping Deepfake App*, TIME (Sept. 4, 2019 at 10:57 AM), https://time.com/5668482/chinese-face-swap-app-zao-deep-fakes/ [https://perma.cc/4JS8-C4WF].

30. *Id.*

31. *See Pentagon's Race Against Deepfakes*, CNN BUSINESS INTERACTIVE (2019), https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

32. *See* Will Knight, *The World's Top Deepfake Artist Is Wrestling With The Monster He Created*, MIT TECH. REV. (Aug. 16, 2019), https://www.technologyreview.com/s/614083/the-worlds-top-deepfake-artist-is-wrestling-with-the-monster-he-created/ [https://perma.cc/M2KL-8WZC].

Netflix film, *The Irishman*.[33] As technology improves, some hypothesize that actors will be able to license their likeness for use in television and movies without ever needing to read lines on camera.[34] Take the same technique, put it in the hands of the consumer, and suddenly the consumer becomes the director.[35] Moviegoers can make their ideal cast ensemble for their favorite movie possible with this new technology.[36] Ever wonder what Nicholas Cage would look like in *Superman*?[37] People on the Internet did, and one of the first trends of consumer-use deepfakes included putting Cage into as many movies as possible.[38] The Internet's obsession with Cage (maybe catapulted from his appearance in *Face/Off*)[39] shows the potential for consumers to embrace their creative sides as they start reimagining film.

The fascination with swapping faces helped create a market for deepfakes that consumers can create with the push of a button.[40] For instance, a popular Chinese app, Zao, allows users to upload their own photos and then superimpose their face onto a celebrity's, making the user appear to star in famous Hollywood movies.[41] The app works in seconds, and for the short amount of time used to make the video, the quality is surprisingly good.[42] Other apps such as FaceApp gained popularity when users found enjoyment making themselves age and swap genders.[43] The gaming industry is also looking to deepfakes to help make their games more attractive, allowing consumers to "play as themselves" rather than choose a character avatar.[44]

Besides their entertainment purposes, deepfakes can enrich our educational experiences and apply to the healthcare field.[45] Using a combination of GANs with virtual reality technology, prominent historical figures can appear before our very eyes. *TIME* magazine helped create an all-immersive exhibit of a depiction of Martin Luther King Jr. giving his famed "I Have a Dream" speech.[46] Health companies and researchers have also benefitted from deepfakes by using the technology to create fake brain scans with algorithms that spot tumors.[47] Just as the GAN approach helps brings the

33. *See* Angela Watercutter, *The Irishman Gets De-Aging Right – No Tracking Dots Necessary*, WIRED (May 12, 2019), https://www.wired.com/story/the-irishman-netflix-ilm-de-aging/ [https://perma.cc/LD6H-7XSR].
34. *Sleepwalkers*, *supra* note 21, at 23:00–24:00.
35. *Id.* at 26:30–29:00.
36. *Id.*
37. *Id.*
38. *Id.*
39. *Sleepwalkers*, *supra* note 21, at 27:00.
40. Murphy & Huang, *supra* note 29.
41. *Id.*
42. *Id.*
43. *Id.*
44. Knight, *supra* note 32.
45. *See* Simon Chandler, *Why Deepfakes Are a Net Positive for Humanity*, FORBES (Mar 9, 2020), https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/#97adbfc2f84f [https://perma.cc/Q92L-TDAL].
46. TIME: THE MARCH (2019), https://time.com/the-march/ [https://perma.cc/AS4R-EPP8].
47. *See* Chandler, *supra* note 45.

dead back to life, it can also bring life back to a patient who has lost their voice.[48]

Although deepfakes have the potential for positive applications, the majority of deepfakes circulating the web are pornographic in nature.[49] Startup Deeptrace found that pornographic deepfakes, while accounting for about 96% of deepfakes on the Internet,[50] are also disproportionately female.[51]

In December 2017, one user on Reddit posted a thread showcasing how technology made it possible to superimpose a celebrity's face onto a porn star's face, making it appear as though the celebrity was starring in a porn video.[52] In these early stages of deepfakes, the quality was poor, and it was relatively easy to distinguish the videos as fakes. However, that did not stop the harm caused by pornographic deepfakes from spreading worldwide.

In Malaysia, for example, where gay sex is illegal, a political aide was arrested following publication of a video showing him having sex with another man.[53] While the Malaysian prime minister alleged the video was a deepfake, independent experts were unable to tell if his allegation could be proved correct. [54] If the video could have been proved to be a deepfake, the political aide may not have lost his job, even though he still suffered emotional and reputational harm. But if the video was real, it presents another challenge: those accused of committing illegal acts can falsely claim manipulation of video evidence.

As deepfakes become more sophisticated and integrated into society, they present authentication challenges in a growing landscape of disinformation.[55] Not only will individuals need to be increasingly aware of fact and source checking, but they should also be wary of the prominence for plausible deniability, with public figures able to deny the credibility of a leaked video, pointing out that it might be a deepfake.[56] To combat this grim outlook, foresight is key. Educating people about deepfakes before they become technically advanced might help quell future damage from exposure to deepfakes by boosting awareness. Social media companies need to play their part in diffusing the problem of disinformation in society by adopting policies aimed at tackling manipulative media that seeks to harm. Then, there can be hope for a world where deepfakes can exist for their beneficial purposes without compromising individual liberties and democratic institutions.

---

48. *See* Sleepwalkers*, supra* note 21, at 15:20–17:00.

49. *See* Tom Simonite, *The Web Is Drowning in Deepfakes and Almost All of Them Are Porn,* WIRED (Oct. 13, 2019), https://www.wired.co.uk/article/deepfakes-porn [https://perma.cc/F8EJ-M64E].

50. *Id.*

51. Franks & Waldman, *supra* note 9, at 893–94.

52. *See* Samantha Cole, *AI-Assisted Fake Porn Is Here and We're All F**ked,* VICE: MOTHERBOARD (Dec. 11, 2017), https://www.vice.com/en_us/article/gydydm/gal-gadot-fake-ai-porn [https://perma.cc/5XAB-F3E6].

53. *See* Simonite, *supra* note 49.

54. *Id.*

55. *Id.*

56. *Id.*

III. DEEPFAKES AMPLIFY THE PROBLEM OF DISINFORMATION

> "Just remember: What you're seeing and what you're reading is not what's happening."
>
> – President Donald Trump[57]

Photos and videos add credibility to stories because we trust our senses. Deepfakes force us to betray our reliable senses of hearing and sight because by their very nature, they misrepresent something real.[58] The common saying, "seeing is believing," is less true, thanks to deepfakes.

Adding to the confusion, former President Donald Trump repeatedly criticized the media's coverage of events, questioning the credibility of the press and telling his supporters not to believe what he called, the "fake news" media.[59] Fake news is not a new issue, but one that the Trump Administration and the emergence of social media sites have exacerbated.[60] Social media sites are known catalysts for causing distrust and panic with a proliferation of false information. Deepfakes, likely to infiltrate the fake news haven of social media sites, threaten to bring a new wave of confusion around trusting our sources and senses.

This section will discuss fake news generally, and how deepfakes will likely aggravate the fake news problem. Many social media companies have written their own policies to stop the spread of deepfakes, and their awareness and policies point towards a step in the right direction.

A. Disinformation Campaigns and the Difficulty in Seeking out the Truth

Social media has created a new space for political candidates to launch their campaigns and reach their supporters.[61] There is an obsession with the idea of going viral, which essentially means mass publicity.[62] Real news and

---

57. Justin Wise, *Trump: What You're Seeing in the News 'Is Not What's Happening,'* THE HILL (July 24, 2018), https://thehill.com/homenews/administration/398606-trump-what-youre-seeing-in-the-news-is-not-whats-happening-inbox-x [https://perma.cc/9PVJ-ZHF9] (reporting on President Trump giving a speech in Kansas at the Veterans of Foreign Wars National Convention).

58. *See id.*

59. *Id.*

60. *See* McKay Coppins, *The Billion-Dollar Disinformation Campaign to Reelect the President,* THE ATLANTIC (Feb. 10, 2020, 2:30 PM), https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/ [https://perma.cc/4RK5-2MKH].

61. *See* John Wihbey, *The Challenges of Democratizing News and Information: Examining Data on Social Media, Viral Patterns and Digital Influence*, *in* Shorenstein Center on Media, Politics

and Public Policy Discussion Paper Series 2 (2014) (emphasizing that social media sites boast billions of users).

62. *See id.* at 8.

fake news alike get attention due to the trending algorithms on social media sites.[63] Businesses quickly picked up on this phenomenon and started "viral marketing."[64] The explosive effect that this phenomenon promises, reaching millions of people seemingly instantly, is an attractive prospect to any marketer. But the vast reach of social media has also led to nefarious, disinformation campaigns.

1. Weaponizing Social Media

The Philippines has the highest consumption of social media worldwide.[65] Journalist Maria Ressa said that "100% of Filipinos on the Internet are on Facebook."[66] This makes the country a perfect testing site for how influential social media campaigns can be, particularly on Facebook. The Philippines has been described as "patient zero" for using disinformation campaigns to help elect their current President, Rodrigo Duterte, before similar disinformation campaigns emerged in the U.K. with Brexit and the U.S. with former President Trump's 2016 election victory.[67] Duterte is good at playing the disinformation campaign game; when the Philippines announced new election rules in 2019[68] and Facebook started rolling out fact-checking techniques, the Duterte campaign adapted, creating ways to bypass the fact-checkers.[69] Duterte's team seemed to take a page out of a 2011 Kremlin manual that views disinformation as an "invisible radiation" appearing to take effect without individuals being realized they are being acted upon.[70]

The Duterte/Kremlin campaign tactics made their way to the U.S.[71] In the 2016 U.S. presidential election, fake news was rampant on social media

---

63. *See id*.

64. *See id.* at 25.

65. *See* GLOBAL WEB INDEX, SOCIAL 20 (2018), https://www.globalwebindex.com/hubfs/Downloads/Social-H2-2018-report.pdf [https://perma.cc/B6XD-GHMC] (finding that Filipinos spend on average 4 hours on social media a day).

66. *See* Ailsa Chang, *'A Thousand Cuts' Documentary Tracks Disinformation in Duterte's Philippines*, NPR (Feb. 3, 2020), https://www.npr.org/2020/02/03/802392333/a-thousand-cuts-documentary-tracks-disinformation-in-dutertes-philippines [https://perma.cc/7WDA-VJDT].

67. *See id*.; *see also* Craig Silverman, *The Philippines Was a Test of Facebook's New Approach to Countering Disinformation. Things Got Worse.,* BUZZFEED NEWS (Aug. 7, 2019), https://www.buzzfeednews.com/article/craigsilverman/2020-philippines-disinformation [https://perma.cc/LT5H-QPAZ] (citing an interview with Facebook's public policy director for global elections, Katie Harbarth, in which Harbath referred to the Philippines as "patient zero").

68. *See* Michael Bueza*, #PHVote: Campaign Rules for 2019 Midterm Elect*ions, RAPPLER (Feb. 28, 2019), https://www.rappler.com/nation/politics/elections/2019/224390-comelec-campaign-rules [https://perma.cc/NWC4-Y5K5].

69. *See* Silverman, *supra* note 67 (for example, Duterte's campaign avoided fact checkers by relying on microtargeting and promoting articles with minimal amounts of truth to avoid being flagged as false).

70. *See* Coppins, *supra* note 60.

71. *See id.* (noting that the Trump campaign understood the power of using "disinformation architecture" like that used in the Duterte campaign on Facebook and "methods of disinformation" referenced in a "2011 manual for Russian civil servants").

sites, with microtargeting being one of the key strategies used by candidates.[72] From #pizzagate to Pope Francis endorsing President Trump, the 2016 campaign trail was filled with falsities.[73] Misinformation drowned out fact. Even when the fake information was debunked, many social media users were already convinced. This phenomenon occurs due to the illusory truth effect.[74] The illusory truth effect describes how repeat exposure to false information increases the chances of people accepting the false information as true.[75] Ideas like counter-speech likely won't work because people who repeatedly encounter a fake story are more likely to remember it as true.[76]

In a society where we question everything, making the truth harder to discern, deepfakes will only add more uncertainty to the mix. Our continuous questioning leads us as a democratic society to value seeking out the truth, something that misleading speech carried in the medium of video manipulation makes quite difficult.[77] A Pew Research Center study conducted in November and December 2018 found that over half of the people surveyed believed that Americans' trust in the federal government and each other has been shrinking.[78] In a separate, further inquiry, around 49% of technology experts believed that technology will have a negative impact and mostly weaken core aspects of democracy, such as trust in government, in the coming decade.[79]

The decline in trust and lack of gatekeeping has made it extremely difficult to control the spread of disinformation.[80] Adding to this challenge are First Amendment concerns and platform liability issues related to Section 230 of the CDA.

2. Fake Speech is (Mostly) Free Speech

> Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the

72. *Id.*

73. *See* Hannah Ritchie, *Read All About It: The Biggest Fake News Stories of 2016*, CNBC (Dec. 30, 2016, 2:04 AM), https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html [https://perma.cc/HZ56-68QP].

74. *See* Franks & Waldman, supra note 9, at 894.

75. *See id.*

76. *Id.*

77. *Id.*

78. LEE RAINIE ET AL., PEW RES. CTR., TRUST AND DISTRUST IN AM. 3 (2019) (showing also that people believe it is important to fix this decline in trust and that the low trust makes it harder to solve problems in the U.S.).

79. Janna Anderson & Lee Rainie, *Many Tech Experts Say Digital Disruption Will Hurt Democracy*, PEW RES. CTR. (Feb. 21, 2020), https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/ [https://perma.cc/EB8P-JAEC].

80. Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1763–65 (2019).

> right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[81]

Freedom of speech is a fundamental right enshrined in the U.S. Constitution. Unlike other countries, the U.S. holds free speech to such a high standard it is difficult to restrict. Fake speech is merely a consequence of allowing people to engage in civil discourse and further the belief in the "marketplace of ideas."[82] The marketplace of ideas invokes the optimism that the truth will win out eventually, but as the illusory truth effect demonstrates, the marketplace of ideas is not an immaculate concept. Deepfakes are not ideas simply countered with "better" ideas. Since deepfakes involve freedom of expression, as long as they do not end up causing physical harm to a person, laws banning or restricting deepfakes would be unlikely to pass the strict scrutiny test of the First Amendment.[83]

Deepfakes by their very nature promote fake speech, but fake speech is constitutionally protected under *New York Times v. Sullivan*.[84] In that case, the U.S. Supreme Court held that public officials cannot sue for defamation unless they prove "actual malice," meaning the plaintiff must show that the false statement was made with knowledge of its falsity and in reckless disregard to the truth.[85] The Court then rationalized in *U.S. v. Alvarez* that fake speech should be protected because by itself, fake speech can be valuable in encouraging public discourse and it does not cause any legally cognizable harm.[86]

The Supreme Court has offered little guidance when it comes to fake speech in virtual applications, like videos. But in *Ashcroft v. Free Speech Coalition*, the Court suggested in dictum that "computer morphing" (using real images of children to frame the images being used in videos) might not be protected speech because it would cause harm similar to that in an appropriation suit, using the real child's likeness without their consent.[87] Defining true harm when it comes to speech is challenging, and the Court in *Ashcroft* chose to characterize harmful speech based on its emotional and reputational impacts.[88] But the Court in *Brandenburg v. Ohio* held that speech amounts to harmful incitement only when it is likely to produce imminent lawless action, commonly referred to as the *Brandenburg* test.[89]

---

81. U.S. CONST. amend. I.
82. Franks & Weldman, *supra* note 9, at 894.
83. Chesney & Citron, *supra* note 7, at 1790.
84. *See* N.Y. Times v. Sullivan, 376 U.S. 254 (1964).
85. *Id.* at 276.
86. *See* U.S. v. Alvarez, 567 U.S. 709, 719 (2012).
87. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 242 (2002) (holding that virtual child pornography is a protected form of free speech because no children are harmed and fake images are used).
88. *Id.*
89. *See* Brandenburg v. Ohio, 395 U.S. 44 (1969)

Attempts to regulate free speech, especially political speech, are often seen as an overreach of government power.[90] The fear is that speech regulation could turn partisan, with the government choosing to strike down speech with which it disagrees.[91] Some states have enacted laws banning political deepfakes, but these laws are wrought with First Amendment concerns.

a. Political Speech Deepfakes

In 2019, Texas amended its Election Code, making it a crime to create and publish a deepfake video within 30 days of an election with the intent to injure a candidate or influence the results of an election.[92] Violations of the law are punishable by up to a year in jail and a $4,000 fine.[93] The Act defines a deepfake as "a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality."[94] This definition is overbroad and appears to apply to shallowfakes and deepfakes alike as it does not draw a distinction between artificially made videos. There is also no exception for satire or parody videos that have been used in campaigns before, making illegal any video that "intends to deceive."[95]

The Texas law is an example of good intentions through misguided efforts. In an attempt to ban all political deepfake videos, the Act may do more harm than good. The law threatens to define truth, inserting government as a mediator to decide what deception means. It is also so broad that numerous political ads of past and present would likely trigger criminal liability for their creators or distributors if they ran within 30 days of an election.[96] It is unlikely that this law will withstand First Amendment challenges, as it does not seem narrowly tailored enough to restrict speech.[97]

The California legislature also recently addressed deepfakes. Effective as of January 1, 2020, California Assembly Bills 602 (AB 602) and 730 (AB 730) aim to curb the distribution of deepfakes.[98]AB 602 creates a private right

90. *See* Brown v. Hartlage, 456 U.S. 45, 46 (1982) ("The State's fear that voters might make an ill-advised choice does not provide the State with a compelling justification for limiting speech.").

91. *See* Helen Norton, *Lies and the Constitution*, 2012 SUP. CT. REV. 161, 199 (2012).

92. TEX. ELEC. CODE tit. 15, § 225.004 (2019).

93. *See* Matthew F. Farraro et al., *First Federal Legislation on Deepfakes Signed into Law*, WILMERHALE (Dec. 23, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law [https://perma.cc/87AF-XBYU].

94. TEX. ELEC. CODE tit. 15, § 225.004.

95. *Id.*

96. *See* Mark Rumold, *Not a Hoax: The Very Real Threat of Political 'Deepfakes' Laws*, ELEC. FRONTIER FOUND. (Apr. 27, 2020), https://www.eff.org/deeplinks/2020/04/not-hoax-very-real-threat-political-deepfakes-laws [https://perma.cc/YG83-VR6Q].

97. *See, e.g.*, Susan B. Anthony List v. Driehaus, 814 F.3d 466 (6th Cir. 2016) (holding election-based lies were an insufficient reason to restrict speech).

98. *See* K.C. Halm et. al, *Two New California Laws Tackle Deepfake Videos in Politics and Porn*, DAVIS WRIGHT TREMAINE LLP (Oct. 14, 2019), https://www.dwt.com/insights/2019/10/california-deepfakes-law [https://perma.cc/M4GD-SGCP].

of action for individuals depicted in sexually explicit material through digital or electronic technology.[99] Individuals can recover damages for emotional distress or statutory damages up to $150,000 if the act was committed with malice.[100]

AB 730 makes it illegal to create or distribute videos, images, or audio of politicians appearing in "fake videos" within 60 days of an election.[101] AB 730 defines "materially deceptive audio or visual media" as media involving a candidate that is intentionally manipulated and would reasonably confuse a person as to the authenticity of the media.[102] The law does not apply to satire or parody and allows fake video or audio ads as long as there is a disclosure on the video clarifying the video is manipulated.[103] AB 730 has drawn criticism for lacking First Amendment exemptions.[104] Because political speech has robust First Amendment protection, this law is likely going to be difficult to enforce.[105]

Other states are following suit. Maine, Maryland, and Washington are among those states that have proposed deepfake bills. [106] However, because of the difficulty of regulating speech, specifically political speech, it is unlikely that such bills would withstand First Amendment challenges, unless they carefully carve out First Amendment protections.[107] Political attack ads have existed for centuries, so the addition of deepfakes purporting to show candidates saying and doing things they never said or did would have to be significantly distinguished from other forms of political protected speech.

b. Defamation Actions

Deepfakes largely involve using another person's likeness without their consent, leading some to believe the remedy to combat fake speech

---

99. CAL. CIV. CODE § 1708.86 (2019).
100. *Id.*
101. CAL. ELEC. CODE § 20010 (2019).
102. *Id*.
103. *Id.*
104. *See* Evan Symon, *'Deepfake' Videos of Political Candidates in Ads Now Illegal In California,* CAL. GLOBE (Oct. 7, 2019, 8:17PM), https://californiaglobe.com/section-2/deepfake-videos-of-political-candidates-in-ads-now-illegal-in-california/ [https://perma.cc/D654-T7EW].
105. *See* Kari Paul, *California Makes 'Deepfake' Videos Illegal, But Law May Be Hard to Enforce*, GUARDIAN (Oct. 7, 2019), https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce [https://perma.cc/6ZK5-2HEF].
106. *See* Scott Thistle, *Maine Lawmakers Take Up Bill to Ban 'Deepfake' Political Ads*, PRESSHERALD (Jan. 29, 2020), https://www.pressherald.com/2020/01/29/maine-lawmakers-take-up-bill-to-ban-deepfake-political-ads/# [https://perma.cc/3LQG-BAEN] (the proposed Maine law would prohibit the publication and distribution of a deepfake video of a candidate within 60 days of an election. The political candidate targeted in the fake ad could seek redress through a court order to block the content and the opportunity to pursue civil action against the maker of the deepfake); *see also* Matthew Feeney, *Deepfake Laws Risk Creating More Problems Than They Solve*, CATO (Mar. 1, 2021) https://www.cato.org/sites/cato.org/files/2021-03/Paper-Deepfake-Laws-Risk-Creating-More-Problems-Than-They-Solve.pdf.
107. *See* Rumold, *supra* note 96.

found in deepfakes already exists in defamation law.[108] The problem with defamation suits for combatting deepfakes is that they require a higher standard for public officials to prove the falsity of a statement. As seen in *New York Times v. Sullivan*, the burden is on the public official to prove speech is false under the actual malice standard by clear and convincing evidence.[109] The defendant, on the other hand, need not show the speech is true.[110] Proving actual malice is in theory difficult because it requires showing that the defendant had actual knowledge that the speech was false or that the person acted in reckless disregard of the truth.[111]

Getting legal remedies for a deepfake action in general might be difficult. To succeed, the plaintiff would need to know the creator of the deepfake.[112] Lawsuits are also often costly and time-consuming.[113] In addition, not all deepfakes involve a specific individual, meaning there might not be standing to sue in some cases.[114] And then there is the difficulty of suing the platform hosting the video because of CDA § 230 protections.[115]

c. CDA Section 230 Protections[116]

> 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.[117]

In the 1997 Fourth Circuit case, *Zeran v. AOL*, the court held that liability upon notice has a chilling effect on the freedom of Internet speech.[118] Since 1997, Internet speech has skyrocketed. Today, online social media platforms would be extremely burdened if they were liable to be sued for every false speech represented or posted on their site. Similarly, if such platforms became aware of fake, or what some might deem harmful posts, it would not be incumbent upon them to take down the speech, because that would contradict the marketplace of ideas theory heralded by free speech enthusiasts and Internet users alike. However, this should not give social

---

108. *See* DAVID GREENE, WE DON'T NEED NEW LAWS FOR FAKED VIDEOS, WE ALREADY HAVE THEM (2018), https://www.eff.org/deeplinks/2018/02/we-dont-need-new-laws-faked-videos-we-already-have-them [https://perma.cc/7RCA-N7NN].

109. Bose Corp. v. Consumers Union of U.S., Inc., 466 U.S. 485, 511–12 (1984); *see generally Sullivan*, 376 U.S. 254 (1964).

110. *Sullivan*, 376 U.S. at 279.

111. *See* Greene, *supra* note 108.

112. *See generally* Chesney & Citron, *supra* note 7, at 1792.

113. *Id.*

114. *Id.*

115. *Id.* at 1796.

116. This Article refers to Section 230 as part of the CDA for ease of reference, but Section 230, per the FCC, is technically part of the Communications Act. *See* Thomas M. Johnson Jr., *The FCC's Authority to Interpret Section 230 of the Communications Act*, FCC (Oct. 21, 2020), https://www.fcc.gov/news-events/blog/2020/10/21/fccs-authority-interpret-section-230-communications-act [https://perma.cc/K674-PQVM].

117. 47 U.S.C. § 230(c)(1) (2018).

118. Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997).

media platforms the excuse to turn a blind eye to illegal activities occurring on their sites.[119]Although they currently have no legal obligation to monitor speech activities on their sites, society urges them to have an ethical duty to reward good behavior and encourage the free flow of ideas in a way that benefits others. Noting this, many social media companies have enacted their own Rules of Engagement or Community Standards and Polices that users must abide by if they wish to participate on those platforms. With this in mind, social media companies may not need legal repercussions to get them to act. Rather, moral and political pressures might be enough to incentivize social media companies to engage in a form of beneficial content moderation.[120]

B. What Social Media Companies are Doing About Deepfakes

In July 2019, Representative Adam Schiff (D-CA), head of the House Intelligence Committee, sent letters to social media companies asking them to describe their plans for combatting the spread of deepfakes on their sites, especially ahead of the 2020 presidential election and the growing threat of disinformation.[121] Schiff expressed (valid) concern for the proliferation of false information and misrepresentations to spread on social media sites, causing panic and distrust.[122]

Social media platforms, catalysts for wreaking havoc by spreading false information, should take steps to stop the spread of harmful, false information caused by manipulated media.[123] That includes adopting policies that: (1) define manipulated media such as deepfakes; (2) address criteria for take-down techniques; (3) comply with the First Amendment; and (4) identify the differences, if any, between political and commercial speech portrayed through manipulated media. Most of the policies currently in place fail to address at least one of these proposals.

119. *See* Chesney & Citron, *supra* note 7, at 1797.

120. *Id.* at 1795.

121. Press Release, Adam Schiff, Member, U.S. House of Representatives, Schiff Presses Facebook, Google and Twitter for Policies on Deepfakes Ahead of 2020 Election (July 15, 2019), https://schiff.house.gov/news/press-releases/schiff-presses-facebook-google-and-twitter-for-policies-on-deepfakes-ahead-of-2020-election [https://perma.cc/L7CQ-J7L9].

122. *See, e.g.*, Hugh Langley, *Rep. Adam Schiff Told Google and Twitter to Step Up Their Fight Against Coronavirus Misinformation with an Unexpected Message: Be More Like Facebook*, BUS. INSIDER (Apr. 30, 2020, 6:59PM), https://www.businessinsider.com/adam-schiff-tells-google-and-twitter-to-look-to-facebook-2020-4 [https://perma.cc/G7HU-C9BE].

123. *See, e.g.*, Jesselyn Cook, *Online Anti-Vax Communities Have Become A Pipeline for QAnon Radicalization*, HUFFINGTON POST (Nov. 28, 2020), https://www.huffpost.com/entry/qanon-anti-vax-coronavirus_n_5fbeb0c0c5b61d04bfa6921a [https://perma.cc/N22C-LL7B].

1. Facebook

Facebook claims its key to tackling harmful deepfakes is "collaboration."[124] On January 6, 2020, Monika Bickert, Facebook's Vice President for Global Policy Management, released Facebook's strategy for combatting deepfakes and other forms of manipulated media.[125] The strategy involved working with academia, government, and industry to develop solutions, as well as implementing investigations of AI-generated content.[126] Facebook, along with Amazon Web Services, Microsoft and other partners, launched the Deepfake Detection Challenge (DFDC) in September 2019.[127] The goal of the DFDC, is to bring academics and researchers together to find innovative ways to detect deepfakes.[128] Facebook also partnered with Reuters to help journalists identify deepfakes in a free online course.[129]

Facebook also has a policy in its Community Standards specifically related to manipulated media.[130] That policy states that Facebook will remove deceptive manipulated media if it has been edited or synthesized in ways such that an average person would be misled as to the authenticity of the media.[131] The policy also carves out an exception for satire or parody media.[132] Facebook's manipulated media policy has been criticized both as overbroad and too narrow.[133] As Whitney Phillips from *WIRED* put it, the policy is "best described as a slice of Swiss cheese that's mostly holes."[134]

In an attempt to avoid overregulation while still protecting free speech, Facebook allows users who have content taken down for violating Facebook's policies to challenge their takedown with an independent third-party fact checker.[135] Facebook also said it will not invariably take down manipulated media that violates its policies and will instead label the affected media.[136] Facebook argues this labelling process will help educate people as to what "fake news" is, but it is unlikely that simple labelling measures will keep

124. *See* Monika Bickert, *Enforcing Against Manipulated Media*, FACEBOOK (Jan. 6, 2020), https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/ [https://perma.cc/ZV2U-29CT].

125. *Id.*

126. *Id.*

127. *Id.*

128. *See Description of Deepfake Detection Challenge*, KAGGLE, https://www.kaggle.com/c/deepfake-detection-challenge/overview/description (last visited Feb. 15, 2021) [https://perma.cc/4C7M-XXZM?type=image].

129. *See* Reuters Staff, *Reuters Partners with Facebook Journalism Project to Help Newsrooms Around the World Spot Deepfakes and Manipulated Media*, REUTERS (Dec. 17, 2017), https://www.reuters.com/manipulatedmedia/en/ [https://perma.cc/6NU3-5WS6].

130. *Facebook Community Standards, "Manipulated Media"*, FACEBOOK (2020), https://www.facebook.com/communitystandards/manipulated_media [https://perma.cc/RWB2-QDA6].

131. *Id.*

132. *Id.*

133. *See* Whitney Phillips, *The Internet Is a Toxic Hellscape—But We Can Fix It,* WIRED, (Feb. 3, 2020), https://www.wired.com/story/the-internet-is-a-toxic-hellscape-but-we-can-fix-it/ [https://perma.cc/6DJC-39S5].

134. *Id.*

135. Bickert, *supra* note 124.

136. *Id.*

people from seeing and believing the media as true.[137] As we saw with the illusory truth effect, the opposite is in fact true.[138]

2. Twitter

About a month after Facebook announced its deepfake policy, on February 4, 2020, Twitter announced a new policy related to "synthetic and manipulated media."[139] Twitter's policy was user-focused. For example, the company posted a survey in the fall of 2019 soliciting feedback on its proposed policy from Twitter users who commented with the hashtag #TwitterPolicyFeedback.[140] After receiving around 6,500 responses globally, Twitter posted its findings and crafted its new rule.[141] The new rule states: "You may not deceptively share synthetic or manipulated media that are likely to cause harm. In addition, we may label Tweets containing synthetic and manipulated media to help people understand their authenticity and to provide additional context."[142]

Twitter's approach includes labeling deceptively altered or fabricated content, only removing the content if it impacts public safety or is likely to cause serious harm.[143]

Is the content significantly and deceptively altered or fabricated?	Is the content shared in a deceptive manner?	Is the content likely to impact public safety or cause serious harm?	
✓	✗	✗	Content **may** be labeled.
✗	✓	✗	Content **may** be labeled.
✓	✗	✓	Content is **likely** to be labeled, or **may** be removed.*
✓	✓	✗	Content is **likely** to be labeled.
✓	✓	✓	Content is **likely** to be removed.

Twitter's policy seems to apply to shallowfakes as well as deepfakes, stating that the Twitter team is likely to act on significant forms of alteration

137. *See* Donie O'Sullivan & Marshall Cohen, *Facebook Begins Labeling, but Not Fact-Checking, Posts From Trump And Biden*, CNN BUS. (July 21, 2020), https://www.cnn.com/2020/07/21/tech/facebook-label-trump-biden/index.html [https://perma.cc/29NW-EZMJ].

138. *See* Franks & Waldman, *supra* note 9, at 894–95.

139. *See* Yoel Roth & Ashita Achuthan, *Building Rules in Public: Our Approach to Synthetic & Manipulated Media*, TWITTER BLOG (Feb. 4, 2020), https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html [https://perma.cc/K6EW-XYBB].

140. *Id.*

141. *Id.*

142. *General Guidelines and Policies: Synthetic and Manipulated Media Policy*, TWITTER HELP CTR., https://help.twitter.com/en/rules-and-policies/manipulated-media (last visited May 4, 2020) [https://perma.cc/3G7C-UJZK].

143. *Id.*

such as audio or video content doctored to change its meaning.[144] This gives Twitter discretion to determine if a video is manipulated in such a way that is inauthentic to merit labels or removal from its site. Twitter maintains it will be an impartial editor, only labeling or removing videos identified by its technology or reported by a third party.[145] Some of the serious harms that could be cause for removal include threats to the privacy or ability of a person or group to freely express themselves or participate in civic events.[146]

Twitter's first case in applying its new policy encountered problems. White House social media director for former President Donald Trump, Dan Scavino, tweeted a manipulated video of (then) former Vice President Joe Biden appearing to endorse Trump for reelection in 2020, which Trump also retweeted.[147] Twitter labeled the tweet as "manipulated media," but the tag only appeared if the tweet showed up on someone's timeline and was not visible to users who tried to search for the video or physically clicked on the video.[148]

Since then, Twitter has been on a labeling frenzy,[149] going so far as to kick Trump off the site in 2021 following an attack by his supporters on the U.S. Capitol.[150] Twitter claimed it was permanently suspending Trump's account due to risk of "further incitement of violence."[151] Prior to the ban, Twitter had already started to label a slew of Trump's tweets, hiding the tweets, and limiting replies, based on Trump's false claims that he won the election and allegations of voter fraud.[152] Twitter's labeling stated: "Some or all of the content shared in this Tweet is disputed and might be misleading about an election or other civic process."[153]

3. Google/YouTube

YouTube, owned by Google, reiterated its stance on election-related content in an official YouTube blog on February 3, 2020.[154] YouTube's

144. *Id.*
145. *See id.*
146. *Id.*
147. *See* Ivan Metha, *Trump's Retweet with Doctored Biden Video Earns Twitter's First 'Manipulated Media' Label*, THE NEXT WEB (March 9, 2020), https://thenextweb.com/twitter/2020/03/09/trumps-tweet-with-doctored-biden-video-earns-twitters-first-manipulated-media-label/ [https://perma.cc/9RVZ-RWQ9].
148. *Id.*
149. *See, e.g.*, Twitter Safety, *Updates to Our Work on COVID-19 Vaccine Misinformation*, TWITTER BLOG (Mar. 1, 2021), https://blog.twitter.com/en_us/topics/company/2021/updates-to-our-work-on-covid-19-vaccine-misinformation.html [https://perma.cc/7UCK-N7X8].
150. Twitter Inc., *Permanent Suspension of @realDonaldTrump*, TWITTER BLOG (Jan. 8, 2021), https://blog.twitter.com/en_us/topics/company/2020/suspension.html [https://perma.cc/J9AX-3BQH].
151. *Id.*
152. *Id.*
153. *Id.*
154. *See* Leslie Miller, *How YouTube Supports Elections*, YOUTUBE OFF. BLOG (Feb. 3, 2020), https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html [https://perma.cc/9NTF-KR5Q].

deceptive practices policies state that: "[C]ontent that has been technically manipulated or doctored in a way that misleads users (beyond clips taken out of context) and may pose a serious risk of egregious harm" will be removed.[155] YouTube further states it will remove content that attempts to mislead people about the voting process or any other false information relating to elections.[156]

YouTube will not only remove false content if it fits the criteria, but it will also terminate channels that "[a]ttempt to impersonate another person or channel, misrepresent their country of origin, or conceal their association with a government actor."[157]

In 2018, YouTube created an Intelligence Desk to help review technically-manipulated content and take proactive approaches to mitigate the spread of the content.[158] YouTube also changed its recommendations system to prevent people from viewing misinformation on its site.[159] The Intelligence Desk and recommendation system are attempts by YouTube to be proactive and get ahead of videos before they become viral, when they can do the most damage.[160] To achieve this, YouTube relies on Google data, user reports, social media trends, and third-party consultants.[161] YouTube later added human vetting and content moderators.[162]

Google has tried to warn about the dangers surrounding deepfakes by releasing an open-source database containing 3,000 manipulated videos.[163] Google's hope was that researchers would start to develop deepfake detection tools.[164]

Also noteworthy is that YouTube found that it was within its policies to take down a shallowfake video of Nancy Pelosi appearing to slur her words during a speech.[165] Facebook, on the other hand, kept the video up.[166]

---

155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.*
159. Miller, *supra* note 154.
160. *See id.*
161. Alex Kantrowitz, *YouTube Is Assembling New Teams to Spot Inappropriate Content Early*, BUZZFEED (Jan 19, 2018), https://www.buzzfeednews.com/article/alexkantrowitz/youtube-intelligence-desk-will-spot-inappropriate-content [https://perma.cc/6MAH-6BQL].
162. *Id.*
163. Karen Hao, *Google Has Released A Giant Database of Deepfakes to Help Fight Deepfakes*, MIT TECH. REV. (Sept. 25, 2019), https://www.technologyreview.com/f/614426/google-has-released-a-giant-database-of-deepfakes-to-help-fight-deepfakes/ [https://perma.cc/ME9Z-MUWH]; *see also* Nick Dufour & Andrew Gully, *Contributing to Deepfake Detection Research*, GOOGLE AI BLOG (Sept. 24, 2019), https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html[https://perma.cc/7JCW-5CTK].
164. *See* Dufour & Gully, *supra* note 163.
165. *See* Mervosh, *supra* note 10.
166. *Id.*

IV. MITIGATING THE DEEPFAKE THREAT

> "[W]e must reject a culture in which facts themselves are manipulated and even manufactured."
>
> – President Joe Biden[167]

Trusting the authority of public officials and the government generally will play a huge role in helping to combat the threat of deepfakes. Instead of fostering distrust in the media, the Biden Administration seeks to bring truth back to light. But it cannot do so alone. Social media companies have taken steps in the right direction by raising awareness of deepfakes by creating policies banning certain kinds of manipulated media from their sites.[168] However, because social media companies are largely self-regulating, their policies differ in how deepfakes are defined, and they fail to adequately protect free speech rights.[169] To provide a stronger, more united front on behalf of social media companies, proposals range from amending CDA Section 230 to investing in various technological solutions. However, perhaps the biggest challenge social media companies face in regulating deepfakes and other fake news is moderating content in line with free speech. If social media companies have too much power to regulate what is being said on their platforms, this could seriously diminish individuals' freedom of expression.

A. Amending CDA Section 230

While some have criticized amending Section 230, believing that it is vital to the Internet's existence, Danielle Citron and Benjamin Wittes are convinced that an amendment, while retaining much of platforms' liability, is viable.[170] Citron's and Wittes' proposed amendment is more of a compromise, requiring companies to use reasonable content moderation practices to earn the immunity provided by Section 230.[171] It is not impossible to amend Section 230, and the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), which allowed greater regulation of sex trafficking content on the Internet, is proof of that.[172]

Section 230 is outdated. One of the biggest selling points of Section 230 is that it lets platforms off the hook from sifting through massive amounts of

---

167. Joseph R. Biden, Jr., President, United States of American, Inaugural Address (Jan. 20, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/01/20/inaugural-address-by-president-joseph-r-biden-jr/ [https://perma.cc/6MTY-8FUE].

168. *See supra* Section II.B.

169. *Id.*

170. *See* Chesney & Citron, *supra* note 7, at 1798–99.

171. *See* Danielle Citron & Quinta Jurecic, *Platform Justice:Content Moderation at an Inflection Point*, Hoover Inst. Essay 2 (2018), https://www.scribd.com/document/387911222/Platform-Justice-Content-Moderation-at-an-Inflection-Point#download&from_embed [https://perma.cc/8G7K-Z7KU].

172. *See* Chesney & Citron, *supra* note 7, at 1798–99.

data that would otherwise be deemed impossible to monitor.[173] However, technology, like the Internet, has evolved since then. Many sites now have compliance monitors built in, through machine learning and AI, that allows social media platforms to track and take down harmful content, such as child pornography and IP violations.[174] This approach can be applied to deepfakes as well. Social media companies already have the technology to combat the spread of harmful information on their sites, now they just need a legislative push.

With the recognized harms of deepfakes, Section 230 should and can be amended to prevent harmful disinformation from rampantly spreading on social media sites. It has been done before, and it can be done again.[175] Any proposed amendment would have to ensure social media platforms are not engaging in over-regulation and would consider the First Amendment.[176] Because false speech is not unconstitutional, an amendment to Section 230 would have to specifically account for false speech that harms. In defining speech that harms, legislators should look towards defamation actions and other appropriation torts. Congress can incentivize platforms to take down such false, harmful speech, by still granting overreaching immunity for most content published on social media sites due to the broad scope of Section 230. That is the beauty of amending, rather than dismantling and getting rid of Section 230 altogether.

B. Stronger Deepfake Legislation

Instead of placing the burden on social media platforms to monitor and remove deepfakes or face liability under a newly amended Section 230, another approach Congress could take would be to enact a federal law could successfully regulate deepfakes by clearly defining them as manipulated media. This will enable social media platforms to adapt their policies to that definition while alleviating First Amendment concerns. Most of the laws currently surrounding deepfakes in the U.S. are more research-focused[177] or related more directly to pornographic deepfakes.[178] Deepfake laws that purport to ban deepfakes for deceptive speech are largely nonexistent, likely due to concerns that such laws impermissibly block free speech.

---

173. *See supra* Section II.A.2.c.

174. *See* Tim Hwang, *Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment Interventions,* Stanford PACS 32, https://pacscenter.stanford.edu/dealing-with-disinformation-evaluating-the-case-for-cda-230-amendment-interventions/ (last visited Mar. 31, 2021) [https://perma.cc/5TL5-J4S8].

175. *See* Chesney & Citron, *supra* note 7, at 1798–99.

176. *See id.*

177. *See, e.g.*, Matthew Ferraro, *Congress's Deepening Interest in Deepfakes*, THE HILL (Dec. 29, 2020, 12:00PM), https://thehill.com/opinion/cybersecurity/531911-congresss-deepening-interest-in-deepfakes [https://perma.cc/W9R6-3ALF] (the Identifying Outputs of Generative Adversarial Networks (IOGAN) Act requires the Director of the National Science Foundation to support research and the National Institute of Standards and Technology to develop standards for examining deepfakes).

178. *See id.* (Virginia criminalized the distribution of nonconsensual deepfake pornography in 2019, establishing a maximum one year in jail and $2,500 fine).

On December 20, 2019, the National Defense Authorization Act (NDAA) for the 2020 fiscal year weighed in on the deepfake debate.[179] The NDAA requires the Director of National Intelligence (DNI) to submit a comprehensive report on the foreign weaponization of deepfakes to Congressional Intelligence Committees.[180] The DNI must also notify Congress of foreign deepfake disinformation activities specifically targeting the U.S. election process.[181] The DNI is also authorized to award up to $5 million to encourage development of deepfake detection technology.[182]

Deepfakes are not just a problem in the U.S., and other countries have adopted their own legislation to tackle the mounting challenges deepfakes present. Deepfakes have been prevalent in China, for example, a country that might consume as much information as the U.S. China recently banned online video and audio providers from using deepfakes, citing concerns over the growing disinformation war occurring globally.[183] The ban further extends to both providers and users of online video news and audio services from using or distributing deepfakes or fake news.[184] Providers and users of online video news and audio information services must label any content that involves new technologies such as deep learning.[185] Content providers must also use technology to detect manufactured or manipulated content in violation of the regulation.[186] China's ban encompasses deepfakes used in the political sense and any other area deepfakes might emerge, such as virtual reality.[187] China's deepfake ban appears to ban deepfakes writ large, even creative or artistic ones, and includes consequences for refusal to comply.

While the U.S. would not likely enact laws similar to those of China, it is helpful to see another country's approach to the rising problem of deepfakes. The U.S. is presented with its own challenges in combatting deepfakes, but the legislation currently enacted is a step in the right direction. A stronger approach will be needed in the coming years, but scientists and technologists are trying to come up with their own solution in the meantime.

C. Fighting Technology with Technology

Algorithms and artificial intelligence might seem like an attractive solution to moderating content online at first blush, but there is a plethora of issues that arise when AI is involved.[188] Unfortunately, we are not at the point

179. *Id.*
180. *Id.*
181. *Id.*
182. Ferraro, *supra* note 177.
183. Meng Jing, *China Issues New Rules to Clamp Down on Deepfake Technologies Used to Create and Broadcast Fake News,* S. China Morning Post (Nov. 29, 2019), https://www.scmp.com/tech/apps-social/article/3039978/china-issues-new-rules-clamp-down-deepfake-technologies-used [https://perma.cc/77ZC-TMWR] (providing that China has also voiced concerns over deepfakes from creation of the face-swap app Zao).
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. *See* Chesney & Citron, *supra* note 7, at 1787.

yet where AI returns highly accurate takedown responses.[189] In the event that AI makes a mistake, it runs the risk of violating free speech by filtering out protected speech and media.

Deepfake scanners and other video editing software might be a more attractive approach.[190] Researchers are starting to create tools that attempt to dissect deepfake videos and distinguish the real from the fake. For example, Binghamton University in New York has teamed up with Intel to create "FakeCatcher," a tool that reveals deepfakes by discovering subtle differences in skin color caused by the human heartbeat.[191] Social media companies should implement such deepfake detection software on their sites. Users should also be able to challenge the software's finding of a deepfake if they believe it was in error.

Another moderating option is blockchain, a popular resource for authenticating business and financial records. Blockchain can be used for authenticating videos.[192] Using blockchain technology, and when a video is uploaded to a site, the metadata from the video would be captured (including the upload time, location, and creator/uploader's ID), which would create a transparent and traceable route proving the authenticity of the video.[193] Any fake, copy, or change to the video would be noted through the blockchain by that video's own unique metadata.[194] The technology is out there. Social media companies just have to engage with the researchers developing it to combat the manipulative media together.

D. Knowledge is Power

While we might not be able to stop the oncoming threat of deepfakes, we can at least start implementing the tools to help increase awareness of deepfakes. The problem with deepfakes is that they reflect a bigger problem within society itself, stemming from a general lack of trust in public officials and our basic democratic institutions.[195] But because we are already faced with similar problems like fake news, deepfakes might be the wake-up call we need to help fix disinformation in our society.[196]

Deepfakes are gaining prominence as creative, innovative tools, but not all consumers know about them. If more people become aware of the

189. *See* Mark Scott & Laura Kayali, *What Happened When Humans Stopped Managing Social Media Content*, POLITICO (Oct. 21, 2020), https://www.politico.eu/article/facebook-content-moderation-automation/ [https://perma.cc/UNR6-YUY9].

190. *See, e.g.*, *About Us*, DEEPWARE, https://deepware.ai/about/ (last visited Mar. 31, 2021) [https://perma.cc/Q27P-PBJ6].

191. *See* Chris Kocher, *Best Way to Detect 'Deepfake' Videos? Check for the Pulse*, BINGHAMTON UNIV. (Oct. 21, 2020), https://www.binghamton.edu/news/story/2713/best-way-to-detect-deepfake-videos-check-for-the-pulse [https://perma.cc/9HKW-X7BN].

192. *See* Jason Tashea, *Some States Are Allowing People and Companies to Use Blockchain to Authenticate Documents*, ABA J. (Sept. 1, 2019), https://www.abajournal.com/magazine/article/best-evidence [https://perma.cc/GF4L-AHTR].

193. *Id.*

194. *Id.*

195. *See* Silbey & Hartzog, *supra* note 6, at 964.

196. *Id.*

existence of deepfakes, they will be less likely to be fooled by one. Learning how to evaluate facts, test systems, and challenge accounts by examining alternative perspectives is a way to turn people into deep thinkers, and in turn deep thinkers will not be so easily fooled by deepfakes.

V. CONCLUSION

Deepfakes arguably have creative expressive values, and if we learn how to filter out the harmful deepfakes from the harmless, society will benefit. Current legal remedies are inadequate because of the timing and nature of deepfakes. Deepfakes are most damaging when people are exposed to them and believe their lies. However, an outright ban on deepfakes is impossible in light of the First Amendment. But amid all of these challenges, social media companies are working with academics, the government, and other leaders in the technology industry to create adoptable solutions, and they should continue to do so. Other remedies, such as amending Section 230 or state laws are likewise feasible. Although the perfect solution is not here yet, it is in sight. I will believe it when I see it.

Amazon Ring Master of the Surveillance Circus

Christopher Frascella*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School. Thank you to Matthew Guariglia, Nat Meysenburg, and Prof. Andrew Ferguson for taking the time to offer seasoned perspective on the lack of oversight of surveillance technologies. Major thanks to my colleagues in the Federal Communications Law Journal, in particular for their promptness and patience with incorporating news updates as practices evolved, but also more generally for their collegial support and diligent attention throughout the review process.

I. INTRODUCTION

In an era when many call for defunding police departments and when racial inequities in policing and surveillance are at the fore, it is important for local law enforcement to cultivate trust with the people they protect by improving the transparency and accountability of their surveillance practices. Instead, hundreds of departments are operating like marketing partners, and in at least one instance facilitating and subsidizing the sale of one company's surveillance tech products to consumers.

This Note will focus on police departments' promotion of Amazon Ring doorbell cameras—surveillance tech that, by design, enables police to request access to footage from consumers before requesting a warrant from courts—and of the related Neighbors app, which combines aspects of a neighborhood watch program and an online message board, and allows for easy sharing of Ring footage.[1] Police departments have received compensation from Amazon for their efforts in the form of discounted Amazon Ring units proportionate to the number of local downloads of Amazon's Neighbors app, promoted Amazon products openly over their official social media accounts, and signed agreements giving Amazon oversight over police departments' public communications about Amazon's products.[2]

Surveillance technology companies should be held to the same standard of transparency and truthfulness in advertising as other industries. Similarly, police departments should be treated as any other marketing organization when acting as influencers. Consumer protection law can be used to compel disclosure of these relationships, and to create the resistance that should exist when police departments become complicit in peddling a nationwide surveillance network of questionable efficacy and demonstrated capacity to exacerbate existing social inequities.

Communities can now aggregate information and act with greater speed and ease than ever before—including facilitating the deployment of law enforcement resources. By virtue of American privacy law's slow development and Amazon's clever strategy in incentivizing law enforcement to market its products, Amazon Ring created a network of doorbell surveillance cameras potentially accessible to police departments by a single click rather than by a warrant. While this is a threat to the privacy of any individual who happens to be "in frame" of one or more doorbell cameras, partnerships like these pose additional risk to communities of color due to the social, technological, and institutionalized racial biases at play. This systemic threat is growing at breakneck speed, in large part because Amazon has deputized local police as a partner marketing channel.

Consumer protection law may provide the only immediate friction to slow this otherwise rapid and geographically widespread deterioration of civil

1. *See The Ring Story*, RING, https://ring.com/about (last visited Jan. 27, 2021) [https://perma.cc/B4H2-M9MA].

2. *Infra* Section II.

liberties by forcing transparency regarding the nature of the relationships between local police departments and Amazon Ring. This Note begins in Section II with an overview of relevant Amazon products, Ring and Neighbors, and an overview of why without enacted federal privacy legislation, consumer protection law may be the only remedy immediately available. Section III provides context as to the growth of surveillance technology and the relationship between surveillance tech vendors and police departments. A more detailed explanation follows in Section IV of why traditional legal remedies do not apply to situations like that of Amazon Ring and why that legal impotence is unlikely to change soon. This Note concludes with a brief analysis of (1) state Unfair and Deceptive Acts or Practices (UDAP) laws and (2) the FTC's Endorsement Guides, explaining how they serve as the best means for immediate redress.

II. SURVEILLANCE, STARTUP CULTURE, AND SOCIETY

A. Ring is Intuitively Troubling, But Permissible

Despite the threats to the privacy of consumers and non-consumers, there are no legal barriers to use of the Ring product. Homeowners choose to purchase a Ring doorbell camera unit, sign a contract giving Amazon ownership of the data, install the Ring unit appropriately (so that it captures video of their doorstep), and provide the required consent (often by clicking a button in an automated email)[3] for the police to access the Ring video feed.

Because of this structure, Ring customers are not compelled to do anything with their property. Amazon is not responsible for customer misuse. Police cannot access the video without either the property owner's permission or a warrant.[4] And passers-by captured on video have no expectation of privacy while walking in public view.

Moreover, Amazon ceased two of its most questionable practices: providing police departments with (1) heat maps of Ring coverage and (2) reports of property owners who deny their local department's requests to view their Ring data. As of 2020, Amazon allows users to preemptively opt out of requests from police to the user, and as of 2021, offers opt-in encryption to

3. Drew Harwell (@drewharwell), TWITTER (Aug. 28, 2019, 1:55 PM), https://twitter.com/drewharwell/status/1166771255724453890.

4. *See Ring Law Enforcement Guidelines*, RING, https://support.ring.com/hc/en-us/articles/360001318523-Ring-Law-Enforcement-Guidelines (last visited Feb. 2, 2021) [https://perma.cc/3SWD-BL8B] ("Ring distinguishes between content and non-content information. We may produce non-content information in response to a valid subpoena, search warrant, or other court order. Content information will only be disclosed in response to a valid search warrant or with the consent of the account owner."); *see generally Law Enforcement Information Requests in 2020*, RING, (last visited April 19, 2021) https://blog.ring.com/2021/01/20/law-enforcement-information-requests-in-2020/ (providing a report on the company's responses to law enforcement requests during 2020).

ensure Ring data is not visible without deliberate action from the user.[5] Arguably, Ring is exhibiting the 21st century "move fast and break things" startup culture in rolling out a new product.[6]

As for other obvious stakeholders, property owners have the right to protect their property interests, and police are within their rights to fulfill their public safety mandate using the most efficient means available, assuming those means are legal.

B. Today's Privacy Harms, Made Worse Tomorrow

Consumers who purchase Ring equipment and do not opt-in to encryption are subject to Amazon harvesting and using their data. However, arguably the greater risk here is to those who do not purchase the equipment but are still surveilled. As the use of Ring grows, communities will be subject to constant surveillance, with questionable accuracy and limited accountability.[7] This becomes truly chilling when combined with experimental technologies already gaining traction in the marketplace, such as facial recognition (FR), which promises to create a 21st century corporate panopticon.[8] Admittedly, Amazon has implemented a self-imposed

5. Ring, *The New Control Center Empowers Ring Customers to Manage Important Privacy and Security Settings*, RING BLOG (Jan. 30, 2020), https://blog.ring.com/2020/01/30/the-new-control-center-empowers-ring-customers-to-manage-important-privacy-and-security-settings/ [https://perma.cc/YJ7S-T3MT]; Ring, *Understanding Video End-to-End Encryption (E2EE),* RING SUPPORT, https://support.ring.com/hc/en-us/articles/360054941511-Understanding-Video-End-to-End-Encryption-E2EE- (last accessed Feb. 20, 2021).

6. *See generally* Hemant Taneja, *The Era of "Move Fast and Break Things" is Over*, HARV. BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over [https://perma.cc/3SAW-T249].

7. Advocates concerned about the military-industrial complex-esque expansion of police power via deep discount Big Tech surveillance would certainly prefer to win this kind of fight on privacy grounds. However, the unfortunate fact is that the vast majority of Americans are without the legal authority to prevail in defending their privacy against corporations collecting and/or selling their behavior (and now their neighbors' behavior) as a digital commodity. Europe recently revoked the United States' special status for data transfers due to the extent of disproportionately extensive government surveillance and the lack of remedy for those subject to it. Court of Justice of the European Union, *The Court of Justice Invalidates Decision 2016/1250 On The Adequacy Of The Protection Provided By The EU-US Data Protection Shield*, Press Release No 91/20, CURIA (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf [https://perma.cc/54MD-9T5Q]. Understandably, this massive collection of data by law enforcement agencies has implications for those concerned with criminal justice reform. *See, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2019).

8. "Through this seemingly constant surveillance, Bentham believed all groups of society could be altered." *Ethics Explainer: The Panopticon*, ETHICS CTR. (Jul. 18, 2017), https://ethics.org.au/ethics-explainer-panopticon-what-is-the-panopticon-effect/.

moratorium on selling facial recognition technology to law enforcement.[9] However, this does not address the underlying surveillance technology infrastructure problem, especially if in selling these products to consumers, Amazon facilitates sharing that data with police departments, as part of the product's design.[10] These in-roads to a surveillance state are forming faster than the public's ability to understand and respond to the threats they pose; this is in large part because police often endorse solutions, such as Ring and the related Neighbors app, from the Amazon surveillance suite.[11]

Discussion of the Neighbors app below illustrates how this kind of surveillance can harm the fabric of a community, often with racist subtext. One Amazon worker argued that Ring is "not compatible with a free society."[12] An Amazon software engineer offered: "The privacy issues are not fixable with regulation, and there is no balance that can be struck. . . . Ring should be shut down immediately and not brought back."[13]

In terms of criminal justice implications, Supreme Court case law suggests that errors made as a result of imperfect database-driven technologies, which can easily result in wrongful identifications (perhaps even of members of Congress[14]), could be excused by the "good-faith" rule,[15] meaning American citizens have no reasonable expectation of accountability

---

9. Isobel Asher Hamilton, *Outrage Over Police Brutality Has Finally Convinced Amazon, Microsoft, and IBM to Rule Out Selling Facial Recognition Tech to Law Enforcement. Here's What's Going on*, BUS. INSIDER (June 13, 2020), https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6?op=1 [https://perma.cc/F65P-2RU5].

10. Namely, it does not preclude further development of the infrastructure upon which FR can be readily deployed once companies' moratoria end. *See* Caroline Haskins, *Amazon, IBM, And Microsoft Won't Say Which Police Departments Used Their Facial Recognition Technology*, BUZZFEED NEWS (June 12, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/amazon-ibm-and-microsoft-wont-say-which-police-departments [https://perma.cc/8V2X-E3A3].

11. *See generally Neighbors by Ring*, RING, https://ring.com/neighbors (last visited Oct. 21, 2020) [https://perma.cc/BP63-LBUY]. Neighbors is a social media platform that combines aspects of neighborhood watch and a community bulletin board. Another example of this kind of product is Nextdoor. Chris Taylor, *Nextdoor Is Next: Why the Social Network of Systemic Racism Is Ripe for Change*, MASHABLE (June 11, 2020), https://mashable.com/article/nextdoor-racism/ [https://perma.cc/Q336-GTMB]. Amazon's suite of tools includes the controversial Sidewalk project as well. Ry Crist, *Amazon Sidewalk Will Create Entire Smart Neighborhoods. Here's What You Should Know*, CNET (Oct. 7, 2020), https://www.cnet.com/how-to/amazon-sidewalk-will-create-entire-smart-neighborhoods-faq-ble-900-mhz/ [https://perma.cc/H7XU-FDBK].

12. Jay Greene, *Amazon Employees Launch Mass Defiance of Company Communications Policy in Support of Colleagues*, WASH. POST (Jan. 27, 2020), https://www.washingtonpost.com/technology/2020/01/26/amazon-employees-plan-mass-defiance-company-communications-policy-support-colleagues/ [https://perma.cc/N8DY-EU8X].

13. *Id.*

14. *See* Russell Brandom, *Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots*, VERGE (Jul. 26, 2018) https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

15. *See* Herring v. United States, 555 U.S. 135, 142–44 (2009) (finding negligently maintained database did not amount to systemic error).

for police or for vendors of hastily deployed, FR-amplified surveillance tech, except perhaps in the most egregious of circumstances. And we can expect such errors will occur, indeed, some already have.[16] A recent study by the National Institute of Standards and Technology (NIST) documented the potential extent of race-based disparities in the accuracy of the technology: Asian and African American people were up to 100 times more likely to be misidentified by this technology than white men, with Native American subjects experiencing the highest rate of false positives.[17]

The technological infrastructure is already in place. Amazon has attempted to sell its own FR product called Rekognition [18] to police departments[19] and already filed a patent to use FR technology in conjunction with Ring.[20] As of late 2019, there were more than 7 million downloads of the companion app, Neighbors.[21] Globally, more than 10 million Ring units have been installed.[22] And by the end of 2020, forty-eight states had at least one police or fire department participating in the Ring program, with local

16. Although not a result of Amazon Ring, there are already three documented cases of false arrests caused by improper use of FR technology. *See, e.g.*, Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/3JZX-DFE4]; Kris Holt, *Facial Recognition Linked to A Second Wrongful Arrest by Detroit Police*, ENGADGET (July 10, 2020), https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html [https://perma.cc/KXT3-5BEX]; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020, updated Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

17. Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ (Amazon opted not to participate in NIST's study, though 99 other companies, academic institutions, and developers did) [https://perma.cc/JQW4-RV25].

18. *See geneally What Is Amazon Rekognition?*, AMAZON WEB SERVS., https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html (last visited Apr. 14, 2020) [https://perma.cc/YX9Y-XZ47].

19. An Amazon Employee, *I'm an Amazon Employee. My Company Shouldn't Sell Facial Recognition Tech to Police*, MEDIUM (Oct. 16, 2018), https://medium.com/@amazon_employee/im-an-amazon-employee-my-company-shouldn-t-sell-facial-recognition-tech-to-police-36b5fde934ac [https://perma.cc/VRV2-ZWBX].

20. U.S. Patent Application No. US 2018/0341835 A1 (filed Nov. 29, 2018) https://www.aclunc.org/docs/Amazon_Patent.pdf (last accessed Apr. 14, 2020) [https://perma.cc/C5N3-FSGK]. However, Amazon announced an undefined "moratorium" on law enforcement use of Amazon's facial recognition technology until June 2021. Alfred Ng, *Amazon Owes Answers On Facial Recognition Moratorium, Lawmaker Says*, CNET (June 17, 2020), https://www.cnet.com/news/amazon-owes-answers-on-facial-recognition-moratorium-lawmaker-says/ [https://perma.cc/CH4Y-SVNA].

21. Sarah Perez, *Amazon's Ring Partners With National Center for Missing & Exploited Children to Put Missing Posters in Neighbors App*, TECHCRUNCH (Dec. 19, 2019), https://techcrunch.com/2019/12/19/amazons-ring-partners-with-national-center-for-missing-exploited-children-to-put-missing-posters-in-neighbors-app/ [https://perma.cc/LDF2-EVCC].

22. *Id.*

law enforcement agencies in at least two states piloting programs to integrate Ring footage into their Real Time Crime Centers.[23]

C. A Solution to Protect Consumers and Non-Consumers

There have been several local bans[24] and attempts at federal legislation[25] to address privacy concerns of facial recognition specifically. But national security expert Bruce Schneier aptly argues that focusing on facial recognition misses the bigger point:

> A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible.[26]

Schneier goes on to argue for consumer protection-style solutions, including regulation of data brokers and additional consumer education and debate: "We need to have a serious conversation about all the technologies of identification, correlation and discrimination, and decide how much we as a

---

23. Kim Lyons, *Amazon's Ring Now Reportedly Partners with More Than 2,000 US Police and Fire Departments*, VERGE (Jan. 31, 2021), https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras [https://perma.cc/4WEH-S3ZB] (noting participating police and fire departments rose from 40 in 2018 to 2,014 in 2020); Matthew Guariglia, *Police in Mississippi to Pilot a Program to Live-Stream Amazon Ring Cameras*, MOZILLA FOUND. (Nov. 19, 2020), https://foundation.mozilla.org/en/blog/police-mississippi-pilot-program-live-stream-amazon-ring-cameras/ [https://perma.cc/UXD8-ZBME] (including Amazon's response, distancing itself from Jackson program); *see Surveillance Compounded: Real-Time Crime Centers in the U.S.*, ATLAS SURVEILLANCE, https://atlasofsurveillance.org/real-time-crime-centers (last visited Nov. 21, 2020) (noting that Leon County, FL implemented a similar program integrating Ring data into its Real Time Crime Centers) [https://perma.cc/7M25-JKCT].

24. *San Francisco Bans Facial Recognition*, EPIC (May 15, 2019), https://epic.org/2019/05/san-francisco-bans-facial-reco.html [https://perma.cc/4H82-MU7Q]; *e.g.*, *Ban Facial Recognition*, https://www.banfacialrecognition.com/map/ (last visited Oct. 21, 2020) (showing restrictions in California, Massachusetts, Mississippi, Maine, and Oregon via an interactive map) [https://perma.cc/E2P8-QNMY]; Eric Einhorn, *A Fight Over Facial Recognition Is Dividing Detroit - With High Stakes for Police and Privacy*, NBC NEWS (Aug. 22, 2019), https://www.nbcnews.com/news/us-news/fight-over-facial-recognition-dividing-detroit-high-stakes-police-privacy-n1045046 (indicating that Detroit is likely to restrict law enforcement use of the technology) [https://perma.cc/ZLU6-BHCA].

25. *See, e.g.*, *Grading on a Curve: Privacy Legislation in the 116th Congress (2019-2020)–Updated*, ELEC. PRIV. INFO. CTR. (Apr. 2020), https://epic.org/GradingOnACurve/EPIC-GradingOnACurve-Apr2020.pdf [https://perma.cc/6BHL-BNTH]; *Senators Demand Information From Amazon on Ring and Surveillance*, EPIC (Nov. 21, 2019), https://epic.org/2019/11/senators-demand-information-fr.html [https://perma.cc/CSP7-GW3S].

26. Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/WAV5-BTKT].

society want to be spied on by governments and corporations—and what sorts of influence we want them to have over our lives."[27]

In short: Do the risks associated with using the technology outweigh the risks associated with not using it? While American society grapples with that deeper question, the legal community can answer two additional, but much narrower and simpler questions:

1) What does it look like to hold surveillance technology companies to the same standards as other industries regarding the transparency of their sales practices and the truthful advertising surrounding the effectiveness of their products?
2) How can the law ensure that recruiting police departments as social media influencers does not allow those companies to bypass those standards?

Much can be said about this "perfect storm of privacy threats"[28] and the problem of partnerships between global surveillance-based technology companies and local law enforcement.[29] This Note will address only the what, the why, the who, and the how of using consumer protection law to compel disclosure of the relationship between police departments and companies selling products like Amazon Ring. There should be a natural friction when Big Tech sells surveillance equipment nationwide to facilitate behavioral data collection in the guise of promoting public safety—but these partnerships with police have reduced that friction.

Consumer protection law can provide a model to address the privacy threats posed by corporate partnerships with law enforcement, like police endorsements and sales of Amazon Ring—by attaching penalties to a lack of transparency in these partnerships as they would with any other form of misleading advertising. These partnerships should be fully disclosed to consumers in promotional materials, as any other marketing relationship

27. *Id.*

28. Matthew Guariglia, *Amazon's Ring Is a Perfect Storm of Privacy Threats*, ELEC. FRONTIER FOUND. (Aug. 8, 2019), https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats [https://perma.cc/JSB4-NRLZ].

29. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/C3Y8-XRAS]. There are many examples of agreements between police departments and surveillance technology vendors, secret even from police leadership. *See, e.g.*, Tim Cushing, *Harris Stingray Nondisclosure Agreement Forbids Cops From Telling Legislators About Surveillance Tech*, TECHDIRT (Jan. 25, 2018), https://www.techdirt.com/articles/20180120/06352239048/harris-stingray-nondisclosure-agreement-forbids-cops-telling-legislators-about-surveillance-tech.shtml [https://perma.cc/L8PV-5FKJ]; Alex Boutilier, et al., *Clearview AI to Pull Out of Canada and Stop Working with RCMP Amid Privacy Investigation*, THE STAR (July 6, 2020), ("More than a dozen police services initially told the Star their forces hadn't tested the tool only to later confirm that officers had used trial versions of Clearview AI without the knowledge or authorization of police leadership.") https://www.thestar.com/news/canada/2020/07/06/clearview-ai-to-pull-out-of-canada-and-stop-working-with-rcmp-amid-privacy-investigation.html [https://perma.cc/2A6V-2E5C].

would be. This still offers no direct redress for bystanders captured by this technology, but it does create greater opportunity for public debate about private-public surveillance partnerships, which could indirectly mitigate the impact of second order privacy harms.

In fact, until a meaningful federal privacy law is passed, consumer protection law is the best, and perhaps only, immediate legal solution to combat the alarming growth of these corporate-law enforcement surveillance partnerships and to increase transparency among consumers and concerned citizens.

III. AMERICA'S SURVEILLANCE ZEITGEIST

A. Surveillance Capitalism Moves Faster Than Tech Regulation

Surveillance technology now collects human behavioral data at an unprecedented scale, a phenomenon which Dr. Shoshana Zuboff attributes to the rise of surveillance capitalism.[30] She defines surveillance capitalism as "the unilateral claiming of private human experience as free raw material for translation into behavioral data" and offers as one unsettling example: "breathing machines purchased by people with sleep apnea . . . secretly sending usage data to health insurers, where the information can be used to justify reduced insurance payments."[31] As its name suggests, surveillance capitalism is driven by private corporations, although products like Ring explicitly offer that data to law enforcement agencies.

What began as data collection necessary to personalize online advertising has since mutated into data collection to create habit-forming products and services, driven by a tech industry that Dr. Zuboff asserts has already begun the transition from gathering behavioral data to using that data to direct behavior.[32]

The proliferation of free services like Facebook, Google/YouTube, and Amazon's Neighbors, subscription services like Amazon Prime, Netflix, and Spotify, and smart home devices like Nest, Ring, and Alexa enable the

30. Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html [https://perma.cc/2DQH-SA9Z]; *e.g.*, Stuart Thompson & Charlie Warzel, *8 Things to Know About Our Investigation Into the Location Business*, N.Y. TIMES (Dec. 19, 2019), (discussing that even children are not safe from surveillance) https://www.nytimes.com/interactive/2019/12/19/opinion/nyt-cellphone-tracking-investigation.html [https://perma.cc/YFE9-6EQX]; IRL *The Surveillance Economy* (Feb. 4, 2019), (identifying the seemingly persistent issue of companies collecting more information than what is needed to improve their products, often allowing for institutionalized injustices) https://irlpodcast.org/season4/episode5/ [https://perma.cc/3HH9-KJWY].

31. John Laidler, *High Tech Is Watching You*, THE HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ [https://perma.cc/25CE-WHJH].

32. *See* John Naughton, *'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism*, GUARDIAN (Jan. 20, 2019), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook [https://perma.cc/KE9Z-J5DE].

collection of loads of behavioral data about individuals and families. And in the case of smart home devices and platforms like Neighbors and Next Door, companies collect data about guests and travelers. As Cambridge Analytica exposed the information of Facebook friends who never consented[33] to take the now-infamous personality quiz,[34] so too will these devices and platforms likely develop profiles on subjects who are unwitting and unwilling at the time of collection. And where tools permit sharing surveillance data with law enforcement, this can exacerbate our country's existing problems with racially-motivated requests for police presence.[35]

As the initial sleep apnea example illustrated, surveillance capitalism is not at all limited to use by law enforcement,[36] but for privacy advocates, this use by law enforcement is among the more troubling applications of these technologies. This is because (1) the technology is not always reliable (often in inequitable ways that can harm people experiencing homelessness, people of color, and undocumented immigrants);[37] (2) even where it is reliable the process required to achieve such reliability may not be followed;[38] and (3) even where the required process is followed to ensure reliability, the

33. *See AG Racine Sues Facebook for Failing to Protect Millions of Users' Data*, OFF. ATT'Y GEN. D.C. (Dec. 19, 2018), https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions [https://perma.cc/VHW9-EG58] [hereinafter *AG Racine Sues Facebook*].

34. *See* Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytics Turned Facebook 'Likes' Into a Lucrative Political Tool*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm [https://perma.cc/6CAN-HBVZ].

35. *See* Daniel Victor, *When White People Call the Police on Black People*, N.Y. TIMES (May 11, 2018), https://www.nytimes.com/2018/05/11/us/black-white-police.html [https://perma.cc/DA84-3GXT].

36. *See* Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too*, N.Y. TIMES (Nov. 4, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html [https://perma.cc/NF87-6Z4G].

37. *See, e.g.*, Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, VICE (Feb. 7, 2019), https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops [https://perma.cc/P8L2-YXD2]; Rick Paulus, *On Nextdoor, the Homeless Are the Enemy*, ONEZERO (Sept. 30 2019), https://onezero.medium.com/how-nextdoor-encourages-hate-of-the-homeless-9200475cda43 [https://perma.cc/A4VV-XZYU]; Hiba Ali, *Amazon's Surveillance System Is a Global Risk to People of Color*, ZORA (Sept. 25, 2019), https://zora.medium.com/amazons-surveillance-system-is-a-global-risk-to-people-of-color-a5030a19d5e1 [https://perma.cc/536J-HB55].

38. *E.g.*, Clare Garvie, *Garbage In, Garbage Out*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), (discussing that in one instance, police implemented FR tech on a picture of Woody Harrelson because an officer believed the suspect looked like the celebrity, yet using FR tech on the actual picture of the suspect yielded no results) https://www.flawedfacedata.com/ [https://perma.cc/LDM4-Y6CT].

technology can still be used for purposes and by agencies other than those for which it was initially intended.[39]

Vendor relationships where law enforcement use of surveillance technology is concerned are notoriously lacking in transparency and accountability.[40] In the absence of regulation, this has led to the growth of local Community Control Over Police Surveillance (CCOPS) organizations,[41] which call for greater transparency regarding law enforcement's use of surveillance technology.[42]

---

39. These practices include the police departments with whom consumers share Ring data passing that data along to other agencies, as well as Amazon sharing the information with employees in other countries for human annotation of captured video feeds to train its recognition capabilities. *See, e.g.*, Alfred Ng, *You Shared Ring Footage With Police. They May Share It, Too*, CNET (Sept. 4, 2019), https://www.cnet.com/news/you-shared-ring-footage-with-police-they-may-share-it-too/ [https://perma.cc/K3HN-3KFK]. (discussing police departments not disclosing to consumers when sharing their videos on to other agencies); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 23, 2015), https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ [https://perma.cc/8VB6-EAC5] (discussing police departments using national security technology to solve petty crimes); Nicole Nguyen & Ryan Mac, *Ring Says It Doesn't Use Facial Recognition, But It Has "A Head of Face Recognition Research"*, BUZZFEED NEWS (Aug. 30, 2019), https://www.buzzfeednews.com/article/nicolenguyen/amazon-ring-facial-recognition-ukraine [https://perma.cc/BK3F-6XBL] (discussing that Amazon uses Ring footage to train facial recognition AI); Dell Cameron, *Cops Are Giving Amazon's Ring Your Real-Time 911 Caller Data*, GIZMODO (Aug. 1, 2019). https://gizmodo.com/cops-are-giving-amazons-ring-your-real-time-911-data-1836883867 (discussing police sharing 911 call data, including location data, with Ring).

40. *See, e.g.*, Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ [https://perma.cc/7XJV-ATJK]; *see also Emily* Sullivan, *Baltimore Spending Board Terminates Controversial Surveillance Plane Contract* (Feb. 3, 2021), https://www.wypr.org/post/baltimore-spending-board-terminates-controversial-surveillance-plane-contract (discussing that the program has been discontinued).

41. *Community Control Over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (last accessed Jan. 26, 2020) [https://perma.cc/PGW4-M8YU]; *e.g.*, *Community Oversight of Surveillance – DC*, ACLU D.C., https://www.acludc.org/en/community-oversight-surveillance-dc (discussing such a program proposed in D.C., the Community Oversight of Surveillance (DC COS)) (last visited Jan. 26, 2020) [https://perma.cc/Z6HT-VXBB]; SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, https://www.stopspying.org/ (discussing such a program in New York City, the Surveillance Technology Oversight Project (STOP)) (last accessed Jan. 26, 2020) [https://perma.cc/TZ5X-KF7J].

42. *See generally* Kade Crockford, *Emails Show Surveillance Oversight Laws Can Stop Secret Police-Amazon Agreements in Their Tracks*, ACLU MASS. (Sept. 10, 2019), https://www.aclum.org/en/publications/emails-show-surveillance-oversight-laws-can-stop-secret-police-amazon-agreements-their (showing that one such group in Massachusetts is encouraged by early results from its civilian oversight efforts).

B. Changing the Calculus on Incentivized Consent for Surveillance

Amazon is particularly problematic because it operates at a national level, but there are still relevant privacy concerns when the data collection is limited to the local level, for instance in the District of Columbia.

Predating Amazon's relationships with police departments, D.C. has used aggressive rebate and voucher programs to encourage citizens to deploy private security cameras.[43] Participation in this program lets the police know which residences installed these devices and capitalizes on a feeling of reciprocity when the police request data from the owner, as the city helped to subsidize the owner's acquisition of the camera. On the one hand, this exacerbates existing suspicions in the community, as law-abiding outsiders to the community (or even tenants, children, and protestors, in their own community[44]) do not get a say over how their image is captured and shared with law enforcement. On the other hand, these kinds of programs increase access to technology that can alleviate fears about lack of security among homeowners, and in D.C.'s case, tenants as well. These kinds of policies incentivize protecting known property interests at the expense of protecting the civil liberties of unknown people.

But surely when entire communities are on the same platform, one which owns all of that surveillance data, as in the case of tech giants like Amazon, that calculus must change.

C. State Consumer Protection Agencies Must Continue to Lead

Although there is interest in regulating this technology at the federal level, no meaningful, relevant legislation has yet been passed. That said, state attorneys general have shown no lack of boldness in bringing antitrust suits against global tech giants like Facebook and Google for their collection and

43. *See Private Security Camera System Incentive Program*, OFF. OF VICTIM SERVS. AND JUST. GRANTS, https://ovsjg.dc.gov/service/private-security-camera-system-incentive-program (last accessed Jan. 26, 2020) [https://perma.cc/8GTL-6N56].

44. Although not specific to DC, the Neighbors app has been known to host posts featuring videos of children walking down the street with a narrator saying, "Whose kids are these?", *see* Drew Harwell, *Ring and Nest Helped Normalize American Surveillance and Turned Us Into a Nation of Voyeurs*, WASH. POST (Feb. 18, 2020), https://www.washingtonpost.com/technology/2020/02/18/ring-nest-surveillance-doorbell-camera/ [https://perma.cc/7965-7Q9W]. Additionally, in 2020, the LAPD requested Ring footage in conjunction with Black-led protests in response to police violence. *See* Matthew Guariglia & Dave Maass, *LAPD Requested Footage of Black Lives Matter Protests*, ELEC. FRONTIER FOUND. (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests. Fewer than 7% of these protests resulted in violence, destruction, or serious uses of force by police. Kevin Rector, *LAPD Reports Show That the Vast Majority of George Floyd Protests Were Peaceful*, LOS ANGELES TIMES (Oct. 23, 2020), https://www.latimes.com/california/story/2020-10-23/lapd-most-george-floyd-protests-peaceful.

alleged misuse of consumer data.[45] The self-imposed moratoria by Amazon, Microsoft, and IBM shortly before the public announcement of the first false arrests in Michigan[46] in 2020 demonstrate both the prematurity of the widespread deployment of this technology and the privacy gains from heightened public awareness of how these technologies are actually used. To the extent that there are statutory facial recognition bans and oversight initiatives, they are primarily at the local level. While a federal solution would be preferable from a civil rights and social justice perspective, the fastest way to bring the law up to speed with technology and with business practices is by focusing on efforts at the state and local level.

IV. THE LAW'S RESPONSE

A. Traditional Legal Remedies Do Not Apply

Contract, constitutional, and property law are unlikely to remedy the privacy issues associated with Amazon's technology.

The Fourth Amendment does not apply when the search is conducted by a private party (e.g., the homeowner). One ACLU attorney, Matt Cagle, has observed:

45. *See, e.g.*, Shannon Bond & Bobby Allyn, *48 AGs, FTC Sue Facebook, Alleging Illegal Power Grabs to 'Neutralize' Rivals*, NPR (Dec. 9, 2020), https://www.npr.org/2020/12/09/944073889/48-attorneys-general-sue-facebook-alleging-illegal-power-grabs-to-neutralize-riv [https://perma.cc/L77A-Y8CA]; Catherine Thorbecke & Aaron Katersky, *Google Hit With New Antitrust Lawsuit From 38 State Attorneys General*, ABC NEWS (Dec. 17, 2020), https://abcnews.go.com/Technology/google-hit-antitrust-lawsuit-38-state-attorneys-general/story?id=74780182 [https://perma.cc/QKR8-FMBX].

46. *See* Rebecca Heilweil, *Big Tech Companies Back Away From Selling Facial Recognition to Police. That's Progress*, VOX (June 11, 2020), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police; Robert Williams, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*, WASH. POST (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/ [https://perma.cc/W2LW-SJTQ]. Less than thirty days after Robert William's op-ed, Engadget published a story describing a second false arrest prompted by police use of facial recognition technology. See Holt, *supra* note 16.

> [T]he simple existence of a program like the Neighbors Portal threatens to blur, if not eliminate, the distinction between private-sector surveillance services and the government's role as enforcer of the law. With regards to the latter, we have powerful constitutional safeguards, while with the former we have only terms of service and privacy policy agreements that no one reads.[47]

To that end, per its terms of service, Ring's rights to the footage taken from a user's front door include "an unlimited, irrevocable, fully paid, and royalty-free, perpetual, worldwide right to re-use, distribute [sic] store, delete, translate, copy, modify, display, sell, create derivative works."[48]

Although Ring has indicated that it would not provide user video data in response to a subpoena,[49] if a user willingly gives up their own data, that would also be a means of side-stepping constitutional safeguards.[50] One scholar has additionally observed, in a manner consistent with the ACLU's concerns, that use of corporate surveillance products in criminal investigations could shield proffered evidence from cross-examination by the defendant due to trade secret and/or intellectual property protections.[51]

Property law offers no redress either, as Ring disclaims any responsibility for the user's improper deployment of the product. "Our devices are not intended to be and should not be installed where the camera is recording someone else's property without prior consent nor public areas."[52] In the context of Amazon's facial recognition product, Rekognition, even an Amazon employee has taken issue with this approach. "For Amazon to say that we require our Rekognition customers to follow the law is no guarantee of civil liberties at all—it's a way to avoid taking responsibility for

---

47. Sam Biddle, *Amazon's Home Surveillance Chief Declared War on 'Dirtbag Criminals' As Company Got Closer to Police*, INTERCEPT_ (Feb. 14, 2019), https://theintercept.com/2019/02/14/amazon-ring-police-surveillance/ [https://perma.cc/BT2X-2SUL].

48. Guariglia, *supra* note 28.

49. Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/NWS2-FAQV]; *How Law Enforcement Uses the Neighbors App*, RING HELP, https://support.ring.com/hc/en-us/articles/360031595491 (last visited Jan. 26, 2020) [https://perma.cc/E9XH-FBEQ].

50. *See Fight for the Future Launches New Campaign Calling on Mayors and City Officials To Ban Police Partnerships With Amazon Ring Surveillance Doorbells*, FIGHT FOR THE FUTURE (July 31, 2019), https://www.fightforthefuture.org/news/2019-07-31-fight-for-the-future-launches-new-campaign-calling/ [https://perma.cc/C5RH-WZXT] [hereinafter Fight for the Future].

51. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STANFORD L. REV. 1343 (May 2018), https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf [https://perma.cc/MEV7-JEG7]*; cf.* Charlie Warzel, *Privacy Is Too Big to Understand*, N.Y. TIMES (Apr. 16, 2019), https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html [https://perma.cc/DH6L-36FT].

52. Biddle, *supra* note 47.

the negative uses of this technology."[53] This presents two problems. First, coupled with the contract law issues discussed above, this means that Amazon is not responsible for information collected by Ring but has the freedom to use that information as it sees fit. Second, one-click consent[54] allows for an end run to be made around the Fourth Amendment's protections, as homeowners can share their surveillance data with law enforcement. Indeed, in response to public concern about police in Jackson, Mississippi piloting a program that harvests Ring data from homeowners in real-time, Amazon offered the following:

> [Amazon and Ring] are not involved in any way with any of the companies or the city in connection with the pilot program. The companies, the police and the city that were discussed in the article do not have access to Ring's systems or the Neighbors App. Ring customers have control and ownership of their devices and videos, and can choose to allow access as they wish.[55]

B. There is a Pressing Need for Alternative Remedies

One might argue that the response of privacy advocates is akin to Chicken Little.[56] Clearly if society feels a grievous harm is happening here, cultural norms and market forces will correct the error. Indeed, this seems to have happened in Orlando, where deployment of Amazon surveillance technology was attempted and discontinued twice.[57] But this is not an issue of what technology local police choose to use. It is an issue of what technologies police encourage consumer-citizens to use, particularly after police departments sign agreements that prohibit them from making any public statement about the technology without company approval.

> If media reaches out with questions about the partnership or the Neighbors app, or for assistance with overall PR strategy, please contact Ring's PR Coordinator . . . All public facing messaging and materials must be approved by both parties; either by using approved templates or submitting to Ring PR for approval.[58]

53. An Amazon Employee, *supra* note 19.

54. Harwell, *supra* note 3.

55. Guariglia, *supra* note 23.

56. "Chicken Little" is a folk tale about a chicken who believes the sky is falling and becomes hysterical with concern that the world is coming to an end after an acorn drops on their head.

57. Nick Statt, *Orlando Police Once Again Ditch Facial Recognition Software*, VERGE (July 18, 2019), https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended [https://perma.cc/Q934-AYTQ].

58. Letter from Corey Williamsen, Freedom of Info. Officer, Vill. of Benseville, to Shreyas Gandlur 8 (Aug. 13, 2019), https://www.documentcloud.org/documents/6359444-Bensenville-IL-Emails.html. [https://perma.cc/9NN2-8PGX].

The average citizen will interpret a remark made by the police, who are sworn to serve and protect the public, as a remark made in the interest of public safety, not as public relations for Amazon coming to the consumer-citizen through the mouthpiece of their local police department. Not only is this unethical, but if people knew the truth about this practice, it could diminish public trust in local police departments. Regardless, a situation in which the police can only make positive statements about a consumer product interferes with the free market for that product.[59]

However, at present, the momentum of surveillance capitalism is nudging corporations towards more expansive clandestine data collection and usage, and the homeowners purchasing Amazon Ring units have a stronger incentive to protect their online orders than the legal rights of strangers. As such, waiting for cultural norms and market correction without additional intervention will allow for continuing privacy harms.

C. The Case for Consumer Protection

The underlying issues surrounding Ring are further exacerbated by the fact that Amazon financially incentivizes police departments to encourage citizens to sign up for the Neighbors app. Amazon does this by offering departments credits towards purchasing Ring units—which police can then sell to citizens at a rate much lower than citizens would get from Amazon directly—proportionate to the number of Neighbors app downloads by citizens in their jurisdiction.[60] However, this exacerbation is one basis upon which consumer protection law may provide a remedy.

State Unfair and Deceptive Acts and Practices (UDAP) laws and the FTC's Endorsement Guides can provide some recourse where contract, property, and constitutional law offer no relief.[61] One of the chief concerns of consumer protection law is misleading statements in product promotions, including insufficient substantiation for efficacy claims and the omission of facts that might inform a purchasing decision (and in some jurisdictions, the

59. Additionally, as an international industry association for surveillance equipment noted, Amazon's behavior lacks transparency in ways that harm the industry as a whole. "We are troubled by recent reports of agreements that are said to drive product-specific promotion, without alerting consumers about these marketing relationships. This lack of transparency goes against our standards as an industry, diminishes public trust, and takes advantage of these public servants." Alfred Ng, *Amazon Ring's Police Partnership 'Troubled' Security Industry Group*, CNET (Aug. 8, 2019), https://www.cnet.com/news/amazon-rings-police-partnerships-troubled-security-industry-group/ [https://perma.cc/H4MK-2UXQ].

60. Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE: MOTHERBOARD, (July 25, 2019, 11:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement [https://perma.cc/8M8Z-AK84].

61. The Lanham Act, codified in part in 15 U.S.C. § 1125(a)(1), could also apply here, as it allows companies to bring suit against their competitors for deceptive practices, on the premise that consumers are purchasing from the deceptive seller rather than the honest seller, costing the honest seller market share and profits as a result of their adhering to honest practices. 15 U.S.C. § 1125 (2018). The Lanham Act is not a primary focus of this Note, as it is a consumer protection vehicle usable only by a competitor surveillance technology company.

reason for a merchant to offer a discount).[62] The FTC's Endorsement Guides indicate, among other things, that when promoting a company's product, the promoter must disclose any benefit they have received from the company in exchange for that promotion, and that the company (Amazon in this instance) can be liable if the promoter or endorser fails to do so.[63] This issue is complicated when partnerships with police departments are concerned, as consumer protection agencies are sometimes barred from bringing legal actions against police departments. Where the corporate entity has editorial authority over what the police department says on social media and in other public statements about the company's surveillance products, that company should be liable for that endorser's statements about those products.

1. UDAP Statutes – Active Law Across All States and D.C.

As noted above, state and local governments enacted UDAP statutes to help protect consumers from deceptive trade practices by merchants. The D.C. UDAP statute, for instance, is called the Consumer Protection Procedures Act (CPPA). CPPA protects D.C. consumers—persons who create the economic demand for a trade practice (other than for the purpose of resale)—from unfair or deceptive trade practices.[64] CPPA protects consumers by providing a private right of action against merchants—persons who sell, lease, or transfer consumer goods or services, directly or indirectly, in the ordinary course of business, or who supply goods and services which would be the subject matter of a trade practice.[65] As an example, D.C.'s Office of the Attorney General brought suit on behalf of D.C. residents against Facebook for the now-infamous Cambridge Analytica incident by filing a complaint for violations of CPPA.[66]

While it seems clear that Amazon could be the subject of a consumer protection suit, interestingly it is also legally possible (though politically unlikely) that a local police department could be sued under CPPA. Under D.C. caselaw, the Metropolitan Police Department (MPD) could be a merchant under CPPA, provided that MPD supplied directly or indirectly consumer goods or services, received remuneration from companies providing consumer goods or services, and/or entered a consumer-merchant relationship.[67] Where jurisdictions have similar UDAP statutes to D.C.'s

62. *See FTC Policy Statement Regarding Advertising Substantiation* (Nov. 23, 1984), https://www.ftc.gov/public-statements/1984/11/ftc-policy-statement-regarding-advertising-substantiation [https://perma.cc/3MYE-FW9Y].

63. Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.5 (2020).

64. The D.C. Code gives weight to the FTC's interpretations of 15 U.S.C. § 45(a) here. D.C. CODE ANN. § 28-3901(b) (West).

65. D.C. CODE ANN. § 28-3901 (West) [hereinafter CPPA].

66. *AG Racine Sues Facebook*, *supra* note 33.

67. *See* Snowder v. D.C., 949 A.2d 590, 599–600 (D.C. 2008) (finding DC Metropolitan Police Department not a merchant because it did not supply consumer goods or services, receive remuneration, or enter a consumer-merchant relationship); CPPA § 28–3901(a)(3).

CPPA,[68] police departments in the regular practice of selling Ring units, or even promoting the Neighbors App, could be found to be acting as merchants.

If a violation is found under the CPPA, consumers can sue directly and nonprofit organizations can sue indirectly.[69] Violations in this instance might include "[failure] to state a material fact if such failure tends to mislead"[70] and/or "falsely stat[ing] the reasons for offering or supplying goods or services at sale or discount prices" [71] as police departments are likely disclosing neither the full details of Amazon's editorial authority nor the incentive they receive to promote downloads of the Neighbors App.

The three major challenges with this approach are potential immunity for law enforcement agencies, political infeasibility even where there is not legal immunity, and the heightened burden of proof under UDAP. Consumer protection cases are not civil rights cases, and as such, where law enforcement enjoys immunity from suit, it might create a barrier in holding Amazon liable under a UDAP consumer protection theory. In terms of political feasibility, an AG may not even want to sue Amazon over the behavior of their own police force. Many UDAP statutes require clear and convincing evidence in their burden of proof.[72]

Remedies for UDAP violations vary by jurisdiction. In D.C., the CPPA allows for treble damages (or $1,500 per violation, if greater), as well as punitive damages and attorney's fees. It also allows for an injunction against the unlawful trade practice.[73]

2. FTC Endorsement Guidelines—Federal Guidance Each State Would Need to Adopt as Regulation

Per the FTC's guidance on endorsements, "The same [disclosure] is usually true if the endorser has been paid or given something of value to tout the product. The reason is obvious: Knowing about the connection is important information for anyone evaluating the endorsement."[74] Especially when the endorser is expected to provide unbiased advice about public safety, it is particularly important that any connection related to value (such as

68. As many as 43 seem to come close. *See* Carolyn L. Carter, *Consumer Protection in the States*, NAT'L CONSUMER L. CTR. 12 (Feb. 2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf [https://perma.cc/8KMZ-XTWG].

69. D.C. CODE § 28–3901.

70. D.C. CODE § 28–3904(f).

71. D.C. CODE § 28–3904(l).

72. *See* Carter, *supra* note 68, at 24–29.

73. *District of Columbia Consumer Protection Laws*, OFF. OF THE ATT'Y GEN. OF D.C., https://oag.dc.gov/consumer-protection/other-consumer-help-agencies-and-websites/submit-consumer-complaint/district-columbia-consumer-protection-laws (last accessed Jan. 26, 2020) [https://perma.cc/8AJR-QGQB].

74. Additionally, nothing in the FTC's Endorsement Guides states that these endorsements are limited to commentary on social media. *The FTC's Endorsement Guides: What People Are Asking*, FED. TRADE COMM'N (2017), https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking [https://perma.cc/7JP9-J4DR].

discounts on products proportionate to app downloads) be disclosed clearly and conspicuously.

Due to the level of control Amazon has over public statements by police departments, it is unlikely that Ring would be able to evade responsibility under this theory:

> It's unrealistic to expect [a company] to be aware of every single statement made by a member of [its] network. But it's up to [the company] to make a reasonable effort to know what participants in [the company's] network are saying. That said, it's unlikely that the activity of a rogue blogger would be the basis of a law enforcement action if your company has a reasonable training, monitoring, and compliance program in place.[75]

However, the FTC itself cannot pursue action against local police departments. State and local governments could adopt standards akin to the FTC's endorsement guidelines in enforcing their UDAP statutes. This would enable them to pursue Amazon for consumer protection violations that the tech company permitted (encouraged, arguably) through the sales tactics utilized by its endorsers, local police departments.[76]

In terms of remedies at the FTC level, if the company entered into a consent order to stop the deceptive act or practice, it could be fined more than $10,000 for each subsequent violation.[77]

3. Practical Limitations of the Consumer Protection Approaches

These consumer protection remedies are likely to be unsatisfying to privacy advocates, who are rightly concerned about systemic abuses in the criminal justice system.[78] Additionally, these remedies do not provide a real opportunity for the non-consumer passerby passively captured on video to

75. *Id.*

76. New York's Attorney General, for instance, has enforcedagainst misconduct similar to the misconduct covered by the FTC's Endorsement Guides, albeit under a different theory. *See New York Attorney General Cracks Down on Falsified Online Reviews*, INFOLAWGROUP, https://www.infolawgroup.com/insights/2013/10/articles/ftc/ny-ag-cracks-down-on-fake-reviews (last accessed Apr. 14, 2020) [https://perma.cc/HG6V-WPLR].

77. 15 U.S.C. § 45.

78. Telephone Interview with Andrew Ferguson, Professor, David A. Clarke Sch. of L. (Nov. 14, 2019).

bring suit.[79] Some UDAP statutes permit nonprofits to bring suits on behalf of consumers. Some may only permit consumers themselves to sue. However, in the absence of federal privacy legislation that accounts for second order biometric privacy threats, that is the best existing law can offer.[80]

D. Other Public Policy Considerations

Although outside the scope of the consumer protection law solutions proposed by this Note, there are other social and cultural issues which may serve as effective messaging points for rallying public support in defense of community oversight of these kinds of surveillance partnerships. One group has created a product warning site listing some of the concerns consumers may have.[81] VICE has noted the concern taxpayers may have with police departments subsidizing the purchase of Ring units,[82] as has the Electronic Frontier Foundation. For example, the EFF has explained that municipalities are "paying Amazon up to $100,000 to reduce costs of Ring cameras by $50 or $100 for city residents."[83]

Some might find it unsavory that Amazon uses doorbell camera data to capitalize on viral video behavior to drive sales.[84] The New York Times compellingly reports on the relationship between Ring and Neighbors, listing numerous examples of scary, funny, and sweet videos captured by Ring and

79. It is only a matter of time until technology like Ring makes situations like deploying police against delivery drivers more efficient. *See* Mariel Padilla, *Black Deliveryman Says He Was Blocked and Interrogated by White Driver*, N.Y. TIMES (May 17, 2020), https://www.nytimes.com/2020/05/17/us/black-delivery-driver-okc-travis-miller.html [https://perma.cc/97ST-7Y3H]. It seems unlikely that Amazon would call for swift investigation when a competitor's delivery service falls victim to Ring-based police deployment. *See* Sven Gustafon, *Police in Detroit Suburb Pin Black Amazon Driver in Incident Over Parking*, MSN: AUTOBLOG (June 10, 2020), https://www.msn.com/en-us/autos/news/police-in-detroit-suburb-pin-black-amazon-driver-in-incident-over-parking/ar-BB15jsTT [https://perma.cc/NL8Q-6QE3].

80. Another example of second order privacy threats can be seen in commercial genetic databases. *See* Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, WIRED (Dec. 26, 2018), ("[D]atabases like GEDMatch [are expected] to grow so big in the next few years that it will be possible to find anyone from just their DNA, even if they haven't voluntarily put it in the public domain") https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/ [https://perma.cc/4RDB-K3C3].

81. *Amazon Ring Cameras Are Not Safe*, https://www.ringsafetywarning.com/ (last accessed Jan. 26, 2020) [https://perma.cc/TUW8-9GNE].

82. Caroline Haskins, *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, VICE (Aug. 2, 2019), https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money [https://perma.cc/59SS-EDK9].

83. Matthew Guariglia, *Five Concerns about Amazon Ring's Deals with Police*, EFF (Aug. 30, 2019), https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police [https://perma.cc/UC69-VNUF].

84. *See* Ben Fox Rubin, *How Ring's Neighbors App Is Making Home Security a Social Thing*, CNET (Dec. 3, 2018), https://www.cnet.com/news/how-rings-neighbors-app-is-making-home-security-a-social-thing/ [https://perma.cc/6G48-PKFF].

shared on Neighbors.[85] Looking towards the future of what the normalization of this kind of technology could lead to, Evan Greer of Fight for the Future, a privacy advocacy group, has argued:

> Amazon is building a privately run, for-profit surveillance state, and they're getting local police to market it for them in exchange for VIP access to the panopticon . . . This corporate and government overstep allows law enforcement agencies to side-step judicial oversight by asking customers to give up their privacy rights by sharing confidential information with local police departments.[86]

Other commentators have voiced concerns with how Ring's proposed "suspicious activity detection" will be deployed[87] with enhanced biometrics (beyond facial recognition)[88] and with constant omnipresent surveillance due to density of devices.

> O'Sullivan suggests that the ubiquity of devices means you could be surveilled by Amazon even if you don't own its products. "If you have enough Ring doorbell cameras on your block, it doesn't matter if you bought one or not; you're being monitored and, down the road, perhaps your device is pinging them.[89]

When government agencies make a mistake due to dysfunctional technology, courts can opt not to suppress evidence obtained from it under the "good faith" exception. [90] There are several instances of innocent individuals who, through unfortunate coincidence, were captured by the surveillance apparatus and were subject to undue police scrutiny. As Bruce

---

85. *See* John Herrman, *Who's Watching Your Porch?*, N.Y. TIMES (Jan. 19, 2020), https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-security.html [https://perma.cc/77GA-ASK4].

86. Fight for the Future, *supra* note 50. Some would remedy the lack of judicial oversight by requiring civilian oversight, *see Community Control Over Police Surveillance supra* note 41.

87. Biddle, *supra* note 47, "Amazon's Home Surveillance Chief…"

88. *See* Madhumita Murgia, *Who's Using Your Face? The Ugly Truth About Facial Recognition*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e [https://perma.cc/5Q57-WDFL].

89. Charlie Warzel, *Amazon Wants to Surveil Your Dog*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/opinion/amazon-privacy.html. [https://perma.cc/VK7A-4GKG]. Relatedly, Brad Smith, President of Microsoft, has observed that "[w]hen combined with ubiquitous cameras and massive computing power and storage in the cloud, a government could use facial recognition technology to enable continuous surveillance of specific individuals. It could follow anyone anywhere, or for that matter, everyone everywhere." Amitai Etzioni, *Facial Recognition Meets the Fourth Amendment Test*, YAHOO! NEWS (Sept. 22, 2019) https://news.yahoo.com/facial-recognition-meets-fourth-amendment-191500422.html [https://perma.cc/28FZ-BWHU].

90. *See* Herring v. United States, 555 U.S. 135, 146–47 (2009) (noting recklessly maintained database might justify excluding evidence obtained due to inaccurate information, but isolated instances of negligence do not).

Schneier, cybersecurity expert, notes: we need to consider where the tradeoff ends for the security of property.[91]

V. FRICTION IS THE BEST NEAR-TERM SOLUTION

Because traditional claims under contract, property, and constitutional law likely favor Amazon, until robust federal privacy legislation passes, consumer protection law may be the only method for slowing corporate-facilitated police surveillance—namely by using local UDAP statutes and/or adopting and enforcing provisions like the FTC's Endorsement Guides at a local level. These methods can result in courts issuing financial penalties against Amazon as well as injunctions requiring greater transparency from Amazon, specifically regarding the representations made by police departments in the marketplace about the Ring product and the nature of the relationship between their department and Amazon. While privacy advocates would likely prefer to challenge the type of data collected or method of collection altogether, such action would require an immense amount of public education and debate. Only then could Congress pass federal legislation.

As such, to provide as immediate a stopgap as possible until that lengthy process can be completed, the best approach is to create friction in the sales growth of products like Amazon Ring and in the processes used by the police departments deputized as sales teams by tech giants like Amazon.

A. The Limits of Actionable Conduct Under Consumer Protection Law

Although privacy advocates are concerned with law enforcement making an end-run around the Constitution, a consumer protection law approach to the problem posed by corporate-law enforcement partnerships (such as Amazon Ring and local police departments) would not reach that far, only addressing problems such as:

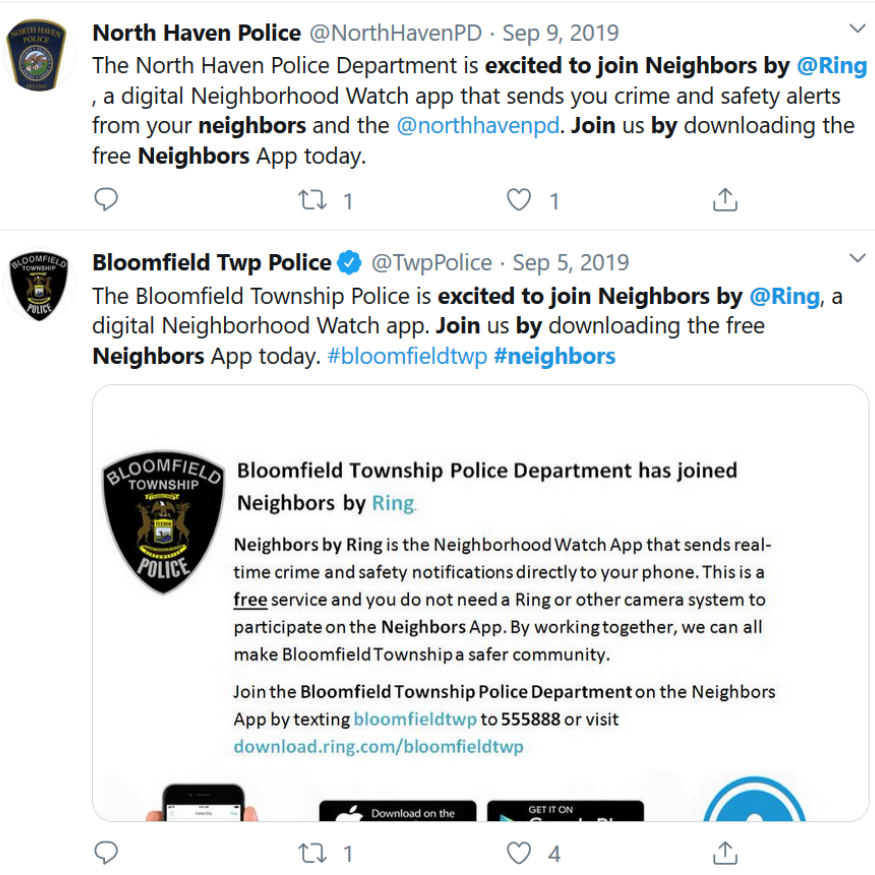
91. *See* Schneier, *supra* note 26; Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/UWC7-XMBY].

1) Misrepresentations or omissions by police departments about motivations for encouraging residents to download the Neighbors app, and relatedly, of discounted Ring units available directly or indirectly through the police department;
2) Misrepresentations or omissions by police departments about the nature of their agreement to work with Amazon Ring, specifically the editorial authority Amazon has over police departments' public statements regarding the Ring product;
3) Misrepresentations by Amazon Ring about the effectiveness of its product;
4) Misrepresentations or omissions by Amazon Ring about its privacy policies, specifically what data it collects from users and how it uses the data it collects from users;
5) Misrepresentations or omissions by Amazon Ring about the security of its product;
6) Harms to competitors (who likely also sell smart home surveillance products but do so without utilizing misleading partnerships with local police departments).

Amazon has partnered with more than 400 police departments,[92] a partnership which entails promoting Ring products (including the Neighbors app) on official police channels. "All partnerships require police to get all public statements about Ring approved by the company first, as Gizmodo reported. Police are also given a series of scripts by Ring which lay out how police are supposed to talk about the company on Neighbors."[93]

92. Jamie Siminoff, *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*, RING: BLOG (Aug. 28, 2019), https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/ [https://perma.cc/YUV2-NAVN]. More recent reports suggest this number may be closer to 2,000 as of 2021, *see* Lyons, *supra* note 23.

93. Caroline Haskins, *Ring Says It's Partnered with 405 Police Departments, Here's What We Know*, VICE (Aug. 28, 2019), https://www.vice.com/en_us/article/a35vy4/ring-says-its-partnered-with-405-police-departments-heres-what-we-still-dont-know [https://perma.cc/2SQG-46H6].



These promotions often conspicuously leave out a material motivation for the encouragement to download (i.e., discounted Ring units), which would have been a clear violation of the FTC's endorsement guidelines had the endorsing party been subject to the FTC's authority.[94]

Regarding editorial authority, Wired reported one instance from a New Jersey police department that highlighted the company's level of control over public statements:

94. *See* Antonio Villas-Boas, *Amazon Requires Police Departments To Advertise Ring Home Security Products to Residents In Return for Free Ring Cameras*, BUS. INSIDER (July 25, 2019), https://www.businessinsider.com/amazon-ring-require-police-advertise-for-free-ring-cameras-2019-7 [https://perma.cc/DU9N-4772].

> 'Unfortunately I can't make [the mayor and public safety director] say anything specific,' Bloomfield Police Captain Vincent Kerney wrote back to the Ring staffer. 'All of the information was copied and pasted directly from your press releases with the exception of the quotes.' The Ring public relations representative insisted the changes be made at least on Facebook, which they later were, according to the post's edit history. The Bloomfield Police Department did not return a request for comment.[95]

Ring's claims about the effectiveness of its product are also potential cause for consumer protection action because its own studies are inadequate, the data from those studies remain undisclosed, and independent studies do not corroborate the company's claims.[96] Amazon has the burden of substantiating its efficacy claims, and it does not seem capable of meeting it. One meta-study from MIT has found that despite Ring's claims of reducing crime, "the only study carried out independently of Ring found that neighborhoods without Ring doorbells were actually less likely to suffer break-ins than those with them." MIT went on to share one expert's questioning of the legitimacy of Ring's own studies. "I don't see the decrease in crime [Ring claims]," says Maria Cuellar, a statistician and assistant professor of criminology at the University of Pennsylvania, referring to the public district-level data. She says the sample size is too small, too: "It's not enough to say whether the effect is something you see in the data, or just some random variation." Other times, Ring did not provide the data that supported its claims when contrary evidence seemed to disprove them. Subsequent reporting on these studies further undercuts their validity as substantiation of crime reduction claims.[97]

There are also potential issues with violations of consumer expectations of privacy and security. In one instance, Amazon shared data with a Ukrainian development team.[98] Police can share users' data with other agencies.[99] Amazon can use it to train their own facial recognition programs and can sell the data to others.[100] And—in a practice that may even subject police to legal

---

95. Louise Matsakis, *Cops Are Offering Ring Doorbell Cameras in Exchange for Info*, WIRED (Aug. 2, 2019), https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/ [https://perma.cc/6ZR6-NN8T].

96. *See, e.g.*, Mark Harris, *Video Doorbell Firm Ring Says Its Devices Slash Crime—But The Evidence Looks Flimsy*, MIT TECH. REV. (Oct. 29, 2018), https://www.technologyreview.com/s/612307/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/ [https://perma.cc/ET3Q-YK2F].

97. *See* Cyrus Farivar, *Cute videos, But Little Evidence: Police say Amazon Ring Isn't Much of a Crime Fighter*, NBC NEWS (Feb. 15, 2020), https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026.

98. Biddle, *supra* note 47.

99. *See* Ng, supra note 20.

100. Octavio Mares, *How Amazon Is Selling Your Facial Recognition Data Using a Doorbell*, INFO. SEC. NEWSPAPER, (Aug. 14, 2019), https://www.securitynewspaper.com/2019/08/14/how-amazon-is-selling-your-facial-recognition-data-using-a-doorbell/ [https://perma.cc/UT3P-VABE].

action as it represents misuse of sensitive data—police share 911 data with Amazon.[101] Ring also has historically encountered problems with the security of its devices in disturbing ways.[102]

B. Friction and Deterrence through UDAP

Existing state and local UDAP statutes could effectively slow the spread of sales methodologies like those used by Amazon to sell Ring.

As of the time of this writing, Amazon had not yet substantiated its claims of reducing crime or making neighborhoods safer. In fact, the only information publicly available, via third parties, refuted Amazon's claims.[103] By limiting Amazon's ability to make unsubstantiated claims about Ring's effectiveness in reducing crime, police departments may be less likely to form partnerships with Ring, and consumers less likely to purchase Ring units. In jurisdictions where companies are liable for the actions of their endorsers, police departments that repeat Amazon's unsubstantiated claims could give rise to additional liability for Amazon under the local UDAP statute. Where jurisdictions have similar UDAP statutes to D.C.'s CPPA, [104] police departments that sell Ring units or even promote the Neighbors App could be treated as merchants.

Although it may be politically unfeasible to sue a police department, D.C. case law suggests that police departments could violate the CPPA if they supplied services and/or received remuneration for the services provided and/or entered into a consumer-merchant relationship.[105] As noted above,[106] consumers and nonprofits can bring suit in D.C. under its consumer protection statute, and that right of action is common among the states.[107] To the extent that other jurisdictions have similar consumer protection laws, and that their corresponding police departments exhibit the reported behaviors—e.g., neglecting to disclose the discounts received through Neighbor app downloads or directly selling Ring units to residents or receiving remuneration from Amazon for their indirect facilitation of Ring sales—there may be immediately actionable behavior against the police departments and/or against Amazon for the police department's actions under such laws.

The biggest challenge with this approach is if the representations about the product are being made by the police department but not directly by Amazon (even if the communications are approved or pre-written by

101. *See* Cameron, *supra* note 39.

102. *See, e.g.*, Joseph Cox & Samantha Cole, *How Hackers Are Breaking into Ring Cameras*, VICE (Dec. 11, 2019), https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras [https://perma.cc/P28G-9PR8].

103. *See, e.g.*, Harris, *supra* note 96; Farivar, *supra* note 97.

104. *See* Carter, *supra* note 68. Violations in this instance might include "[failure] to state a material fact if such failure tends to mislead" and/or "falsely state the reasons for offering or supplying goods or services at sale or discount prices" as police departments are likely not disclosing the full details of Amazon's editorial authority nor the incentive they receive to promote downloads of the Neighbors App. D.C. CODE § 28–3904(f).

105. *See* Snowder v. D.C., 949 A.2d 590, 599–600 (D.C. 2008).

106. D.C. CODE § 28-3901(b).

107. *See* Carter, *supra* note 68.

Amazon), jurisdictions in which police departments are immune from suits by consumer protection agencies may block liability for Amazon as well. In such jurisdictions there would unfortunately still be no recourse, as (1) the company which could be liable is not making the representation to the consumer, (2) the merchant/endorser who cannot be liable is making the representation to the consumer, and (3) the jurisdiction does not permit acts by the immune merchant/endorser to create liability for the company. It is unlikely that any jurisdiction would permit this trifecta of policies, especially when the company has such powerful editorial authority with the merchant/endorser in question as Amazon Ring does with local police departments. At a minimum this does not appear to be the case in D.C., where courts may consider police to be merchants.

An additional challenge is burden of proof, as many UDAP statutes require clear and convincing evidence, which makes it harder to succeed once the court reaches consideration of the merits.

C. Friction and Deterrence Using the FTC's Endorsement Guides as a Model

Even if the FTC could bring claims under the FTC Act against Amazon for endorsements made by police departments,[108] it may be politically unfeasible. While state Attorneys General may encounter similar political obstacles, they have demonstrated their readiness to take on tech giants like Facebook and Google over issues of commodification of consumer data and violations of privacy, and as such, might sue the corporate provider of the surveillance technology, such as Amazon.[109]

As noted above, the FTC's guidance on endorsements requires disclosure when an endorser has "been paid or given something of value to tout the product" and that the company must have a "reasonable training, monitoring, and compliance program in place" to ensure endorser conduct complies with the FTC's guidelines.[110] Because of Amazon's substantial level of control over the communications and representations made by police departments about its Ring product, a state or local government enacting a

108. FTC's jurisdiction is limited to "persons, partnerships, or corporations." 15 U.S.C. § 45(a)(2). Its organic statute defines a corporation as an entity "organized to carry on business for its own profit or that of its members." 15 U.S.C. § 44. Municipal police departments do not fall within this purview.

109. *See* Bond & Allyn, *supra* note 45.

110. FED. TRADE COMM'N, *supra* note 74, at 1, 14; *see also* Letter from Mary K. Engle, Assoc. Dir., Div. of Advert. Pract., Fed. Trade Comm'n, to Aaron Hendleman & Lydia Parnes, Counsel for Nordstrom, Inc. (Feb. 22, 2013) (on file with Fed. Trade Comm'n), https://www.ftc.gov/sites/default/files/documents/closing_letters/nordstrom-rack/130222nordstromrackletter.pdf. Violations of these guidelines can result in enforcement penalties under the Commission's Section 5 authority. *See* Mark S. Goodrich & Jason Howell, *Check in on Influencer Marketing*, CONSUMER PROT. REV. (Aug. 31, 2020), https://www.consumerprotectionreview.com/2020/08/check-in-on-influencer-marketing/ [https://perma.cc/ZC9U-EY6P]; Richard B. Newman, *Another Lesson From the Federal Trade Commission on Endorsement Guideline Compliance*, FTC DEF. LAW. (Nov. 16, 2018), https://ftcdefenselawyer.com/another-lesson-from-federal-trade-commission-endorsement-guideline-compliance/ [https://perma.cc/V288-XNNQ].

policy comparable to the FTC's guidance on endorsements would provide authority for its local consumer protection agency to take action against Amazon for not only failing to ensure compliance but in fact for encouraging non-compliance. For Amazon to comply, it would need to apply its oversight over police departments just as zealously to ensure greater transparency about the effectiveness of its product, the benefits police departments are receiving for their endorsements of Ring and Neighbors, and the underlying partnership between Amazon and police departments more generally.

As anyone who has watched an advertisement replete with disclaimers can attest, such additional disclosures would likely chill consumer interest in the product, regardless of the content of those disclosures. Additionally, the content itself may cause political and cultural change in how citizens view their police departments and the individuals responsible for the policies of those departments, which in turn could result in a change in practices by those police departments in their dealings with vendors of surveillance products. These are admittedly indirect and hypothetical results. However, it may be the most immediately practical path forward in the absence of on-point federal privacy legislation.

In a best case scenario for privacy advocates, Amazon could be found liable for its own actions in addition to the actions of the police departments acting under its direction, stacking financial penalties for the multiple violations and potentially creating a stronger case for a broad injunction requiring greater transparency in advertising by Ring, including what it approves and/or pre-writes for police departments.

UDAP statutes presently provide states the ability to compel transparency in advertising, issue financial penalties for unsubstantiated claims used in advertising, and possibly even sue the offending government agencies (though that may not be politically feasible). Endorsement guidelines could provide a powerful tool for consumer protection agencies to attack tech giants routing sales through government entities using unfair or deceptive methods.

These approaches available through consumer protection law represent the fastest methods for creating friction in the otherwise explosive growth of surveillance technology directly *resulting from* unsavory partnerships between global tech companies and local police departments and likely *resulting in* disproportionate contact with the criminal justice system.

VI. CONCLUSION

Americans can expect inadequately disclosed partnerships between global technology companies and police departments to continue to proliferate in the absence of friction and deterrents making such partnerships inefficient. Although the most comprehensive solution would be a meaningful federal privacy law, a more immediate solution exists in consumer protection law. Although consumer privacy laws do not adequately address the underlying privacy issues of these technologies (especially their use by law enforcement), a more immediate solution that addresses transparency is

encouraged as the adoption of this technology continues to expand at a breakneck pace.

Can Victims of Child Sexual Abuse Material Use Copyright as a Method of Full Restitution from Possessors and Distributors?

Erin Seeton*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; M.A., Kinesiology, University of Alabama; B.A., Economics, University of Alabama. I would like to thank my family and friends for listening to me talk about this very troubling topic ad nauseum for roughly nine months. I would also like to thank Michael Beder, Journal Adjunct and a special thanks to Christine Kumar, Vol. 72 Notes Editor for always encouraging me and giving me the confidence to write even when I didn't want to. Finally, I would like to acknowledge the strength and resilience of CSAM victims and those working tirelessly to support them every step of the way.

I. INTRODUCTION

In 2014, a young woman known pseudonymously as Amy appeared in court seeking victim's restitution in the case *Paroline v. United States*.[1] In *Paroline*, defendant Doyle Paroline pleaded guilty to possession of between 150 to 300 images of child sexual abuse, including two of Amy, in 2009.[2] At the time of the *Paroline* case, the images of Amy's childhood sexual abuse were some of the most widely seen and distributed child sexual abuse images on the Internet, with more than 70,000 individual images on computers all over the world.[3] Amy sought restitution under 18 U.S.C § 2259[4] totaling over $3.4 million for her lost wages and other financial harm caused by the continued circulation of her abuse.[5] The United States Supreme Court in *Paroline* held that a victim could collect restitution under § 2259 "only to the extent the defendant's offense proximately caused a victim's losses."[6] This holding severely limited Amy's ability to collect restitution damages for lost wages. Because of Amy's abuse, she has been unable to regularly work, and will require psychological and psychiatric treatment for the rest of her life.[7] Amy received counseling throughout the 1990s, and in 1999, her psychologist reported that she was getting back to normal and healing from her abuse. But in the early 2000s, she found out that her abuse images were some of the most shared online, and her recovery took a drastic downturn.[8] The knowledge that abusers still share and possess her image has taken a serious toll on her mental health.[9]

In response to this set back in Amy's ability to recover financially from those who view and distribute her abuse, her attorney, James Marsh, negotiated with the abuser, her uncle, for the transfer of the copyright of the abuse images to Amy.[10] Marsh then registered the copyright of these images with the United States Copyright Office, providing descriptions of the images instead of the images themselves, due to the illegality of the images.[11]

It is illegal in the United States to produce, distribute, receive, and possess child sexual abuse images.[12] Victims of these crimes are eligible to

1. Paroline v. United States, 572 U.S. 434 (2014).
2. *Id.* at 439.
3. Warren Binford et al., *Beyond Paroline: Ensuring Meaningful Remedies for Child Pornography Victims at Home and Abroad*, 35 CHILD. LEGAL RTS. J. 117, 117 (2015).
4. 18 U.S.C. § 2259 imposes mandatory restitution for victims of child pornography production and trafficking.
5. *Paroline*, 572 U.S. at 441.
6. *Id.* at 434.
7. Paul G. Cassell & James R. Marsh, *The New Amy, Vicky, and Andy Act: A Positive Step Toward Full Restitution for Child Pornography Victims*, 31 FED. SENT. R. 187, 187 (2019).
8. *See id.*
9. *See id.*
10. Binford, *supra* note 3, at 153.
11. *Id.*
12. 18 U.S.C. §§ 2251–2252 (2012).

collect restitution under several different schemes,[13] but actually recovering financially from the harm can be difficult because litigation costs are high for the victim, both monetarily and psychologically. Many victim restitution laws still require victims to prove how defendants caused their harm, which can lead to victims reliving their trauma when they bring suit, thereby increasing emotional cost for victims and decreasing their willingness to litigate these claims.[14] Even the most recent restitution scheme, the Amy, Vicky, and Andy Act ("AVAA"), which does not require a nexus of harm, still only delivers nominal damages for possession of images.[15] The minimum a victim can collect from a defendant under the AVAA is $3,000.[16] Yet Amy's estimated losses total over $3,000,000, meaning that she would have to litigate over 1,000 minimum restitution cases to fully recover financially.[17] Amy's attorney presumably thought that he could litigate fewer cases with higher damage rewards to achieve full restitution for Amy under the Copyright Act of 1976. Additionally, when victims own the copyright of the images or videos in which they appear, they have the ability to send take-down notices as provided in the Digital Millennium Copyright Act ("DMCA").[18] Under the DMCA, copyright owners are able to send notices to service providers[19] informing them that there is infringing material on their sites, and if a service provider does not take down the infringing material, the copyright owner may sue the service provider for contributory or vicarious copyright infringement.[20]

There are other incentives for victims to move to own the copyright of the images and recordings depicting their abuse. In other intimate media realms, such as pornography involving adults but created through coercion or abuse, and sexual images publicized without consent (also known as "revenge pornography"), scholars have argued that there is a marked benefit to the victims when they own and feel like they have control over their abuse imagery.[21] Even if victims cannot fully stop the circulation of their abuse images, the knowledge that they have power over the images, as opposed to their abuser, can be calming and eases some anxiety relating to the continued circulation of the images.[22]

---

13. *See, e.g.*, Victim and Witness Protection Act of 1982, Pub. L. No. 97-291, 96 Stat. 1248 (1982) (codified at 18 U.S.C. § 3664 (2018)); Victims Compensation and Assistance Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984) (codified as amended at 42 U.S.C. § 10691 (2018)); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 2259, 108 Stat. 1796 (1994) (codified as amended at 18 U.S.C. § 2259 (2018)); Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299, 132 Stat. 4383 (2018).

14. Binford et al., *supra* note 3, at 136.

15. 18 U.S.C. § 2259 (2018) [hereinafter AVAA].

16. *Id.*

17. Cassell & Marsh, *supra* note 7 at 188–89.

18. Digital Millenium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, 2887 (codified at 17 U.S.C. § 512) (enacted Oct. 28, 1998).

19. "Service providers" under the DMCA include websites and Internet service providers (ISPs). *See* 17 U.S.C. § 512(K) (2012).

20. 17 U.S.C. § 512.

21. Binford et al., *supra* note 3, at 154.

22. *Id.*

This method of receiving full restitution should be examined carefully. Although Amy's attorney was seemingly able to register the images with the Copyright Office, it is still unclear if a judge would uphold the registration in court. The Supreme Court has never answered whether copyright protection for material that is illegal in its mere creation would be enforceable. There are complexities within the copyright regime that could make the fight to gain ownership, and then exercise of that ownership, more burdensome than suing hundreds of times under victim's restitution statutes. Such complexities include the hardship of negotiating with abusers for the transfer of the rights, creators' rights to terminate those transfers at later dates, and the costs associated with policing the Internet for the copyright-protected images. Many obvious solutions to these problems involve making small, but meaningful changes to the basic definitions of the Copyright Act. Nevertheless, the issue is extremely complex, especially considering that victims' compensation falls far outside the purpose of the American copyright system. Even so, in some situations, copyright could be a tool for victims to achieve full restitution from those who possess and distribute their abuse images.

This Note argues that because the current restitution regime is inadequate and harrowing for victims, victims of child sexual abuse material should be able to pursue fuller restitution by obtaining ownership of their abuse material and suing those who download, publish, or otherwise infringe the copyright of these images. This Note also suggests three amendments to the Copyright Act to streamline the litigation process and ensure that victims can obtain more beneficial damages awards in the easiest way possible. This Note will first look at the harm that circulation of child sexual abuse material (CSAM), also known as child pornography, inflicts on victims and why restitution is so vital for the healing of victims. Next, this Note will discuss the current laws in place that authorize CSAM victims to seek restitution from their abusers and the challenges victims face when attempting to do so. Section III will explain the basics of copyright law as it relates to victims attempting to utilize the copyright system, including the purpose of copyright law, what can be copyrighted, and what protections copyright owners have. Sections IV and V of this Note will discuss the benefits and detriments of having a content-neutral copyright scheme and how a victim could potentially benefit from using copyright law. Section VI addresses how detrimental negotiating for a copyright could be for a victim, and why an amendment is necessary. In the final section, this Note suggests three amendments to the Copyright Act of 1976 that would effectively make minors depicted in CSAM the authors of the work, prevent abusers from regaining ownership of the CSAM they create, and dispose of the registration prerequisite in works relating to CSAM.

II. THE POSSESSION AND DISTRIBUTION OF CSAM CAUSES VICTIMS HARM

The Supreme Court has long held that the harm suffered by child pornography victims is twofold.[23] The Court in *New York v. Ferber* first held that CSAM (called "child pornography" by the Court) harms victims not just by the abuse involved in the creation of the material, but also in the continued viewing and distribution of the material because the images or recordings are a "permanent record" of the abuse.[24] The continued circulation of the material "may haunt [the child] in future years, long after the original misdeed took place," because the child must live knowing that their abuse material is part of a mass distribution network of child pornography.[25] And the Court decided *Ferber* in 1982, when the abuse images were undoubtedly hard copies only—actual photographs that had to be printed and developed.

While the distribution of CSAM has always been a serious problem, the Internet and digital images have made circulation easier and more widespread than ever, and it is growing exponentially.[26] In 1998 there were just 3,000 child sexual abuse images on the Internet; in 2014 there were one million; in 2018, 18.4 million; and in 2019, over 45 million.[27] Because of the infinite lifespan of images and videos posted online, the harm recognized in *Ferber* caused by circulation is virtually never-ending and victims are powerless to end their abuse. Amy, the victim in the *Paroline* case, began seeing a therapist in the early- to mid-1990s after her initial abuse.[28] In the early 2000s, Amy found out that her abuse images were some of the most circulated online, causing her recovery, which her psychologist reported to be going very well, to regress.[29] The knowledge that abusers still share and possess her images ruined her mental health.[30]

There are many ways that CSAM financially harms its victims. Victims will likely spend their entire lives requiring psychological care and nearly all victims "suffer lifelong psychological damage and may never overcome the harm, even after lifelong therapy."[31] Victims have reported feelings of shame, disgust, loathing, guilt, paranoia, worthlessness, and powerlessness, culminating in diagnoses of post-traumatic stress disorder, depression, anxiety disorders, and psychoses.[32] This psychological damage comes not only from the original abuse, but also from the knowledge that a record of

23. New York v. Ferber, 458 U.S. 747, 759 (1982).
24. *Id.*
25. *Id.* at 759, n.10.
26. Michael H. Keller & Gabriel J.X. Dance, *The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES (Sept. 28, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html [https://perma.cc/C3NW-VX6R].
27. *Id.*
28. Cassell, *supra* note 7, at 187.
29. *Id.*
30. *See id.*
31. Binford et al., *supra* note 3, at 127.
32. *Id.* at 127–28.

their abuse will live on the Internet, likely forever.[33] Many victims feel anxious about being recognized in public and having to interact with someone who may have viewed their abuse.[34] Some victims report disguising themselves every time they leave their homes so that they won't be recognized in public.[35] Child pornography victims are more likely than most to abuse alcohol later in life, "with the severity of the child abuse correlating with the severity of alcohol abuse."[36] Victims also suffer mental anguish because in many instances, CSAM is used to groom other children in order to create new CSAM, so victims are aware that their abuse may be used to harm others.[37] To make matters worse, there are few mental health professionals equipped to deal with this type of abuse, making it "difficult for victims to find effective therapeutic support."[38]

In addition to the difficulties of psychological care, victims suffer lost income due to their inability to maintain regular employment caused by fear of being recognized, and many victims spend their lives in and out of psychiatric care.[39] Victims also incur costs related to litigation, namely attorneys' fees, transportation, and childcare.[40] Victims often have trouble forming meaningful adult relationships, which can further damage their mental and emotional health.[41]

Amy, the victim in *Paroline*, calculated her total lifetime losses to be over $3 million.[42] Without a proper restitution scheme and a way to fully recover financially from her abuse, she cannot recover emotionally and mentally.

III. CURRENT AND HISTORICAL RESTITUTION SCHEMES FOR VICTIMS AND WHY THEY FAIL TO PROVIDE FULL FINANCIAL RECOVERY

Victims of CSAM suffer immense harm, not just emotionally, but also financially.[43] Government prohibition of the creation, distribution, and possession of child pornography helps curb the victimization of children by deterring and punishing abusers. But victimized children are left with large medical and mental health bills that could continue to increase throughout their lives due to sustained trauma.[44] In addition to the actual costs brought on by this abuse, many victims of CSAM are unable to work full-time because

33. *Id.* at 128.
34. *Id.* at 127.
35. Keller & Dance, *supra* note 25.
36. Binford et al., *supra* note 3, at 127.
37. *Id.*
38. *Id.* at 128.
39. *Id.*
40. 18 U.S.C. § 2259(b)(3) (2012).
41. Binford et al., *supra* note 3 at 127.
42. Cassell, *supra* note 7, at 187.
43. Binford et al., *supra* note 3, at 136.
44. *Id.* at 127, 136.

of their mental health struggles.[45] The U.S. has several victim's restitution schemes meant to compensate victims for harm suffered at the hands of their abusers.[46]

Despite their good intentions, many restitution schemes fall short when it comes to full recovery for victims. One of the earliest victims' restitution laws, the Victim and Witness Protection Act of 1982, allowed victims to recover financially for physical and psychological care.[47] While this law was a big step forward in ensuring that victims can afford to pay for physical and mental health care, it required the presiding judge to consider the financial situation of the defendant before assigning any restitution payments.[48]

Only two years later, Congress passed the Victims Compensation and Assistance Act of 1984, which required states to have a general victims' restitution fund that compensates victims with money collected from criminal fines.[49] However, these funds tend to be only for victims of violent crimes, meaning that victims cannot collect when defendants only possessed or circulated CSAM rather than committing the depicted abuse.[50] These funds seem to be underutilized, with only 200,000 victims collecting from this fund, despite nearly seven million violent crimes occurring per year.[51] These funds may be underutilized because many victims are ineligible to receive them or perhaps victims are not aware that they are entitled to collect.[52] Additionally, these funds are only available for U.S. citizens to collect from U.S.-based criminals.[53] In the case of CSAM, the harm is global, with material depicting American children circulated globally via the Internet, and the same with CSAM depicting foreign children reaching American soil, but neither of these groups can collect from the fund.[54] Even more worrisome, many of these state funds require that the victim reimburse the state if they collect any kind of restitution directly from a defendant.[55]

The Violence Against Women Act, another potential recovery mechanism for victims, includes a Mandatory Victims Restitution Statute (MVRS), codified at 18 U.S.C. § 2259, which makes the discretionary portion of the Victim and Witness Protection Act obsolete, as it requires restitution to

45. Cassell, *supra* note 7, at 187.

46. *See, e.g.*, sources cited *supra* note 13.

47. Victim and Witness Protection Act of 1982, Pub. L. No. 97-291, 96 Stat. 1248 (1982) (codified at 18 U.S.C. § 3664 (2018)).

48. *Id.*

49. 42 U.S.C. § 10691 (2018).

50. Binford et al., *supra* note 3, at 134.

51. *Crime Victim Compensation: An Overview*, NAT'L ASS'N OF CRIME VICTIM COMP. BDS., http://www.nacvcb.org/index.asp?bid=14 (last visited Apr. 18, 2021) [https://perma.cc/8WYZ-5YJM].

52. *See* Douglas Evans, *Compensating Victims of Crime*, JON JAY COLL. CRIM. JUST. 10 (June 2014), http://www.njjn.org/uploads/digital-library/jf_johnjay3.pdf [https://perma.cc/46VP-K3DZ] (explaining that some victim's restitution laws require that victims report the crime within a set amount of time and many do not do so and that studies show that many victims of crimes were never notified of their rights to receive compensation).

53. Binford et al., *supra* note 3, at 134.

54. *Id.*

55. *Id.* at 135.

be paid regardless of the defendant's financial situation or ability to pay.[56] This statute mandates that victims be paid at all levels of the CSAM market, including creation, distribution, and possession, but requires victims to prove that the defendant's actions were a proximate cause of their harm.[57] Congress amended the MVRS in 2018 after many years of attempting to do away with the causation requirement addressed in *Paroline v. United States*.[58] This amendment, the AVAA, removes the proximate cause requirement of the original MVRS.[59] But the statute, like nearly all of the restitution laws, has relatively low minimum compensation compared to most victims' actual financial losses. Thus, some victims are required to litigate hundreds if not thousands of cases to fully recover.[60] If victims of CSAM are able to utilize the copyright system, they could win full financial restitution at faster rates with fewer cases litigated than traditional restitution channels currently allow.

IV. COPYRIGHT BASICS AND MINIMUM REQUIREMENTS FOR PROTECTION

A. Purpose of Copyright Law

The federal government has authority to issue legal protections to authors of creative works through the Intellectual Property Clause of the United States Constitution.[61] This clause, also called the Progress Clause or the Copyright and Patent Clause, allows Congress to "promote the progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[62] Copyright law enables authors of various types of works to reap the benefits of their creative labor, and it also allows authors to exercise control over their work, empowering them to decide when, where, and how their work is publicly displayed or privately held. Just as an author can choose to allow the public to consume their work, an author can decide to exclude anyone from viewing it, if they so desire. Under current copyright law, the owner of the copyright receives protection for the entire life of the author, and then an additional 70 years after the author's death.[63]

56. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 2259, 108 Stat. 1796 (1994) (codified as amended at 18 U.S.C. § 2259 (2018)).
57. *Id.*
58. Cassell, *supra* note 7, at 187.
59. *See* Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299, 132 Stat. 4383 (2018); Cassell, *supra* note 7, at 191.
60. Cassell, *supra* note 7, at 188.
61. U.S. CONST. art. 1 § 8, cl. 8.
62. *Id.*
63. 17 U.S.C. § 302(a) (2018).

B. *Only Original and Fixed Works Are Eligible for Copyright Protection*

The Copyright Act lays out the basic requirements necessary for copyright protection. First, "original works of authorship fixed in any tangible medium of expression," are afforded copyright protection.[64] Section 102(a) of the Copyright Act provides a few examples of protectable works of authorship, including "pictorial, graphic, and sculptural works," as well as "motion pictures and other audiovisual works."[65] Therefore, under this definition, a photograph or video constituting CSAM would be protectable under copyright law, so long as it meets the originality requirement, because photographs and videos are fixed by definition.

1. To Be Eligible for Copyright Protection, a Work Must Be Original

Not all works of authorship are protectable. While the statute does not define originality or offer a threshold for just how original a work needs to be in order to earn copyright protection, the Supreme Court formed a two-part test for determining originality in *Feist Publications, Inc. v. Rural Telephone Service Co*.[66] For a work to meet the originality requirement of the Copyright Act, it must be a work that (1) is "independently created by the author (as opposed to copied from other works)," and (2) "possesses some minimal degree of creativity."[67] Only the parts of a work that the author created can be protected by copyright. The creativity prong is a little murkier, but the Court in *Feist* stated that even a "slight amount," of creativity will suffice, and that "a vast majority of works would make the grade quite easily."[68] The Court then clarified that the work does not have to be innovative or novel; to satisfy the creativity prong, it only must be more than "so mechanical or routine as to require no creativity whatsoever."[69] Works need not be aesthetically pleasing or even what most people would consider good art, because "no matter how crude, humble, or obvious," a work is original so long as it "possess[es] some creative spark."[70] Examples of works that do not meet the modicum of creativity standard are almanacs, phonebooks, and other compilations of facts that are arranged in an obvious way, such as chronologically or alphabetically.[71]

64. 17 U.S.C. § 102(a) (2018).
65. *Id.*
66. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991).
67. *Id.*
68. *Id.* at 346.
69. *Id.* at 379.
70. *Id.* at 345 (quoting 1 M. NIMMER AND D. NIMMER, COPYRIGHT § 1.08(C)(1)(1990)).
71. *See, e.g.*, *id.* at 363.

2. To Be Eligible for Copyright Protection, a Work Must Be Fixed

In addition to the originality requirement of the Copyright Act, there is a fixation requirement.[72] Most traditional types of expression are fixed by definition. A book is printed on paper. A movie is recorded on film, and a song is copied onto a disc. Photographs and videos meet the fixation requirement once they are taken, whether on film or digitally.[73]

V. CONTENT NEUTRALITY AND COPYRIGHT OF ILLEGAL OR OBSCENE WORKS

While no abuser has tried to assert copyright ownership of the abuse imagery they created (likely due to obvious implication of criminal liability), CSAM is eligible for copyright protection based on the text of the Copyright Act. CSAM typically consists of photographs and videos that qualify as original works of authorship as defined by the Copyright Act. Despite how disconcerting it is to consider, the likelihood that child pornography would meet the minimal creativity standard is high, partly because the bar for creativity is so low, but also because the technical aspects required to frame up a photograph or video are minimally creative.[74] The statute alone provides no reason to deny CSAM at least thin copyright protection, the protection against literal reproduction of the work.

Although CSAM meets the basic requirements to gain copyright protection, there is a more important question: should copyright protection be made available for works that are repugnant to moral decency and public policy? Should something as despicable as CSAM earn protection of the federal government in some instances (copyright), but otherwise trigger heavy (and well deserved) criminal penalties in others? The purpose of copyright law is, among other things, to encourage creativity and foster a free flow of information.[75] Protecting CSAM does neither of those things, so it is an open question whether the aforementioned benefits to victims outweigh compromising copyright law's basic purpose.

The Supreme Court has never heard a case in which someone tried to enforce copyright protection for a per se illegal work, such as child pornography, but it has heard a few cases regarding copyright of other morally questionable works of authorship.[76] Scholars, too, have written about the benefits and detriments of a content neutral copyright system and the

72. 17 U.S.C. § 102(a) (2018).
73. 17 U.S.C. §§ 101–02(a) (2018).
74. Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 60 (1884).
75. U.S. CONST. art. 1 § 8, cl. 8.
76. *See generally* Mitchell Bros. Film Grp. v. Cinema Adult Theater, 604 F.2d 852 (5th Cir. 1979); Jartech, Inc. v. Clancy, 666 F.2d 403 (9th Cir. 1982).

implications of allowing protection for illegal and immoral works.[77] Although the Copyright Office only needs to consider whether material is an "original work of authorship fixed in any tangible medium of expression,"[78] for many years, examiners followed instructions to deny applications for registrations of illegal works if the examiner knew the content of the work was illegal.[79] This changed in 1959, when the Attorney General decided that refusal of registration on the grounds of illegality was no longer mandatory, but instead at the discretion of the examiner.[80] Until 1979, courts usually held that illegal works were never eligible for copyright protection and denied plaintiffs remedies.[81] The ambiguity of illegal works' eligibility to gain copyright protection began in 1979 when the Fifth Circuit held otherwise in *Mitchell Bros. Film Grp. v. Cinema Adult Theater*.[82] In *Mitchell Bros.*, the court held that a pornographic film was copyrightable whether or not it was considered obscene.[83]

After *Mitchell Bros.*, other circuit courts considered the same question. The Ninth Circuit followed suit in *Jartech, Inc. v. Clancy*, holding that obscene (and therefore illegal) material is copyrightable and the obscenity of the material is not a defense to infringement.[84] But the Second Circuit declined to follow the Fifth and Ninth Circuits due to "strong public policy" arguments against copyright protection for obscene material.[85] The Second Circuit explained that its decision intended to stop the distribution of obscene material and to avoid benefitting the plaintiffs—the creators of the material.[86] Perhaps the court would have ruled differently if the case intended to cease and discourage the distribution of obscene material and punish the creators of that material. Additionally, the Seventh Circuit, while not deciding on the issue, recognized that "the prevailing view is that even illegality is not a bar to copyrightability."[87] Based on this precedent, it would seem that child pornography is eligible for copyright protection and that a court would likely enforce the rights of the owner, and in the case of CSAM, an abuser, in an infringement suit. This is likely not an issue in CSAM cases because the creators of any CSAM would incriminate themselves and any network of other creators they may have built by identifying themselves as authors of illegal child pornography. But if a victim registered their copyright like Amy, the victim in *Paroline*, it seems likely that a court would hear and rule on an infringement suit.

77. *See, e.g.*, Eldar Haber, *Copyrighted Crimes: The Copyrightability of Illegal Works*, 16 YALE J.L. & TECH. 454 (2014).
78. 17 U.S.C. § 102(a) (2012).
79. Haber, *supra* note 77, at 463–64.
80. *Id.*
81. *Id.* at 465.
82. *Mitchell Bros*., 604 F.2d at 852.
83. *Id.* at 854, 858.
84. Jartech, Inc. v. Clancy, 666 F.2d 403, 408 (9th Cir. 1982).
85. Devil Films, Inc. v. Nectar Video, 29 F.Supp. 2d 174, 176–77 (S.D.N.Y. 1998).
86. *Id.*
87. Haber, *supra* note 77, at 466 (citing FlavaWorks, Inc. v. Gunter, 689 F.3d 754, 755 (7th Cir. 2012)).

On the other hand, without any kind of content-based restrictions, granting federal protection to illegal works could be seen as the federal government endorsing or rewarding these works.[88] This issue can be solved by amending the Copyright Act so that immediately upon creation, the ownership rights of CSAM vest in the minor victim or victims depicted rather than the creator, so government never endorses these illegal materials, and the creator can never benefit from the material.

Additionally, one of the main reasons why having a content-neutral copyright system is so important is because we value free speech so highly and denying protection for some works and not others can be a constitutional violation of a creator's First Amendment free speech rights and prevents the free flow of information. Even if the prospect of content-based copyright registration draws concerns by those strongly in favor of free speech, it should not for CSAM cases because the Supreme Court has held that child pornography is not speech.[89] Still, restricting any material sends the message that our copyright scheme is not content-neutral and undermines the purpose of the Copyright Act.

VI. BENEFITS TO VICTIMS BY UTILIZING COPYRIGHT OWNERSHIP

Despite the queasy feeling that may come from the idea of enforcing copyrights of illegal works, specifically CSAM, the benefits that stem from doing so for victims are great. Victims would have more control of their abuse material and would have a streamlined process for recovering damages that current criminal victims' restitution statutes fail to provide.

A. Rights Protected Under Copyright Law

Once an original work has been fixed, it has copyright protection.[90] There are six rights included in that protection, each defined in Section 106 of the Copyright Act.[91] Whomever owns a copyright has the exclusive right to do or authorize any of the following: (1) "reproduce" the work; (2) "prepare derivative works" based on the work; (3) "distribute copies" of the work to the public by sale or any other transfer; (4) publicly perform the work; (5) publicly display the work; and (6) "perform the work publicly by means of digital audio transmission."[92] This Note is primarily concerned with reproduction, distribution, display, and performance rights. The owner of a copyright is the only one that legally can make copies of their work unless they authorize another to do so.[93] Reproducing a work includes anything from

88. *Id.* at 484.
89. New York v. Ferber, 458 U.S. 747, 779–80 (1982).
90. 17 U.S.C. § 102(a) (2018).
91. 17 U.S.C. § 106 (2018).
92. *Id.*
93. 17. U.S.C. § 106.

making a literal copy on a copy machine to downloading a photo to a computer or other digital storage device.[94] Distribution means selling but also lending or circulating.[95] Displaying or performing the work publicly can mean posting it on a website or even showing others physical copies at home, depending on who was invited.[96]

B. Remedies Afforded to Copyright Owners Upon Infringement

Once the owner of a copyright finds that someone infringed their copyright, they can bring suit in federal court.[97] If a court finds infringement, there are a few remedies that will typically be awarded, namely damages and injunctions.

1. Damages

Damages in copyright law come in two forms, actual and statutory. Copyright owners are entitled to the actual damages suffered from the actions of the infringer, most often lost profits.[98] However, actual damages may be small and, similarly to victim's restitution law, the harm can be difficult to prove, so there is another choice. If the copyright was already registered at the time the infringement occurred, the copyright owner can receive statutory damages, which can range from no less than $750 and up to $30,000 per work infringed, at the discretion of the judge.[99] The judge will determine the award amount based on several factors, including financial benefit to the defendant as a result of the infringement, the relative innocence or willfulness of the defendant when infringing, and deterrent to other potential infringers.[100] If a fact finder decides that a defendant truly was innocent and had no knowledge that the work was under copyright protection, the damage award may be lowered to $200 per work infringed.[101] On the other hand, if a court finds willful infringement, "the court in its discretion may increase the award . . . to a sum of not more than $150,000."[102] The Second Circuit created a test to determine willfulness in *Island Software & Computer Serv. v. Microsoft Corp.*[103] To prove willful infringement the defendant (1) must have been aware of the fact that their activity was infringing, and (2) must have acted in

94. 17 U.S.C. § 101 (2018).
95. 17 U.S.C. § 106(3).
96. 17 U.S.C. § 101. Public display or performance for the purpose of copyright is defined as either showing or performing the work in any place open to the public where a substantial number of persons outside of a normal circle of a family and its acquaintances are gathered; or transmitting or communicating the work to a place that is open to the public or to many people at one time even if they are not in the same place.
97. 17 U.S.C. § 501(b) (2018).
98. 17 U.S.C. § 504.
99. 17 U.S.C. §§ 411(a), 504(c) (2018).
100. Island Software & Comput. Serv. v. Microsoft Corp., 413 F.3d 257, 263 (2d Cir. 2005).
101. 17 U.S.C. § 504(c)(2).
102. *Id.*
103. *Island Software & Comput. Serv.*, 413 F.3d at 257.

"reckless disregard for, or willful blindness to, the copyright holder's rights."[104]

While not guaranteed, the odds of getting greater payments from copyright remedies than from victim's restitution laws are high because the damage award is calculated per individual image.[105] For example, if someone possessed 50 different images of Amy, under the AVAA,[106] she would get varying amounts of restitution depending on how the judge in each specific case decides. There is a chance that a judge would order a large restitution award, but the guarantee is only $3,000.[107] If she were to sue the possessor for copyright infringement and opt for statutory damages, then she would be guaranteed a minimum of $10,000 (50 different images multiplied by the statutory damages minimum of $200) or more if a judge deemed the infringement to be willful or especially egregious.[108] Based on this difference alone, the benefits of suing under Title 17 to recover would be vast for victims of CSAM, especially victims like Amy, whose abuse imagery is extensive and widespread.

2. Removal Under the Digital Millennium Copyright Act

Similar to an injunction, under the DMCA, a copyright owner can issue take-down notices to websites that display the owner's copyrighted work.[109] Many content-hosting websites fall under a safe harbor exception in the DMCA, shielding them from contributory infringement claims.[110] If a website is a safe harbor and one of its users posts infringing material on the website, only the user can be sued for copyright infringement, and the website gets protection.[111] To keep its safe harbor status, a website must (1) not actually know or have reason to know that there is infringing material on their site and must act expeditiously to remove the material upon becoming aware or knowledgeable of the infringement; (2) not receive financial benefit that is "directly attributable to the infringing activity" if the site "has the right and ability to control" the activity; and (3) upon receiving a take-down notice, the site must comply with such notice quickly.[112] If a content-hosting website does not obey these provisions, a court will likely remove its safe harbor status, and a copyright holder may sue the website for contributory or vicarious infringement.

104. *Id.* at 263.
105. 17 U.S.C. § 504(c).
106. 18 U.S.C. § 2259 (as amended 2018).
107. *Id.*
108. 17 U.S.C. § 504.
109. 17 U.S.C. § 512(c)(3) (2012).
110. 17 U.S.C. § 512(c)(1).
111. *Id.*
112. 17 U.S.C. § 512(c)(1).

C. *Technology Exists to Detect Infringement and Send Take-Down Notices to Copyright Infringers, Meaning Victims Could Find and Sue Infringers Through Copyright Attorneys Without Ever Appearing in Court*

There are programs that catch both copyright infringement and child pornography, so if an attorney or nonprofit could take charge of policing victim-owned CSAM copyright, the victim would not need any contact with defendants or CSAM.[113] Once the abuse imagery is uploaded into the system, these programs scan the Internet for exact reproductions of the imagery, inform the owner of apparent infringing activity, and send take-down notices to the infringers.[114] This creates a possible benefit to victims that stems from their ability to control and affirmatively police their own abuse via the DMCA. There may be some power that comes from literally owning your own abuse material.[115]

VII. UNDER CURRENT COPYRIGHT LAW, VICTIMS CAN NEGOTIATE WITH THEIR ABUSERS FOR OWNERSHIP OF THE COPYRIGHT IN THEIR ABUSE IMAGES, BUT THIS IS UNCERTAIN AND CAN BE PSYCHOLOGICALLY DAMAGING TO VICTIMS

In *Paroline*, Amy's attorney negotiated with her abuser for copyright of Amy's abuse images.[116] There is no evidence that suggests this was an easy process, but Amy ultimately succeeded. Other victims may not have as much luck. Currently, this method of restitution is still new and has not been regularly used, so it may be easier than ever for victims to acquire the copyright ownership in this way. It is possible that many abusers see no value in the copyright, either because they believe it is not enforceable or because registering and enforcing a copyright would publicize their conduct and draw attention to them. Perhaps they would quickly dispose of the ownership for a lesser restitution payment, but it is likely that many abusers would keep the copyright because the victims have very little bargaining power.

Such negotiations could be detrimental to the victims because concessions in negotiation could compromise their potential restitution. The negotiation process could also be emotionally taxing, and litigation costs could be high, leading victims to dismiss the process altogether. Another problem with this solution is the termination right of creators. The original

113. *New Technology Fights Child Porn By Tracking Its "PhotoDNA"*, MICROSOFT, (Dec. 15, 2009) https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/#sm.0001mpmupctevct7pjn11vtwrw6xj [https://perma.cc/D3JA-MCQK].

114. *Id.*

115. Binford et al., *supra* note 3, at 154.

116. *Id.*

owner of the work, the author, has a right to terminate any transfers.[117] This means that roughly 35 years after negotiating with an abuser, the abuser has the right to terminate the transfer, taking back ownership of the copyright.[118] Because victims' images likely will live on the Internet and continue to be viewed forever, a time limit of 35 years diminishes full restitution for victims.

While negotiating for the copyright of the material could be a valuable tool for victims that have previously been abused, a few amendments to the Copyright Act would allow future victims copyright ownership of their abuse images from the moment the material is created and do away with many of the problems faced in the negotiation process.

VIII. AMENDING THE COPYRIGHT ACT WOULD ALLOW CSAM VICTIMS TO ACHIEVE FULL FINANCIAL RECOVERY FROM THOSE WHO POSSESS THEIR ABUSE IMAGERY

The amendments proposed in this section are not an excuse for Congress to avoid adjusting the minimum awards for victims in CSAM cases. Ultimately, congressional action is the most efficient and unconvoluted way for victims to financially recover fully. Amending the Copyright Act is less direct but could still ultimately lead to stronger victim financial recovery. Full recovery of monetary damages may allow victims to get the best care for the other harm they suffered at the hands of their abusers, and ultimately lead them to begin recovering from the abuse completely. Among the direct benefits to the victims of these crimes, there are policy and administrability benefits to the government as well. Higher damage awards may act as an even greater deterrent to potential abusers leading to fewer abused children, and greater damages awards allow victims to litigate fewer cases to be able to recover fully, which will lighten the burden on the court system.

Restitution is a tricky balancing act of the rights of victims to be free from the financial burden the defendant placed on them and the rights of the defendant to avoid punishment beyond his wrongdoing, which is why nearly every restitution scheme requires victims to prove how the defendant directly caused their harm. There may be issues with overburdening defendants with forcing them to pay copyright infringement damages, but the benefit provided to the victims, the probable deterrence to future abusers, and the fewer overall suits brought by victims limiting the strain on the court system would outweigh the harm to defendants.

Therefore, Congress should amend the Copyright Act with three minor changes to make it easier for CSAM victims to litigate claims of copyright infringement.

117. 17 U.S.C. § 203(a)(3) (2012).
118. *Id.*

A. Amending the Definition of Authorship for Works Relating to 18 U.S.C. §§ 2251 and 2252 So Ownership of Copyright in CSAM Initially Vests in the Minor(s) Depicted

The first suggested change is to amend the definition of authorship in Section 201(a) of the Copyright Act, which says that copyright ownership "vests initially in the author or authors of the work."[119] Instead, it should include a clause at the end, providing that "in works relating to 18 U.S.C. §§ 2251–52,[120] the author shall be defined as the minor child or children depicted in the work."

Ownership of a copyright in a work initially vests in the author of the work.[121] For the purpose of copyright law, "author" does not just mean someone who wrote a book, but instead it is a general term referring to the creator of any type of work that is protected by copyright.[122] The Copyright Act does not define what makes someone an author, but case law illustrates that the author is typically one who physically created the work or the one who had control over the work's creation, even if they did not literally create the work.[123]

Although ownership initially vests in the author, the author can transfer their ownership rights to anyone at any time in the duration of the work's protection, but such transfers must be made in writing.[124] Any grants of ownership made by the author can be terminated (that is, the ownership will be returned to the author) about 35 years after the initial transfer.[125] Termination of the grant is not automatic. The author, or the author's heirs, must file a notice of termination with the Copyright Office and the grantee in order to have the ownership returned, but once that is done, the grant is terminated, and all ownership rights revert to the author or the author's surviving family.[126]

By ensuring that the copyright ownership of the abuse imagery initially vests in the minor victim(s) depicted rather than the person who took the photograph, the victim is protected from ever having to negotiate with their abuser and having their copyright ownership terminated.

---

119. 17 U.S.C. § 201(a) (2018).

120. *See generally* 18 U.S.C. §§ 2251–52. These are the relevant child sexual abuse production and distribution statutes. By specifically naming these in the amendment, the amendment only applies to works involving child sexual abuse so as to not upend the copyright system by making *any* child depicted in a work the author of the work.

121. 17 U.S.C. § 201(a).

122. The Copyright Act does not define "author." It is a general term for the creator of all types of works eligible for copyright protection throughout the statute. *See e.g.*, 17 U.S.C. §§ 101, 103(b), 201 (2012).

123. *See* Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 737 (1989); Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 58 (1884).

124. 17 U.S.C. §§ 201(d), 204(a) (2018).

125. 17 U.S.C. § 203(a)(3) (2018).

126. 17 U.S.C. § 203(a)(2)–(4), 203(b).

B. Amending the Ability to Terminate Transfers

The second change involves amending Section 203(a), which provides that an author can terminate any grants of ownership rights starting 35 years after the transfer.[127] Congress could add a provision, Section 203(a)(6),[128] that reads "in works relating to §§ 2251–52, there shall be no right of termination." This amendment would not affect victims after the enactment of the first amendment, which would establish the minor as the author. But the additional limitation on terminations of transfers would be important to victims who are required to negotiate with their abusers for the copyright to existing abuse materials, as the new limitation would prevent abusers from reclaiming the copyright in 35 years.

C. Amending the Registration Prerequisite for Statutory Damages and Attorney's Fees

The third and final amendment is to the damages portion of the Copyright Act, Section 412. Currently, Section 412 provides that no statutory damages or attorney's fees shall be awarded for "any infringement . . . commenced after first publication of the work and before the effective date of its registration,"[129] meaning that a copyright must be registered when the infringement happens in order to collect statutory damages. Statutory damages require no proof of how the infringement harmed the owner, and thus are the best choice of damages for CSAM victims. Additionally, registration requires a deposit of two copies of the work with the Library of Congress.[130] Because of the illegal nature of CSAM, the act of sending the work to the Library of Congress is in violation of federal child pornography laws, making registration difficult.[131]

Registration is voluntary and ancillary to copyright protection.[132] Registration is optional but still important because it requires a deposit of the work with the Library of Congress, allowing the government to keep track of creative works and providing citizens with access to these works.[133] Because society generally does not see any creative value in CSAM, the benefit of the deposit created by registration is moot. An amendment to Section 412 providing that "in cases relating to 18 U.S.C. § 2251-52, there shall be no registration prerequisite for an award of statutory damages and attorney's

127. 17 U.S.C. § 203(a).

128. It is important here to note that 17 U.S.C. § 203(a) already includes subsections (1)–(5), and the proposed amendment would simply be added to the end as subsection (6).

129. 17 U.S.C. § 412 (2012).

130. 17 U.S.C. § 408(b) (2018).

131. 18 U.S.C. § 2252(a)(1) (2018).

132. 17 U.S.C. § 408(a).

133. U.S. COPYRIGHT OFFICE,: MANDATORY DEPOSIT OF COPIES OR PHONORECORDS FOR THE LIBRARY OF CONGRESS (2019), https://www.copyright.gov/circs/circ07d.pdf [https://perma.cc/K5SE-T7LJ].

fees" would allow victims to sue for statutory damages from the creation of the material, not just registration.

There could be many years between the creation of the material and the victim acknowledging the abuse or law enforcement identifying the abuse. In this time, many people could commit copyright infringement on the victim's abuse imagery, but he or she would not be able to collect damages from those infringers under the current statute. The amendments in this Note would change that.

IX. CONCLUSION

Under current criminal restitution law, it is almost impossible for victims of CSAM to fully recover financially from their abuse due to insufficient restitution. But copyright law, with a handful of statutory fixes, could be a better avenue. By allowing victims of CSAM to register their abuse images and bring suit for copyright infringement against those who possess and distribute those images, victims will be able to fully recover financially from their abuse at faster rates with fewer cases litigated. These changes would not stray far from copyright doctrine while also empowering victims with a new tool to stop the horrors of CSAM.

Debugging the System: Reforming Vulnerability Disclosure Programs in the Private Sector

Jasmine Arooni*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; B.A., Political Science & Entrepreneurship, The University of California, Los Angeles (UCLA). Thank you to the dedicated Federal Communications Law Journal staff for bringing this Note to publication. Special thanks to Meredith Rose, Journal Adjunct, and Atena Sheibani-Nejad, Notes Editor, for their patience and encouragement from start to finish. I would also like to express my gratitude to Professor Daniel J. Solove for his guidance during the writing process and mentorship throughout my law school career. Finally, many thanks to my family for their unconditional love and support.

I. INTRODUCTION

Virtually everything is hackable in today's interconnected world.[1] While a surge of technological advancement confers numerous benefits, it also brings an increased risk of software vulnerabilities.[2] Vulnerabilities are weaknesses in software, including online systems, that can be exploited to damage the confidentiality, integrity, or availability of those systems.[3] Vulnerabilities pose risks of aftermarket exploitation, often in the form of data breaches perpetrated by malicious actors.[4] Remediation of a data breach, on average, costs $3.92 million.[5]

A Vulnerability Disclosure Program ("VDP")[6] is an increasingly popular method to mitigate vulnerability-related risks.[7] VDPs involve enlisting "hackers" (referred to in this Note as "security researchers" for neutrality), to find vulnerabilities before weaknesses can be exploited. Security researchers, in turn, are compensated for their efforts. The cost of paying researchers through a VDP is a small fraction of what it costs to remediate a data breach, as the average VDP payout is $2,041.[8]

In an age where organizations of all shapes and sizes depend on software-based technologies, addressing vulnerabilities quickly is at the crux

1. *See* Roger A. Grimes, *Everything Is Hackable-and Cyber Criminals Can't Be Tracked*, CSO (May 10, 2011), https://www.csoonline.com/article/2621721/everything-is-hackable----and-cyber-criminals-can-t-be-tracked.html [https://perma.cc/K2NV-42D7].

2. *See* AWARENESS AND ADOPTION GRP., NAT'L TELECOMM. & INFO. ASS'N, VULNERABILITY DISCLOSURE ATTITUDES AND ACTIONS 3 (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf [https://perma.cc/MV8H-ETFX].

3. *Id.*

4. *See* ALLEN D. HOUSEHOLDER ET. AL, CARNEGIE MELLON UNIVERSITY, THE CERT GUIDE TO COORDINATED VULNERABILITY DISCLOSURE, SOFTWARE ENGINEERING INSTITUTE 2 (2017), https://resources.sei.cmu.edu/asset_files/specialreport/2017_003_001_503340.pdf [https://perma.cc/7DH4-PEYL].

5. *See* IBM SEC., COST OF A DATA BREACH REPORT 18 (2019), https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf [https://perma.cc/3YAM-D23K].

6. It is important to distinguish the difference between bug bounty programs (BBP) and vulnerability disclosure programs (VDP). A VDP is when a host organization (vendor) invites ethical white hat hacks to explore the organization's systems and report the discovered vulnerabilities to the organization. BBP is a form of VDP by which the organization provides monetary or other incentives for responsibly discovering and reporting vulnerability information. For the purposes of this Note, VDPs and BBPs are referred to collectively as VDPs.

7. *See* LUCA ALLODI & JUKKA RUOHONEN, A BUG BOUNTY PERSPECTIVE ON THE DISCLOSURE OF WEB VULNERABILITIES 1 (2018), https://arxiv.org/pdf/1805.09850.pdf [https://perma.cc/B4C6-RC65].

8. *See* Matt Honea, *Safe Harbor Programs: Ensuring the Bounty Isn't on White Hat Hackers' Heads,* DARK READING, (Apr. 10, 2019), https://www.darkreading.com/application-security/safe-harbor-programs-ensuring-the-bounty-isnt-on-white-hat-hackers-heads/a/d-id/1334339 [https://perma.cc/H4KE-AXFC].

of maintaining an effective security posture.[9] The growing popularity of VDPs indicates that crowdsourced bug discovery brings cost-effective solutions that may surpass in-house security strategies to address vulnerabilities. Organizations that run VDPs ("host organizations") delegate the probing of their internal systems to security researchers who perform testing remotely.[10] By harvesting the potential of security research through VDPs, host organizations may establish scalable solutions to cybersecurity challenges.[11] VDPs provide for around-the-clock security services due to their remote and global nature and may replace or supplement the otherwise-burdensome process of in-house vulnerability management.[12] Today, security research is a vital element of the cybersecurity industry, helping strengthen host organization systems used by billions worldwide.[13]

However, security researchers worry about the legal implications of their VDP participation given the realistic possibility that legal action may follow from conducting research outside of the technical or contractual scope allotted by a host organization.[14] Anti-hacking laws in the U.S., combined with an industry standard of poorly drafted legal terms in private sector VDPs, create a prohibitive and liability-laden environment for security researchers.[15]

Some VDPs offer rewards for vulnerabilities that require researchers to conduct research in direct violation of their legal terms, a practice that violates anti-hacking laws.[16] The search for a specific vulnerability solicited by the host organization might involve research that, under the organization's legal terms, is a violation or not clearly defined as proper or improper activity.[17] In turn, inconsistent or incomplete legal terms can subject a security researcher to the risk of prosecution under current anti-hacking laws in violation of those terms.[18] These poorly drafted terms force researchers to bear the risk. They

9. *See generally* Press Release, BugCrowd, Bugcrowd Announces Industry's First Platform-Enabled Cybersecurity Assessments for Marketplaces (Aug. 6, 2019), https://www.bugcrowd.com/press-release/bugcrowd-announces-industrys-first-platform-enabled-cybersecurity-assessments-for-marketplaces/ [https://perma.cc/3HZ5-CV5H].

10. *Id.*

11. *See* David A. Newman, *Bug-Bounty Programs: A Valuable Tool to Be Used Carefully*, MORRISON FOERSTER (Feb. 18, 2018), https://www.mofo.com/resources/insights/180220-bug-bounty-programs.html [https://perma.cc/Z7EG-9NEU].

12. *See* ALLODI & RUOHONEN, *supra* note 7, at 3.

13. *See The Importance of Security Research: Four Case Studies*, CTR. FOR DEMOCRACY & TECH. (Dec. 2017), https://cdt.org/files/2017/12/2017-12-15-Importance-of-Security-Research.pdf [https://perma.cc/KNC5-VRND].

14. *See* Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. Rev. 383, 397 (2014) (explaining that not all hacking is created equal, as nearly all hacking under bug bounty programs may be illegal if a program's contractual language is not properly crafted).

15. *See* J.M. Porup, *Do You Need A Vulnerability Disclosure Program? The Feds Say Yes*, CSO (Aug. 7, 2018), https://www.csoonline.com/article/3294418/do-you-need-a-vulnerability-disclosure-program-the-feds-say-yes.html [https://perma.cc/P9HS-EH92].

16. *See generally id.*

17. *Id.*

18. *Id.*

must decide their willingness to participate in a program that may not protect them from liability should their research be construed as improper.[19]

To this end, the U.S. federal government has made numerous guiding efforts, one of them being the Department of Justice's "Framework for a Vulnerability Disclosure Program for Online Systems," while simultaneously setting an example in its capacity as a host organization towards reform of the volatile VDP landscape in favor of security researchers.[20] The DOJ Framework outlines a high-level process for how an organization may structure a vulnerability disclosure program and advises host organizations on how to eliminate civil or criminal prosecution risk for security researchers that may arise from a poorly drafted policy.[21] Although the government is thought to lag behind innovative private sector companies in stature, federal agencies, unexpected first-adopters of fair VDP practices, have set the example for how organizations should operate VDPs.[22]

Several organizations in the private sector have taken public steps to reform their VDPs based on the DOJ's helpful guidance. However, after three years since the DOJ Framework's release, it has not had enough of an impact on private sector VDP reform. Given the changing landscape of U.S. government-run VDPs, which captures adequate process and protections for agency VDPs, this Note argues that there should be top-down pressure on the private sector to reform VDP policies and processes, using the DOJ's framework as a tool to do so.

Section I of this Note sets forth the VDP process, including actions taken by the host organization and researchers during VDP creation and the vulnerability lifecycle. Section II explores the current anti-hacking legal landscape and its impact on security research, including the role of safe harbor language. Section III explores the DOJ Framework in detail, highlighting why it is a useful tool towards reducing legal risks to security researchers through private sector VDP reform. Section IV outlines the U.S. government's unconventional adoption of VDPs, the recent call for mandatory and uniform VDPs at every government agency, and the influence the government has on private sector VDPs seen through commercial VDP platforms. Section V proposes that the DOJ Framework, if properly updated and maintained through a multi-stakeholder approach, has the potential to facilitate comprehensive standards in private sector VDPs, using the government's role in the VDP industry as used an exemplary metric that comports with the needs of both host organizations and security researchers alike.

---

19. *Id.*

20. *See generally* U.S. DEP'T OF JUST., A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS (2017), https://www.justice.gov/criminal-ccips/page/file/983996/download [https://perma.cc/3C9X-NKUR] [hereinafter *DOJ Framework*].

21. *Id.*

22. *See* Dan Lohrmann, *Why Offering Bug Bounties Will Be Widespread, Even in Government*, GOV'T TECH., (July 16, 2017), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-offering-bug-bounties-will-be-widespread-even-in-government.html [https://perma.cc/7LXX-S7CY].

II. VULNERABILITY DISCLOSURE PROGRAMS IN PRACTICE: HOW DO THEY WORK?

Organizations most commonly utilize their permanent security operations teams to handle a range of cybersecurity issues in-house.[23] However, addressing vulnerabilities is a time and resource-intensive practice, and an organization aiming to employ long-term, preemptive measures to discover vulnerabilities may face challenges when trying to do so solely through in-house security.[24] For example, few organizations have adequate bandwidth to look for new bugs while mitigating existing ones.[25] Depending on the size of an organization or the number of systems under its ownership, vulnerability-related security issues may generate enough work for an entire business unit within the organization.[26] As a result, there is great incentive for organizations to encourage, reward, and develop relationships with external researchers who find security bugs in organizations' systems in real-time through VDP deployment.[27] When vulnerability hunting is left to a large and global community of external researchers, internal teams can better focus on fixing existing bugs, creating systems to better avoid bugs in the future, and handling other issues within the organization's security infrastructure.[28]

The VDP process ordinarily begins when an organization solicits security research services from the public by setting up an internal VDP.[29] The VDP creation process may vary in formality based on an organization's size, resources, and sophistication.[30] In creating a VDP, host organizations draft and enforce program terms and legal terms ("legal terms"),[31] which effectively serve as contracts between the security researcher and host

23. *See* MCKINSEY & CO., PERSPECTIVES ON TRANSFORMING CYBERSECURITY 20 (2019), https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx [https://perma.cc/WZ8V-965A].

24. *See* Thomas Maillart et al., *Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond With Bug Bounty Programs*, 2 J. OF CYBERSECURITY 81, 88 (2017).

25. *See* Vincent Smyth, *Vulnerability Intelligence*, BCS, (Apr. 4, 2017), https://www.bcs.org/content-hub/vulnerability-intelligence/ [https://perma.cc/52CF-BANF].

26. *Id.*

27. Maillart et al., *supra* note 24, at 81.

28. *See* JASON PUBAL, SANS INSTITUTE INFORMATION SECURITY READING ROOM, BUG BOUNTY PROGRAMS: ENTERPRISE IMPLEMENTATION 2 (2020), https://www.sans.org/reading-room/whitepapers/application/bug-bounty-programs-enterprise-implementation-38250 [https://perma.cc/NF62-QQYU].

29. *See* J.M. Porup, *Bug Bounty Platforms Buy Researcher Silence, Violate Labor Laws, Critics Say*, CSO, (Apr. 2, 2020), https://www.csoonline.com/article/3535888/bug-bounty-platforms-buy-researcher-silence-violate-labor-laws-critics-say.html [https://perma.cc/4YGM-EDPP].

30. *Id.*

31. Program terms often include terms technical and instructional in scope, with formal legal terms included as part of the larger program terms. This Note collectively refers to host organization program terms and legal terms as "legal terms."

organization.[32] In general, security researchers take affirmative actions to manifest assent to contract terms upon submission of a vulnerability to a host's VDP, as well as click-through consent if they agree to a program's general program terms.[33]

The next step occurs when a security researcher discovers a vulnerability in the host organization's system.[34] After discovering a vulnerability, the security researcher reports the vulnerability to the host organization through the VDP.[35] If a security researcher discovers a valid bug, the company's legal terms dictate the next steps in the process regarding what the security researcher can do with their findings.[36] Some host organizations may allow for public disclosure of security research findings, with a prevailing norm that security researchers work closely with host organizations ahead of time to ensure remediation of the vulnerability before public disclosure to avoid unwanted exploit of the vulnerability found in good faith.[37] Other host organizations require confidentiality from security researchers to avoid reputational harm, a practice generally disfavored by the VDP community because host organizations may fail to capture the extent to which confidentiality is required.[38] Some security researchers may choose to publicly disclose a vulnerability without the permission of the host organization, a decision that comes with legal risks.[39] Researchers' risk tolerance often comes down to reputation and reward.[40]

Host organizations reward security researchers for their findings through recognition, professional opportunities, and monetary compensation—the "bounty" in the bug bounty program.[41] Many host organizations pay significant monetary rewards to researchers who discover

32. *See generally* Amit Elazari, *Hacking the Law: Are Bug Bounties a True Safe Harbor?*, ENIGMA, (Jan. 18, 2018), https://www.usenix.org/conference/enigma2018/presentation/elazari [https://perma.cc/9AC4-JY33] (video explaining importance of contractual terms in VDPs).

33. *See* Nguyen v. Barnes & Noble. Inc., 763 F.3d 1171 (9th Cir. 2014) (finding that browse-wrap contracts are generally enforceable in U.S. if sufficient notice is given); *See* RYAN ELLIS AND VIVEK MOHAN, REWIRED: CYBERSECURITY GOVERNANCE 252–53 (Ryan Ellis et al., eds., 2019).

34. *See* HOUSEHOLDER ET. AL., *supra* note 4, at 29.

35. *Id.*

36. *Id.* at 42.

37. *See id.* at 43; *see* Porup, *supra* note 29.

38. *See* Porup, *supra* note 29.

39. *See* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 797 (2016).

40. *Id.* at 818.

41. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1061 (2011).

and disclose vulnerabilities in their systems.[42] According to HackerOne,[43] a VDP coordination service that connects security researchers to host organizations, security researchers earned almost $40 million in monetary rewards through the HackerOne platform alone in 2019, with six hackers surpassing $1 million in lifetime earnings.[44] More competitive programs run by companies like Google, Apple, and Microsoft offer individual bounties up to $1.5 million for critical issues.[45]

According to Kesan and Hayes, "[R]eputation is practically a currency in the information security field. Being known as the person who discovered a major security flaw might prove as valuable as being paid in legal currency."[46] Though some security researchers may bear legal risks in pursuit of recognition or reward, such risk tolerance is rarely sustainable, as organizations have a practice of suing or threatening to sue researchers who discover vulnerabilities in their systems, using broad anti-hacking laws to compel researcher fear and silence.[47]

III. THE CURRENT LEGAL LANDSCAPE: LEGAL RISKS FACED BY VDP SECURITY RESEARCHERS

The Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA) are the primary laws that make up the anti-hacking legal landscape.[48] U.S. anti-hacking laws impose criminal and civil liabilities on certain forms of computer hacking to protect users, organizations, and government from malicious actors.[49] While anti-hacking

42. *See, e.g.*, *Chrome Vulnerability Reward Program Rules*, GOOGLE APPLICATION SEC., https://www.google.com/about/appsecurity/chrome-rewards/ (last visited Apr. 18, 2021) [https://perma.cc/QK69-3L77] ("Rewards for qualifying bugs typically range from $500 to $150,000. We have a standing $150,000 reward. . . ."). A bug bounty program is synonymous to a vulnerability disclosure program (VDP) as used in this context.

43. HackerOne is one of several commercial bug-bounty management platforms which help organizations build and maintain bug bounty programs. *See Company*, HACKERONE, https://www.hackerone.com/company (last visited Apr. 18, 2021) [https://perma.cc/ZEQ6-ND2W].

44. *See The Hacker-Powered Security Report 2020,* HACKERONE (Feb. 23, 2020), https://www.hackerone.com/resources/reporting/the-2020-hacker-report [https://perma.cc/6WRC-Y6WT]; *see Six Hackers Break Bug Bounty Record, Earning Over $1 Million Each On Hackerone*, HACKERONE, (Aug. 29, 2019), https://www.hackerone.com/press-release/six-hackers-break-bug-bounty-record-earning-over-1-million-each-hackerone [https://perma.cc/6S24-PKMJ].

45. *See Six Hackers Break Bug Bounty Record, Earning Over $1 Million Each On Hackerone*, *supra* note 44.

46. *See* Kesan & Hayes, *supra* note 39, at 794.

47. *See* Porup, *supra* note 29.

48. *See generally* 18 U.S.C. § 1030(a) (2012); 17 U.S.C. § 1201(a)(1)(A) (2012); *see also* Kesan & Hayes, *supra* note 39, at 792.

49. *See* Jenna McLaughlin, *Justice Department Releases Guidelines on Controversial Anti-Hacking Law*, THE INTERCEPT, (Oct. 26, 2016), https://theintercept.com/2016/10/26/justice-department-releases-guidelines-on-controversial-anti-hacking-law/ [https://perma.cc/X6SJ-QN8L].

laws intend to capture malicious hacking practices, they often fail to legitimize necessary security research practices used by researchers in VDPs.

Because of the robust VDP community, host organizations have a legitimate interest in insulating themselves from the risk that comes with soliciting security research from the general public.[50] Despite significant industry adoption of VDPs and the significant monetary rewards involved, there are no formal regulatory requirements to deploy VDPs.[51] As a result, the security research community falls victim to uncertainties about the legality of security research due to the failure to comply with program legal terms if such terms are too limiting, unclear, or improperly drafted.[52] Poorly crafted legal terms may subject a researcher to unknown liability, while overly-restrictive terms muzzle researchers and discourage research.[53]

A. The Computer Fraud and Abuse Act and Its Impact on Security Research

The CFAA criminalizes the intentional accessing of a "computer" without authorized access or by exceeding authorized access.[54] "Computer" is broadly defined to include virtually any system with Internet connectivity, including mobile devices.[55] The Second, Fourth, and Ninth Circuits interpret "exceeding authorized access" narrowly, limiting it to bypass of access controls or stealing of account data,[56] while the First, Fifth, Seventh, and Eleventh Circuits read the statute's phrase broadly to include the use of a computer for purposes prohibited in a terms of service agreement.[57] Without regulatory oversight over how host organizations implicate legal repercussions in their terms of service, interpretation of the CFAA's use of "authorization" falls to host organizations' contracts.[58] When combined with the lack of judicial consistency regarding the CFAA, security researchers must choose between the legal risks of running afoul of the CFAA under a broad interpretation or not conducting the research at all.[59]

The CFAA is inapt for modern uses of the Internet, causing widespread public confusion regarding the statute's application. Taking the realities of

---

50. *See* Porup, *supra* note 29 (referencing risk management concerns that may exist inside customer organizations).

51. *Id.*

52. *Id.*

53. *Id.*

54. *See* 18 U.S.C. § 1030 (2012).

55. *See* 18 U.S.C. § 1030(e).

56. *See* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Sols. v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

57. *See* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

58. Kirsch, *supra* note 14, at 399 (noting that it is commonplace for private entities to define and apply criminal activity as it exists under the CFAA).

59. *See* Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research,* CTR. FOR DEMOCRACY & TECH. 9 (Mar. 2018), https://cdt.org/wp-content/uploads/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/85SP-5FLT].

security research into consideration, the uncertainties and inconsistent applications of the CFAA chill security research.[60] Even when a defendant's actions do not result in any financial loss or harm, a violation of the CFAA may lead to criminal penalties, including imprisonment.[61] According to a 2018 study conducted by the Center for Democracy and Technology (CDT) about the risk basis for security research, half of the subjects interviewed for the study reported the CFAA as a primary source of risk.[62]

In 2012, DOJ indicted security researcher Andrew Auernheimer for discovering an email breach in AT&T's servers by writing a program exposing the vulnerability, alerting victims of the breach, and disclosing email addresses obtained through the breach to a public news site.[63] DOJ charged Auernheimer with felony computer hacking under the CFAA in the U.S. District Court for the District of New Jersey, which sentenced him to 41 months in prison.[64] Auernheimer's conviction under the CFAA was based on "unauthorized access" to the system.[65] The finding that Auernheimer bypassed any authorizations—despite not using a password, login, or cookies—to access a publicly available website requires a dangerously broad reading of the CFAA.[66]

Auernheimer was able to reveal the vulnerability without using a password, login, or cookies—all actions which do not constitute a bypass of authorization in a technical sense, despite the court's interpretation of the CFAA.[67] In this case, AT&T did not employ protective measures to control access to the information obtained and disseminated by the defendant.[68] On appeal, Auernheimer argued that the company made the "information available to everyone and thereby authorized the general public to view the information," constituting authorized action under the CFAA.[69] The appeals

60. *Id.* ("Uncertainty potentially resulting in steep criminal penalties creates a significant chilling effect for researchers.").

61. *See* 18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(A).

62. *See* Lorenzo & Adams, *supra* note 59, at 9.

63. *See* United States v. Auernheimer, 748 F.3d 525, 529–31 (3d Cir. 2014).

64. *See* Matt Brian, *Andrew 'weev' Auernheimer Sentenced to 41 Months for Exploiting AT&T iPad Security Flaw*, VERGE, (Mar. 18, 2013), https://www.theverge.com/2013/3/18/4118484/andrew-weev-auernheimer-sentenced-att-ipad-hack [https://perma.cc/Y6US-PNY7].

65. *Id.*

66. A narrow view of the CFAA signals that access to a publicly available website is not "unauthorized access. 18 U.S.C. § 1030(a)(2)(C); *see* Pulte Homes, Inc. v. Laborers' Intern. Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011).

67. *See* Orin Kerr, *United States v. Auernheimer, and Why I Am Representing Auernheimer Pro Bono on Appeal Before the Third Circuit*, THE VOLOKH CONSPIRACY, (Mar. 21, 2013), http://volokh.com/2013/03/21/united-states-v-auernheimer-and-why-i-am-representing-auernheimer-pro-bono-on-appeal-before-the-third-circuit/ [https://perma.cc/KX3C-BC9L].

68. *See Auernheimer*, 748 F.3d at 529.

69. *See Orin Kerr's Appeal Brief for Andrew "Weev" Auernheimer – Another CFAA Case,* GROWKLAW (July 2, 2013), http://www.groklaw.net/articlebasic.php?story=20130702033515452 [https://perma.cc/8CR9-VFZL].

court eventually overturned the district court's ruling on technical grounds, leaving the CFAA's application to Auernheimer's activity unresolved.[70]

The vague interpretation of the CFAA in *Auernheimer* blurs the line between malicious hacking and security research activity.[71] The opinion suggests that the CFAA equates unrestricted access to a webpage like AT&T's with unauthorized access considered unlawful under the CFAA.[72] *Auernheimer* suggests that disclosure methods that entail sharing security flaw information publicly, the type of activity at the core of VDPs, may be subject to criminal penalty. Auernheimer's story creates an uncertain environment for security research, making security researchers wary about disclosing security vulnerabilities following the case's broad application of the CFAA.

B. The DMCA and Its Impact on Security Research

Section 1201(a) of the Digital Millennium Copyright Act (DMCA), the anti-circumvention provision of copyright law, forbids the unauthorized bypass of certain technological boundaries controlling access to software or code protected by copyright.[73] Section 1201(a) does not explicitly differentiate between circumvention of technological boundaries that infringe copyright and circumvention for legitimate reasons, such as authorized security research.[74] Security researchers concerned about the legal risks posed by a potential violation of the DMCA tend to shy away from performing research on systems protected by access controls.[75]

A statutory exemption for security research under the DMCA was extended in 2018, allowing for "good-faith" security research.[76] However, among other limitations, the exemption requires that the research will not violate any applicable law, including the CFAA and contract law.[77] Under this requirement, legal terms continue to ban, either implicitly or by way of poor drafting, researchers from "circumvention" techniques that may be necessary to properly perform security research. Paradoxically, the exemption is meaningless unless VDP terms of use allow for circumvention and establish authorized access under the DMCA, as well as by implication under the

70. *See Appeals Court Overturns Andrew "weev" Auernheimer Conviction*, ELEC. FRONTIER FOUND. (Apr. 11, 2014), https://www.eff.org/press/releases/appeals-court-overturns-andrew-weev-auernheimer-conviction [https://perma.cc/2DZT-53HA].

71. Kirsch, supra note 14, at 394.

72. *Id.*

73. *See* 17 U.S.C. § 1201.

74. *See generally id.*; Stan Adams, *Getting Better All the Time: Security Research and the DMCA*, CTR. FOR DEMOCRACY & TECH., (Oct. 26, 2018), https://cdt.org/insights/getting-better-all-the-time-security-research-and-the-dmca/ [https://perma.cc/D5CV-PDRY].

75. *See* Hall & Adams, *supra* note 59, at 6–7.

76. *See* 17 U.S.C. § 1201(j)(1).

77. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944, 65956 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201).

CFAA.[78] Because many researchers have an incomplete understanding of the conditions for eligibility, the DMCA continues to chill security research.

C. *Safe Harbor Language: A Superficial Fix, Not a Complete Solution*

Adequate safe harbor language in contracts would authorize research in light of anti-hacking laws such as the CFAA and DMCA by including a clearly defined scope of when authorization may occur.[79] However, safe harbor language is the exception and not the rule across VDPs.[80]

But even when safe harbor language exists, it may be an inadequate solution for liability posed to researchers, partly because a host organization may write VDP terms to determine, in its sole discretion, if a security researcher meets the safe harbor criteria. The possibility of this power imbalance, even in the presence of an adequate safe harbor, limits the comfort researchers can take in the presence of safe harbor terms.[81] This power imbalance is not merely hypothetical, but rather a regular practice in the VDP industry today. Some organizations ask security researchers to enter into a series of agreements, in addition to the VDP program terms, as a prerequisite to VDP participation, threatening prosecution under the CFAA if the NDA is refused. For example, PayPal asks security researchers to agree to an NDA as part of their terms and agreements, agreeing not to bring private action or refer a matter for public inquiry only when the security researcher meets all the guidelines of the terms and agreements.[82] Further, platforms like HackerOne openly acknowledge that safe harbor terms offered by host organizations running programs on their platform may be contingent on program terms, including an NDA.[83]

In March of 2020, a blockchain-based voting company, Voatz, referred a student researcher to the FBI over what the company claims was an attempted intrusion by the security researcher.[84] Voatz touts a safe harbor statement as part of its VDP program. Following the criticism and negative reporting following the incident, Voatz retroactively changed its VDP program terms by narrowing the scope of its safe harbor policy and negating full legal protection.[85] Voatz serves as an example of how even a safe harbor may derail the environment of trust between researchers and the host

78. *See* 17 U.S.C. § 1201.

79. *Id.*

80. *See generally Photo Gallery*, AMIT ELAZARI, https://amitelazari.com/#legalbugbounty-hof (last visited Jan. 24, 2020).

81. *See* Porup, *supra* note 29.

82. *See e.g.*, *Paypal - Bug Bounty Program*, HACKERONE, https://hackerone.com/paypal (last visited Jan. 24, 2020) [https://perma.cc/SG57-WAJ2].

83. *See generally Vulnerability Disclosure Guidelines*, HACKERONE, (July 29, 2019), https://www.hackerone.com/disclosure-guidelines [https://perma.cc/3G5M-2Z9R].

84. *See* Yael Grauer, *Voatz Bug Bounty Kicked Off of HackerOne Platform*, COINTELEGRAPH, (Mar. 31, 2020), https://cointelegraph.com/news/voatz-bug-bounty-kicked-off-of-hackerone-platform [https://perma.cc/4A3J-74NU].

85. *Id.*

organization. For safe harbor provisions to work, host organizations must follow their own protocol.

IV. THE DOJ'S DISCRETIONARY GUIDANCE FOR PRIVATE VDPS

In July 2017, the Department of Justice (DOJ) Cybersecurity Unit[86] released a framework outlining guidelines for host organizations to use security research to identify bugs in their systems through VDPs.[87] The DOJ Framework emphasizes the clear boundaries necessary when hosting a VDP to reduce violations under the CFAA and DMCA.[88] The DOJ Framework recognizes the risks associated with careless or overbroad policy language and provides guidance on how adequate VDP procedures may address the range of legal risks involved in running and participating in VDPs.[89] The DOJ Framework does not mandate specific requirements or objectives for vulnerability disclosure but encourages organizations to protect security researchers through their terms, procedures, and processes.[90] Rather, the DOJ Framework is intended to help host organizations effectively run VDPs through standard practices and policies.[91]

The DOJ Framework offers a four-part roadmap of guidelines for host organizations to follow.[92] For example, the DOJ Framework points to templates for VDP creation, provides guidelines for communicating with security researchers, and advises on the adoption of a multi-stakeholder process when designing a VDP.[93] All four steps delineated by the DOJ Framework address, among other things, the importance of safe harbor language.

Dr. Amit Elazari, a prominent scholar in the Bug Bounty and VDP space, compiled an initial list of VDPs that adopt language in adherence with the DOJ Framework's guidance on legal safe harbors for security research.[94]

---

86. The DOJ is responsible agency for CFAA strategy and enforcement. *Cybersecurity Unit*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated Mar. 12, 2020) [https://perma.cc/69QD-XP76].

87. *See DOJ Framework*, *supra* note 20.

88. *Id.* Application to DMCA is implied based on the relationship between the CFAA and DMCA.

89. *Id.* When organizations take the time to establish clear boundaries and unambiguous protocols through their program's policy language, they are more likely to avoid the risks associated with unauthorized security research.

90. *Id.*

91. *Id.* at 1, n.3 ("This guidance is intended as assistance, not authority such that nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter."); *see e.g.*, United States v. Caceres, 440 U.S. 741 (1979); Ellen S. Podgor, *Department of Justice Guidelines: Balancing "Discretionary Justice"*, 13 CORNELL J.L. & PUB. POL'Y 167, 169 (2004) ("Courts routinely find these guidelines strictly internal an d unenforceable at law. [Failure to follow guidelines] cannot be used by the accused . . .").

92. *See id.*

93. *DOJ Framework*, *supra* note 20.

94. *See Photo Gallery*, *supra* note 80; *see generally Public Bug Bounty List*, BUGCROWD, https://www.bugcrowd.com/bug-bounty-list/ (last visited Mar. 22, 2020).

Based on her findings, as of March 2018, 26 VDPs adopted language that follows the DOJ Framework's guidelines on the legal safe harbor. Due to the publication of a safe harbor directory maintained by Disclose.io, there is now a comprehensive and up to date list of VDPs.[95] As of December 2019, 106 of the 311 total VDPs included as part of Disclose.io's comprehensive list of public VDPs successfully include full safe harbors.[96] While qualitative or quantitative research on the correlation between the DOJ Framework does not currently exist, the increase in VDPs with full safe harbors is significant, increasing four-fold in under two years.[97] Academics and security researchers have long advocated for VDP safe harbors, but the release of the DOJ Framework provides a tangible and trustworthy model for host organizations to utilize in writing or reforming VDP policies.

The DOJ Framework provides much more than guidelines for standardizing safe harbor language, which may not be sufficient to fully insulate security researchers from legal risks, as discussed in Part II. The DOJ Framework is meant to help focus host organizations' attention on knowing the risks they face based on their size, resources, and involvement with the researcher community.[98] In sum, the DOJ Framework provides holistic yet flexible guidelines for host organizations to use when considering the efficacy of their VDPs.[99]

The DOJ Framework is a resource for organizations running VDPs, offering a comprehensive form of guidance for host organizations.[100] While it does not mandate legal terms or practices that eliminate or clarify legal risks associated with security research on privately owned systems, it provides the tools to help host organizations do so.[101]

Some organizations have, in response to the DOJ Framework, successfully adopted direct commitments related to restricting legal actions, while other organizations have gone so far as to adopt policy language that legally authorizes access under existing anti-hacking laws. In fact, the government's own VDPs across agency host organizations exemplify the very standards the DOJ Framework aims to socialize, highlighting that the DOJ Framework is not the government's only contribution to the VDP landscape.

V. THE U.S. GOVERNMENT'S INFLUENTIAL ROLE IN VDP GOVERNANCE

Cyberattacks and data breaches do not discriminate. The risk of sweeping financial and reputational damage exists in both the private and

95. *See Public Bug Bounty List*, *supra* note 94.

96. *Id.* 106 out of 311 total VDPs documented on the list is maintained as part of the Disclose.io Safe Harbor project.

97. *Id.*

98. *See generally DOJ Framework*, *supra* note 20

99. *See id.*

100. *See generally Caceres*, 440 U.S. 741.

101. *See e.g.*, *DOJ Framework*, *supra* note 20.

public sectors.[102] The private sector has long crowdsourced vulnerabilities, whereas the U.S. federal government only recently began employing VDPs at the federal agency level.[103] However, VDPs are considered an industry best practice not only in the private sector, but for governments as well.[104] U.S. government-run VDPs distinguish themselves from those in the private sector by providing ethical hackers clear guidelines for submitting bugs found in government systems.[105]

A. The U.S. Government as a "Crowdsourcer": Validating the Importance of Public Engagement to Cybersecurity

The government adopted its first VDP in April 2016 with the Department of Defense's (DOD) "Hack the Pentagon" program.[106] The government's entry into the private sector-dominated VDP world signaled widespread recognition of citizen engagement as a beneficial way to address cybersecurity challenges.[107] The DOD's pilot program exceeded expectations, resulting in over 1,000 vulnerability reports,[108] which the DOD explained would normally take hundreds of hours of internal manpower at a cost above $1 million for the agency without a VDP.[109] The entire cost of the pilot was $150,000, with about half of that amount going to security researchers in payouts.[110] In November 2016, the DOD ran its second program, "Hack the

102. *See* Sarah A. Lafen, *U.N. Regulation - The Best Approach to Effective Cyber Defense?*, 45 SYRACUSE J. INT'L L. & COM. 249, 250 (2018).

103. *See* Sean Martin, *History And Interesting Facts About Bug Bounties - An Appsec Usa 2017 Panel Recap*, ISTP MAGAZINE, Sept. 23, 2017, https://www.itspmagazine.com/itsp-chronicles/history-and-interesting-facts-about-bug-bounties-an-appsec-usa-2017-panel-recap [https://perma.cc/SD6K-KC3N] (noting that the private sector is where the VDP industry was first born, with Netscape launching the first known bug bounty program in 1995. Netscape was very much ahead of its time. Many companies like Google and Microsoft did not launch bug bounty programs until the 2010s. In xthe past decade, growth of the industry has mushroomed).

104. *See The Hacker-Powered Security Report 2019,* HACKERONE (Dec. 3, 2019), https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019 [https://perma.cc/ZGY2-L72D].

105. *See* Lindsey O'Donnell, *U.S. Agencies Must Adopt Vulnerability-Disclosure Policies by March 2021*, THREATPOST (Sept. 2, 2020), https://threatpost.com/u-s-agencies-vulnerability-disclosure-policies-march-2021/158913/ [https://perma.cc/2EPY-W9QP].

106. Press Release, Department of Defense, Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program (Oct. 24, 2018) https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/ [https://perma.cc/6RNU-57BV].

107. *See* Ines Mergel, *Social Media Adoption and Resulting Tactics in the U.S. Federal Government*, 30 GOV'T INFO. QUARTERLY 123, 130 (2013).

108. *See "Hack the Pentagon" Fact Sheet*, U.S. DEP'T. OF DEF., (Jun. 17, 2016), https://dod.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf [https://perma.cc/S9SW-U25T].

109. *See* Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Results*, U.S. DEPT. OF DEF., (Jun. 17, 2016), https://www.defense.gov/Explore/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/ [https://perma.cc/LSM5-ZQW3].

110. *See id.*

Army," through which hackers received $100,000 in total payouts.[111] In conjunction with the "Hack the Army" program, the DOD announced a "Digital Vulnerability Disclosure Policy," providing guidance to security researchers on legal boundaries for testing and disclosing vulnerabilities in DOD websites.[112] Prior to the DOJ's release of its framework, the DOJ's Criminal Division was consulted in the development of this policy language to help the DOD carry out its commitment to working "openly and in good faith with researchers."[113]

The DOD's consistent use of VDPs, while a departure from traditional security strategies employed by the agency, has produced favorable outcomes backed by quantitative evidence and established a route for the government to tap into private sector cybersecurity talent.[114] Following the positive response to the DOD's Hack the Pentagon program, other agencies began to develop similar programs, including the Department of State, Food and Drug Administration (FDA), General Services Administration (GSA), and Department of Homeland Security (DHS).[115] In December 2018, President Donald Trump signed the SECURE Technology Act (H.R. 7327) into law, which required the DHS to establish a security vulnerability disclosure policy and establish a VDP program.[116] The passage of the SECURE Technology Act signals Congress' recognition of the value of VDPs in the context of the government.[117]

B. The U.S. Government as a "Rule Maker": The DHS' Compulsory Authority over Government VDPs

On November 27, 2019, the DHS released the Cybersecurity and Infrastructure Security Agency's (CISA) draft Binding Operational Directive 20-01 ("the DHS Directive") titled "Develop and Publish a Vulnerability

111. *See* Michael Mimoso, *Hack the Army Bounty Pays Out $100,000; 118 Flaws Fixed*, THREAT POST, (Jan. 20, 2017), https://threatpost.com/hack-the-army-bounty-pays-out-100000-118-flaws-fixed/123216/ [https://perma.cc/Q6BN-X98J].

112. *See DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army" Kick-Off*, U.S. DEP'T. OF DEF., (Nov. 21, 2016), https://www.defense.gov/Newsroom/Releases/Release/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/ [https://perma.cc/RFE8-ZGJV].

113. *Id.*

114. *See, e.g.*, *The Hacker-Powered Security Report 2019*, HACKERONE 11 (Dec. 3, 2019), https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019 [https://perma.cc/4Q2S-DZ94] (highlighting that as of December 2019, the DOD has detected more than 10,000 researcher-discovered security vulnerabilities over the short lifespan of its multiple VDPs).

115. *Id.*

116. *See* SECURE Technology Act, H.R. 7327, 115th Cong. (2018); THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/LSX6-YZRQ] (finding that the White House is centrally responsible for the political and strategic management and coordination of cybersecurity policies through the National Security Council).

117. *See generally* H.R. 7327.

Disclosure Policy."[118] The DHS Directive requires every federal agency to run a VDP, mandating the creation of a formal process for researchers to report vulnerabilities within the agency's public-facing websites or information technology infrastructure, and a system for addressing vulnerabilities discovered through the VDP.[119] The DHS Directive calls for each agency to set standardized vulnerability disclosure policies,[120] which will help promote the establishment of clear boundaries around the legalities of hacking government systems. The DHS Directive effectively mandates agencies to bring themselves up to speed within six months with a VDP and disclosure policy and requires that all internet-accessible systems and services are in the scope of the policy by the two-year mark.[121] The DHS Directive, which was open for public comment until December 27, 2019, specifically outlines the principles that each agency's VDP must contain, including language that requires agency programs to delineate legal protections for researchers, the scope of agency assets open to program participants, and guidelines for how the agency will resolve reported bugs.[122]

C. The Government as an "Example": The Impact of Government VDPs on the Private Sector, as Evidenced Through Commercial VDP Management

When the DOD launched the first known government VDP, "Hack the Pentagon," the effort was outsourced to HackerOne, which not only operated the initiative, but also advised the DOD on the creation and growth of the program.[123] Since 2016, the DOD has worked with HackerOne on programs like "Hack the Army," "Hack the Airforce," "Hack the Marine Corps," as well as future iterations of "Hack the Pentagon."[124] A partnership between

---

118. *See* Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy (Sept. 2, 2020).

119. *Id.*

120. *Id.*

121. *Id.*

122. *See* Sean Lyngaas, *DHS Is Mulling an Order That Would Force Agencies to Set Up Vulnerability Disclosure Policies*, CYBERSCOOP, (Oct. 23, 2019), https://www.cyberscoop.com/dhs-vulnerability-disclosure-program-bod/ [https://perma.cc/28N2-KVU8]; Develop and Publish a Voluntary Disclosure Policy, 84 Fed. Reg. 69,761 (proposed Dec. 13, 2019).

123. Press Release, NewsWire, Department of Defense Launches Bug Bounty Program on HackerOne (Mar. 31, 2016), https://www.newswire.com/news/department-of-defense-launches-bug-bounty-program-on-hackerone [https://perma.cc/SGK3-5VQM].

124. *See* Marten Mickos, *The Best Is Yet to Come: DoD Awards New Hack the Pentagon Program to HackerOne*, HACKERONE (Oct. 24, 2018), https://www.hackerone.com/blog/Best-Yet-Come-DOD-Awards-New-Hack-Pentagon-Contract-HackerOne [https://perma.cc/NHU7-LP6L]. More recently, the U.S. General Services Administration's Technology Transformation Service also signed a contract with HackerOne for the first bug bounty program run by a civilian federal agency. Tajha Chappellet-Lanier, *GSA Awards $2M Bug Bounty Service Contract to HackerOne*, HACKERONE (Sept. 1, 2018), https://www.fedscoop.com/gsa-hackerone-bug-bounty-contract/ [https://perma.cc/X27F-9AZF].

HackerOne, a private sector startup in its nascent stages, and the DOD, arguably the most security-aware organization in the nation, signals a great deal of credibility and value housed in the use of commercial platforms for VDP management.[125]

The credibility implied in HackerOne's contracts with multiple government agencies, as well as the use of the DOD's VDP as a successful model suggests to the private sector that commercial VDP platforms can accommodate the needs of large, complex enterprises. As a result, many of the largest private companies, including household names like Goldman Sachs, General Motors, Uber, Starbucks, and many others, have signed on to work with platforms trusted by the government.[126] Organizations of all sizes find commercial VDP platforms attractive because experienced third parties assist every step of the process, including writing a policy, setting a scope, and establishing bounties.[127]

Industry use of commercial vendors in VDP management shows the influence of the DOJ Framework, as seen in agreements from companies like HackerOne.[128] Among their many DOJ-Framework-aligned recommendations,[129] HackerOne's "Vulnerability Disclosure Guidelines" include a "Safe Harbor" section which highlights that HackerOne is better able to protect, or help protect, security researchers in difficult disclosure situations if the security researcher's actions comport with the guidelines.[130] While not every organization on the HackerOne platform complies with DOJ Framework guidelines or even the safe harbor language, HackerOne's explicit support for researchers who comply with the DOJ Framework sets a floor for non-compliant VDP host organizations. As a result, a greater number of researchers who feel more comfortable pursuing VDPs contained on HackerOne (as compared to host organizations that run VDPs independently)

---

125. In addition to multiple contracts with U.S. federal government agencies, the European Commission and Singapore's Ministry of Defence (MINDEF) selected HackerOne for their bug bounty programs. The implementation of the Directive signals a trend towards the use of HackerOne and its competitors by a broader range of government agencies, especially those with limited security teams in need of support starting and running mandatory VDPs. *See generally Ministry of Defence, Singapore (MINDEF) Bolsters Security With Second HackerOne Bug Bounty Challenge*, HACKERONE (Sep. 27, 2019), https://www.hackerone.com/press-release/ministry-defence-singapore-mindef-bolsters-security-second-hackerone-bug-bounty, (last visited Nov. 1, 2020) [https://perma.cc/Z5C7-8RGW].

126. *See Goldman Sachs*, HACKERONE, https://hackerone.com/goldmansachs (last visited Jan 24, 2020) [https://perma.cc/VL5R-2U3S]; *General Motors*, HACKERONE, https://hackerone.com/gm (last visited Jan 24, 2020) [https://perma.cc/AEQ5-W7LQ]; *Uber*, HACKERONE, https://hackerone.com/uber (last visited Jan 24, 2020) [https://perma.cc/UP7X-3C36]; *Starbucks*, HACKERONE, https://hackerone.com/statbucks (last visited Jan 24, 2020).

127. *See generally Hacker-Powered Security for StartUps*, HACKERONE (2019), https://www.hackerone.com/resources/e-book/hacker-powered-security-for-startups (last visited Jan. 25, 2020).

128. *See generally Vulnerability Disclosure Guidelines*, https://www.hackerone.com/disclosure-guidelines (last updated July 29, 2019) [https://perma.cc/A268-F3X2].

129. *See generally id.*

130. *Id.*

are likely to flock to the platform. This creates quasi-network effects that draw in host organizations to partner with the platform given the breadth and quality of participating security researchers.

Commercial VDP platforms do not shy away from supporting and encouraging the use of the DOJ Framework, though there is little they can do beyond ensuring that their guidance to clients and overall philosophy align with the recommendation delineated in the framework. While commercial VDP platforms have researcher interests and safety in mind, they must balance their advocacy with the marketing of their services as part of a two-sided market.

VI. THE PATH FORWARD: RECOMMENDATIONS FOR STANDARDIZING PRIVATE SECTOR VDPS USING THE U.S. GOVERNMENT AS AN EXAMPLE

Commercial VDP platforms provide just one of many examples of the private sector looking to the government as a model for running an effective VDP. The credibility and influence of the government in the commercial VDP platform environment is only a snapshot of the VDP industry—one that not all host organizations in the private sector are influenced by. Thus, given current threats to the security research community posed by anti-hacking laws,[131] it is clear that inaction at the private sector level is not a viable option.

This Note argues that the DOJ Framework, combined with the U.S. government's exemplary use of and leadership in VDPs, has the potential to bridge the gap between managing the risks faced by both host organizations and security researchers. However, in its current state, the DOJ Framework is left largely ineffective and many private sector host organizations ignore it. The extensive guidance on strengthening VDP and cybersecurity practices put forth by the DOJ Framework and other regulatory agencies encourage host organizations to make a good faith effort to operate within the DOJ Framework to "stand a better chance if potential legal action" were to result from a cybersecurity incident.[132] While a segment of the VDP community recognizes the DOJ Framework as a step in the right direction, many important considerations about how the DOJ Framework will be used to improve the security research landscape on a wide scale have not been fully evaluated.

Operating within the DOJ Framework and taking advantage of the U.S. government's exemplary use of and leadership in VDPs can be achieved through a culmination of tactics aimed at ensuring that the DOJ Framework

131. *See* Riana Pfefferkorn, *The Importance of Protecting Good-Faith Security Research*, CTR. FOR INTERNET & SOC'Y, (Sept. 14, 2020), https://cyberlaw.stanford.edu/blog/2020/09/importance-protecting-good-faith-security-research [https://perma.cc/5AVK-AQKK]. Application to DMCA is implied based on the relationship between the CFAA and DMCA.

132. *See John K. Higgins*, *DoJ Calls On Private Sector to Strengthen Cybersecurity*, E-COMMERCE TIMES, (May 20, 2015), https://www.ecommercetimes.com/story/82079.html [https://perma.cc/9PMN-BEUY].

evolves alongside the VDP industry. This Note proposes two sustainable tactics for reforming private sector VDPs based on evaluating government and private sector VDPs, the anti-hacking landscape, and evolving cybersecurity practices. First, the private sector can achieve increased adoption of the DOJ Framework by mirroring the flexibility of existing effective cybersecurity standards. Second, the private sector must prioritize researchers' interests, exemplified by the DHS Directive and agency VDPs.

A. Compulsory DOJ Framework: Promoting Reform of Private Sector VDPs Through the Use of Standards

While mandating compliance with the DOJ Framework across private sector VDPs may be possible, few U.S. cybersecurity laws promulgate the authority to mandate private sector practices. Instead, Congress could pass legislation mandating uniform legal terms or standard VDP practices for host organizations, giving researchers the ability to conduct security research without fear of legal repercussions. Such regulation could shift the burden of ensuring that the policy language of the VDP, including the boundaries of both research activity and disclosure, adequately protects researchers participating in VDP programs in good faith. However, the need for government intervention in the form of mandated and standard language across host organizations is paternalistic and unnecessary. It is therefore in the private sector's best interest to allocate resources to secure sensitive information and maintain security.

A one-size-fits-all mandate for how a VDP must protect both researchers and host organizations is an unrealistic goal, even with the DOJ Framework's guidance. While mandatory standardization is a reality across U.S. civilian agencies, the DHS Directive is operated within a narrower scope, on a smaller scale, and based on VDP successes experienced by the DOD and its successors. When this methodology is transferred to the private sector, where VDPs vary in size, scope, resources, and experience, the success rate is much lower. In turn, cybersecurity standards, which are important in developing risk management strategies and effective security practices by establishing common approaches and requirements, are more realistic than mandatory compliance rules when it comes to socializing the DOJ Framework's practices across private sector VDPs.

Cybersecurity standards are created with the industry's needs in mind and usually include a multi-stakeholder approach involving consultation with industry, academia, regulatory bodies, and the public.[133] Cybersecurity standards are especially influential because of their ability to impact industries and markets as a whole. For example, in 2013, the National Institute of Standards and Technology (NIST), created the NIST Cybersecurity Framework, which is often perceived as a de facto standard in

133. 1 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, GOVERNANCE FRAMEWORK FOR EUROPEAN STANDARDISATION 19 (2015), https://www.enisa.europa.eu/publications/policy-industry-research/at_download/fullReport.

cybersecurity.[134] The NIST Framework is highly influential not only in the U.S. but across many other jurisdictions that rely on it as a best practice.[135] The NIST Framework, like the DOJ Framework, is a set of industry standards and best practices for organizations in the management of cybersecurity risks, practices, and operations.[136] Before its release in 2013, NIST underwent an extensive consultation period during which it worked across sectors and industries in a public-private partnership.[137] In 2017, NIST reaffirmed the matters in the original framework, as well as its commitment to implementing the nation's cybersecurity goals.[138]

Like the NIST Framework, the DOJ Framework is capable of spearheading standardized compliance with baseline VDP guidelines through collaboration with the U.S. government to improve the VDP process. The legal terms and incentives presented to researchers correlate to the effectiveness of VDPs, with clear legal terms creating an attractive marketplace for vulnerabilities. For VDPs to operate as a marketplace for vulnerabilities, program terms must be clear and unambiguous. It becomes difficult for security researchers to navigate the rules and restrictions set out by host organizations when those rules are unclear.[139]

The U.S. government has not updated the DOJ Framework since its July 2017 release, though the VDP industry is changing rapidly. Companies around the world regularly launch new VDPs, not only to stay up to date on industry cybersecurity trends but also as reputational tools signaling trustworthiness to customers.[140] Existing host organizations regularly announce significant payouts, exemplified by Google Android's VDP, which recently offered a $1.5 million bounty for a researcher to find a specific Pixel-related exploit.[141] With a constant stream of VDP engagement in both the private and public sectors globally, the DOJ must reaffirm its commitment to its guidelines and make appropriate updates to best facilitate the private sector governance set forth by the framework. NIST's stakeholder engagement efforts played a role in the success of the NIST Framework, and its widespread adoption is likely a result of the consultative process and cross-industry consensus building.[142] A potential solution is increased DOJ

134. *See* Shin-yi Peng, *"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, 51 CORNELL INT'L L.J. 445, 458 (2018).

135. *Id.*

136. *Id.* at 451.

137. *Id.*

138. *Id.* at 452.

139. 1 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *supra* note 133, at 5.

140. *See, e.g.*, Adam Bannister, *Bug Bounty Radar // November 2019,* THE DAILY SWIG, (Nov. 29, 2019), https://portswigger.net/daily-swig/bug-bounty-radar-november-2019 [https://perma.cc/99MW-HMGE].

141. *See* Corinne Reichert, *Google's Android Bug Bounty Program Will Now Pay Out $1.5 Million*, CNET, (Nov. 21, 2019), https://www.cnet.com/news/googles-android-bug-bounty-program-will-now-pay-out-1-5-million/ [https://perma.cc/26X6-W276].

142. *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 328 (2015).

engagement with private sector stakeholders, a process that would necessitate private sector VDP players to acknowledge the DOJ Framework. This may encourage private sector stakeholders to voice concerns about the DOJ Framework instead of ignoring its guidance and potentially running a VDP which puts researchers at risk. It is not clear if the DOJ consulted stakeholders before the initial framework release in 2017. However, this Note argues that some degree of involvement in updating and implementing the framework's standards alongside a variety of stakeholders, mirroring the NIST Framework as a successful cybersecurity standard, is an instrumental step towards reforming VDP practices in the private sector.

B. Mirroring the DHS Approach: The U.S. Government as an Example in Responding to Concerns that the Private Sector Fails to Address

The government's rapid involvement in VDPs and adoption of the DHS Directive across all civilian agencies shows that the government's VDP practices are particularly exemplary when it comes to limiting liability risks faced by security researchers. The government's actions in the VDP space explicitly address the harms of poorly crafted legal terms and program policies, which cause security researchers to violate anti-hacking laws merely by participating in the program.

DHS's rationale behind the creation of its DHS Directive as a standard for a government-wide VDP [143] was to promote VDP participation by making it relatively easy, explaining that when "things [are] easier to do, more people will do them."[144] Like the DOJ Framework, the DHS Directive aims to make VDP expectations clear to reduce the complexities that come with security research.[145] To address concerns at the host organization level about how to implement these changes, DHS shared a draft VDP template and guidance for agencies to follow regarding the implementation of their respective VDPs.[146]

As part of the effort to stand up the DHS Directive, DHS explicitly recognized security researchers' main frustrations, including fear of legal action.[147] The Office of the Federal Chief Information Officer announced that government agency VDPs must, according to the DHS Directive, legally insulate those who come forward with vulnerabilities, citing clear differentiation "between acceptable and unacceptable means of gathering

143. *See* Jack Corrigan*, CISA Wants a Vulnerability Disclosure Program At Every Agency*, NEXTGOV, (Nov. 27, 2019), https://www.nextgov.com/cybersecurity/2019/11/cisa-wants-vulnerability-disclosure-program-every-agency/161586/ [https://perma.cc/CX7S-5LLP].

144. *See* Jeanette Manfra, *Improving Vulnerability Disclosure Together,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENC., (Nov. 27, 2019), https://www.cisa.gov/blog/2019/11/27/improving-vulnerability-disclosure-together [https://perma.cc/5QMK-J5QD].

145. *Id.*

146. *Id.*

147. *See* Liam Tung, *US to Order Every Federal Agency to Establish Own Bug Reporting Program in 2020,* CSO, (Nov. 29, 2019), https://www.csoonline.com/article/3500742/us-to-order-every-federal-agency-to-establish-own-bug-reporting-program-in-2020.html.

security" as the way to provide legal cover.[148] Through the DHS Directive, agency VDPs are mandated to provide assurances that good faith security research is not only welcomed but also authorized.[149] The DHS Directive calls on agency VDPs to clearly articulate the systems which are within the scope of vulnerability research activity.[150] If VDPs comply with the DHS Directive's call for clarity, security research is more likely to occur on selected systems in an authorized manner while avoiding unauthorized security research on systems where it is not solicited.

While it is generally uncommon for the government to lead in the information technology space, government agencies operate extremely progressively within the scope of VDPs based on a proven approach to security research.[151] The call for comprehensive and uniform practices across agency VDPs helps protect and incentivize security research at the governmental level amid the volatile anti-hacking legal landscape.

The DOJ should work closely with its counterparts at DHS, as well as across government agencies, to identify the challenges involved in standardization of the VDP process and legal terms on a more defined scale. VDPs are, by nature, premised on the idea of transparency. It is likely that the DHS, through its central oversight of all U.S. federal government VDPs, plans to release detailed qualitative and quantitative information regarding the results of mandatory government agency VDP implementation. The DHS Directive sets forth precise requirements for agencies developing and publishing vulnerability disclosure policies, in addition to rules on how to handle procedure, reporting, and researcher communications. The DOJ, which must also comply with DHS requirements and create a VDP of its own, should extract relevant takeaways and apply them to update the DOJ Framework. Based on the outcomes of the DHS Directive, the DOJ should set forth a parallel process of developing specific terms for industry-specific applications in the private sector. In this hypothetical, the DOJ may have more influence over standardization of VDP processes and terms if the framework is tailored to specific industries, especially those with organizational complexities and higher risks for non-compliance (e.g., financial services).

The private sector and government VDP markets are natural complements given the importance of access to and dissemination of cybersecurity information. A high bounty offered by any VDP industry participant for a specific bug sends a message to both the government and the private sector about the importance of addressing the vulnerability and sharing the results.[152] VDPs create information channels by which

148. Memorandum from Russel T. Vought, Director, Off. Mgmt. & Budget to the Heads of Executive Departments and Agencies (Sept. 2, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf [https://perma.cc/2HAW-T7CG].

149. Manfra *supra* note 144.

150. *Id.*

151. *See White Hat Hackers Help Pentagon Close Its Cybersecurity Holes*, DICE (Mar. 18, 2020), https://insights.dice.com/2020/03/18/white-hat-hackers-help-pentagon-close-its-cybersecurity-holes/ [https://perma.cc/GNJ3-MQ8Q].

152. *See* Serge Egelman et al., *Markets for Zero-Day Exploits: Ethics and Implications*, NEW SEC. PARADIGMS WORKSHOP 41, 44–45 (2013).

organizations can achieve partial objectivity in understanding cybersecurity risks through the successes and improvements experienced by other host organizations, including governments.

While the DOJ Framework may not have binding authority through its VDP guidelines, it establishes the presence of the U.S. government as a model player in the world of VDPs. The U.S. government has an immense interest in encouraging sound practices in the private sector to keep researchers excited and motivated about their participation in VDPs. In sum, through the DHS Directive and practices at agency VDPs, the government has identified steps to maintain the interest of security researchers, and the private sector should mirror this approach by using the DOJ Framework as a standard tool.

VII. CONCLUSION

VDPs are rooted in the idea that "given enough eyeballs, all bugs are shallow."[153] Consequently, the more researchers involved in identifying weaknesses in a host organization's systems, the more security bugs are discovered and addressed.[154] Without adequate legal protections built into VDPs, there will be little incentive for ethical hackers to collaborate with organizations, including companies behind the world's most widely used products and services. While the U.S. government makes up only a portion of the VDP industry, if there is a chilling effect on security research due to inadequate legal protections, the number of eyes available to help solve significant cyber risks, and challenges within the government will decrease as well. The DOJ Framework is a first step to improve VDP practices across host organizations, and the recommendations outlined in this Note improve the existing system by suggesting methods to increase use of the DOJ Framework. While the DOJ may not have binding authority through the VDP guidelines laid out in its framework, creating a direct line of communication with stakeholders, updating potentially outdated recommendations, and looking to the DHS' binding Directive and government agency VDPs as a model has the potential to bridge the gap created by the DOJ Framework's voluntary self-governance model and the current issues faced in the VDP world.

153. Maillart et al., *supra* note 24, at 82.
154. *Id.*

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

COMPTEL v. Federal Communications Commission

Veronica Lark

978 F.3D 1325 (D.C. CIR. 2020)

Petitioners brought two petitions for review of a FCC forbearance order (the "Order") challenging (1) the reasonableness of the forbearance of wholesale requirements and (2) the FCC's failure to address public safety concerns about the forbearance of unbundling requirements, per its statutory obligations.[1] The D.C. Circuit denied petitions, holding that the FCC acted within the scope of its rulemaking authority and that neither component of the order was arbitrary or capricious.[2]

I. BACKGROUND

Under the Telecommunications Act ("the Act"), the FCC has statutory authority to forbear enforcement of a regulation or provision when the following conditions are met: (1) a regulation is no longer necessary to ensure that "charges, practices, classifications, or regulations" in relation with a telecommunications carrier or service "are just and reasonable and are not unjustly or unreasonably discriminatory; (2) enforcement of such regulation or provision is not necessary for the protection of consumers; and (3) forbearance from applying such provision or regulation is consistent with the public interest."[3]

The case here arose when USTelecom, in representing Local Exchange Carriers ("incumbents"), petitioned the FCC to forbear two requirements imposed upon their legacy telecommunications networks. The two requirements derived from an order Congress included the Act to discourage the monopoly that incumbents had over the market.[4] The first requirement was a wholesale rate requirement, which required Local Exchange Carriers to offer a special rate—the difference between retail cost of service and marketing, billing, and collection costs—to Competitive Local Exchange Carriers ("insurgents").[5] The rate was in connection with Time-Division Multiplexing ("TDM") voice services—a mechanism allowing copper wires

1. COMPTEL v. FCC, 978 F.3d 1325, 1330–31 (D.C. Cir. 2020).
2. *See id.* at 1335–36.
3. *Id.* at 1328; *see also* 47 U.S.C. § 160(a); 47 U.S.C. § 160(b) (clarifying the public interest component with relation to the importance of enhancing competition); 47 U.S.C. § 1302 (delineating the FCC's statutory forbearance authority).
4. *See COMPTEL*, 978 F.3d at 1327–29.
5. *Id.* at 1327–28.

to transmit or receive signals.[6] The second requirement was the unbundling requirement to lease copper wire network elements known as the "Analog Loop" to allow for transmissions to be sent from service provider to consumer.[7]

The requests at issue did not pertain to newer next-generation services like Voice Over Internet Protocol (VoIP) which operate using the internet and do not implicate the services and elements at issue with copper wires.[8] USTelecom argued that the anticompetitive purpose of the 1996 requirements is no longer relevant because next-generation providers offering competitive prices have supplanted incumbents in the market.[9] Additionally, they argued, the requirements disincentivized insurgents from transitioning to next-generation services by subsidizing their use of legacy systems.[10]

The FCC assessed the issue pursuant their forbearance authority under 47 U.S.C. § 160(a).[11] The first prong of § 160(a) asks whether the regulation is no longer necessary "to ensure that the charges, practices, classifications, or regulations . . . are just and reasonable and are not unjustly or unreasonably discriminatory." [12] The FCC found that if prices went up for insurgents' purchasing services, it is unlikely that such an increase would be unreasonable for consumers because "intermodal competition will discipline prices."[13] Under the second prong of § 160(a) —concerning whether the regulation is not necessary to protect consumers—the FCC determined that consumers did not need the protection of these requirements due to the competition that currently exists between providers.[14] And finally, under the third prong of § 160(a)—concerning whether the public interest benefits from forbearance—the FCC determined that the public would benefit because insurgents and incumbents would shift to next-generation offerings.[15]

The resulting Order found for incumbents because they face competition from a myriad of telecommunications offerings, and, as a result, no longer have the same level of control over the market.[16] Incumbents now have "just 12% of all voice connections . . . and 37% of all wireline telephone connections."[17]

Commentators opposed the forbearance Order for numerous reasons, many of which were assessed in the petitions for review before the D.C. Circuit.[18]

6. *See id.* at 1328.
7. *Id.*
8. *COMPTEL*, 978 F.3d at 1329.
9. *Id.*
10. *Id.*
11. *Id.* at 1328.
12. *Id.*
13. *Id.* at 1328, 1330.
14. *COMPTEL*, 978 F.3d at 1328, 1330.
15. *Id.*
16. *See id.* at 1329–30.
17. *Id.* at 1330.
18. *Id.* at 1329.

II. ANALYSIS

In response to the FCC's forbearance Order, two parties petitioned for review, challenging the provisions at issue.[19] Incompas challenged the wholesale requirement and California Public Utilities Commission ("CPUC") challenged the unbundling provision.[20] The court consolidated the two cases due to their similarity and USTelecom intervened for the FCC.[21]

The court assessed the contentions raised concerning the wholesale requirement.[22] Specifically, Incompas asserted that the FCC used the wrong market assessment by looking at the national market competition.[23] However, the court agreed with the FCC's scope and assessment, specifically because the agency is engaged in national telecommunications policy-making.[24] The court similarly assessed Incompas' contention that the FCC did not consider the effect on rural markets in the Order.[25] The court agreed with the FCC's scope because the rural market is not comprised of the price-cap incumbents who are affected by the Order.[26] The court agreed that this scope of the Order in relation to the national market and in disregard of rural markets specifically fit within the FCC's authority and did not violate *SEC v. Chenery Corp.* as petitioners urged.[27] When considering CPUC's argument concerning the forbearance of unbundling, the D.C. Circuit similarly agreed with the FCC because its analysis mirrored the analysis for the wholesale requirement.[28]

The court found two separate instances that may have provided grounds for remanding the case, although the court did not ultimately do so.[29] In the Order, the FCC claimed that incumbents were "trapped" by the requirements; however, the court noted a clarifying footnote explaining how "incumbents can relieve themselves of unbundling requirements by retiring copper," allowing the court to find this to be just "careless wording," and not "essential to the FCC's rule," thereby mitigating the need for remand.[30] The FCC also failed to address California's concern with public safety, which is a mandate that the FCC is required to consider; however, the court said that this situation was one of "exceptional circumstances."[31]

19. *COMPTEL*, 978 F.3d at 1330–31.
20. *Id.*
21. *Id.* at 1331.
22. *See id.* at 1331–33.
23. *See id.* at 1331–32.
24. *COMPTEL*, 978 F.3d at 1331–32.
25. *Id.* at 1332.
26. *Id.*
27. *See id.* (citing SEC v. Chenery Corp., 318 U.S. 80, 87–88 (1943)).
28. *See COMPTEL*, 978 F.3d at 1333.
29. *See id.* at 1333–34.
30. *Id.* at 1333.
31. *Id.* at 1334.

III. CONCLUSION

The FCC's forbearance authority was affirmed.[32] Accordingly, the court denied Incompas' and CPUC's petitions for review.[33]

32. *Id.* at 1335.
33. *COMPTEL*, 978 F.3d at 1336.

Competitive Enterprise Institute v. Federal Communications Commission

Brittany Gault

970 F.3D 372 (D.C. CIR. 2020)

In *Competitive Enterprise Institute v. Federal Communications Commission*, the D.C. Circuit partially vacated the FCC's New Charter Order.[1] The court found that consumers had proper standing to challenge the first and third conditions[2] imposed on the merger, and subsequently vacated these conditions considering the FCC's refusal to defend on the merits.[3] The court dismissed the remainder of the appeal for lack of standing.[4]

I. BACKGROUND

This case involved the Competitive Enterprise Institute's (CEI) challenge of merger conditions imposed by the FCC in its New Charter Order.[5] The New Charter Order approved the merger of Charter Communications Inc, Time Warner Cable, and Bright House Networks, which created New Charter, subject to specified conditions.[6] CEI, along with a handful of New Charter customers, challenged four of the conditions on New Charter in this case.[7]

II. ANALYSIS

A. Jurisdiction

Per the Communications Act, any individuals "aggrieved" or "adversely affected" are permitted to appeal an FCC order to the D.C. Circuit.[8] Under the Communications Act, a petition for reconsideration is only required for judicial review in cases where the party seeking review 1) was not party to the proceedings or 2) "relies on law which the commission has

1. Competitive Enter. Inst. v. FCC*,* 970 F.3d 372, 388–89 (D.C. Cir. 2020); Applications of Charter Commc'ns, Inc., Time Warner Cable, Inc., and Advance/Newhouse P'ship, *Memorandum Opinion and Order*, 31 FCC Rcd. 6327 (2016) [hereinafter *New Charter Order*].
2. The FCC imposed six total conditions on the New Charter merger. Four of the six were challenged in this appeal by CEI. *Competitive Enter. Inst.,* 970 F.3d at 387.
3. *Competitive Enter. Inst.,* 970 F.3d at 388.
4. *Id.*
5. *Id.* at 376; *New Charter Order*, 31 FCC Rcd. 6327.
6. *Competitive Enter. Inst.*, 970 F.3d at 378.
7. *Id.* at 376.
8. *Id.* at 380.

been afforded no opportunity to pass."[9] The FCC argued that appellants forfeited rights to seek reconsideration when they failed to file comments earlier in the proceeding.[10] Still, the court has held that the FCC may have such "opportunity to pass" even if a party seeking review never raised the issue. Here, the court found that the FCC had sufficient "opportunity to pass," citing CEI's initial filings of comments and objections made by dissenters to the New Charter Order.[11]

B. Constitutional Standing: Causation and Redressability

To establish constitutional standing necessary for Article III's case or controversy requirement, a party must demonstrate both causation and redressability.[12] This is more difficult to establish in cases concerning the conduct of a third party not before the court.[13] In these cases, a third party must act in a manner to produce causation and permit redressability."[14] Permissible theories of standing for third parties must demonstrate that they are not based on "mere speculation."[15] The nature of the relationship between causation and redressability was also a particular point of contention between the majority and the dissent.[16] The majority relied on economic arguments suggesting that market incentives will induce New Charter to adjust business practices in a manner beneficial to the appellant-consumers once FCC-imposed conditions are removed.[17] In contrast, the dissent remained unconvinced that economic theory will translate to business reality, making redressability unlikely for four contested conditions.[18]

1. The First Condition: Network "Interconnection"

The first contested condition concerns the agreements made between New Charter and "edge providers."[19] These agreements allow broadband providers to collect payment in exchange for allowing edge providers to reach their subscribers.[20] The New Charter Order prohibited these agreements, causing New Charter to forego revenue.[21] The court found that this prohibition harmed New Charter consumers by increasing broadband prices.[22] Plaintiffs also offered related claims alleging harm to broadband quality. [23] Although the court deemed the quality-based claims too speculative, plaintiffs

9. *Id.*
10. *Id.*
11. *Competitive Enter. Inst.*, 970 F.3d at 381.
12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. *Competitive Enter. Inst.*, 970 F.3d at 381–82, *id.* at 389 (Sentell, J., dissenting).
17. *Competitive Enter. Inst.*, 970 F.3d at 382–85.
18. *Id.* at 389 (Sentell, J., dissenting).
19. *Id.* at 382–85.
20. *Id.* at 382.
21. *Competitive Enter. Inst.*, 970 F.3d at 382–83.
22. *Id.*
23. *Id.*

prevailed upon their theory of price harm.[24] Evidence demonstrated that the loss of these agreements resulted in lost revenue, and that consumer bills increased following the merger.[25] Expert witnesses connected the increased prices to the merger condition.[26] The court also considered the unique pricing dynamics of two-sided markets–accepting New Charter's assertion that it operates in a two-sided market, citing *Ohio v. American Express* as persuasive support for consideration of indirect network effects on consumer pricing.[27] The court held that the same evidence proved redressability. Per economic principles, the removal of the interconnection prohibition would allow New Charter to reenter contracts with edge providers, re-balancing the two-sided market to result in a price decrease.[28]

2. The Third Condition: Discounted Service

The third condition required New Charter to provide discounted Internet services to a set number of low-income individuals.[29] Specifically, the plan required New Charter to offer 30 mbps broadband service at the cost of $14.99 per month.[30] Given the lack of similar programs at each company prior to the merger, the court concluded that this policy would not have existed but for the mandatory merger condition.[31] In light of the theoretical economic impact coupled with the actual higher cost to consumers post-merger, the court held that petitioners sufficiently demonstrated causation.[32] The court also held that this harm was redressable–finding that New Charter was "unlikely to retain the program voluntarily."[33] The majority opined that there was a "substantial likelihood" that if permitted, New Charter would restrict the low-income assistance program, and that after doing so, firms would have ability and motive to reduce pricing for other consumers.[34]

3. The Second Condition: User Based Pricing

The second New Charter condition prohibited usage-based pricing.[35] The arguments made by the consumers articulated how this policy effectually used some low-frequency users to subsidize the costs of providing service for others.[36] However, presented with a dearth of evidence that any of the three merged entities offered usage-based pricing plans before merging, the court was uninclined to see how the lack thereof was directly tied to the merger.[37]

---

24. *Id.* at 382–83.
25. *Id.*
26. *Competitive Enter. Inst.*, 970 F.3d at 382–83.
27. *Id.* at 383 (citing Ohio v. Am. Express Co., 138 S. Ct. 2274 (2018)).
28. *Id.*
29. *Id.* at 385–86.
30. *Id.* at 386.
31. *Competitive Enter. Inst.*, 970 F.3d at 385–86.
32. *Id.* at 386–87.
33. *Id.* at 387.
34. *Id.*
35. *Id.* at 385–87.
36. *Competitive Enter. Inst.*, 970 F.3d at 385–87.
37. *Id.*

The court held that petitioners lacked standing to challenge this condition having failed to show causation or redressability. [38]

4. The Fourth Condition: Infrastructure Buildout

The court rejected standing for the consumers challenging the infrastructure provision of the New Charter Order on the grounds that the issue lacked redressability. Since the merged entity already took substantial steps in enacting this program, the court did not believe that the removal of the condition would change the course of action already set in motion. Without the guaranteed abolition of the program or the revenue regained from it, the petitioners failed to articulate how they could directly benefit from removal of the provision.

5. Dissent

Judge Sentelle dissented and concurred in part–dissenting from the majority holding as to the first and third conditions and concurring with the majority finding that CEI did not have standing to challenge the second and fourth conditions.[39] The dissent would find that CEI lacked standing to challenge all of the proposed conditions in dispute.[40] Having opined that CEI lacks standing to challenge any of the contested conditions, the dissent offered no further thoughts on the merits of the case,[41] discussed hereafter.

C. Merits

Subsequent discussion of the merits of the case was comparatively brief.[42] The court declined to offer a full substantive review on the merits in light of the fact that the FCC argued only the issue of standing and made no arguments in the alternative.[43] Objections raised by appellants included: concerns over whether statutory authority to consider the public interest implications of granting "individual licenses" extends to mergers in their entirety; whether conditions could be imposed on *all* licenses, including wireless licenses, although broadband Internet provision is not (directly) covered by Title II; and the imposition of merger conditions that advance consumer benefits that are non-specific to the transaction under review.[44] Although the court declined to resolve these "troubling" questions, its discussion suggests the court found them to be compelling.[45] This approach invites future challenges to FCC-imposed merger conditions and suggests that there may be potential for such a claim to succeed on the grounds that they extend beyond the statutory authority of the FCC. Furthermore, although

38. *Id.*
39. *Id.* at 389 (Sentell, J., dissenting).
40. *Id.* (Sentell, J., dissenting).
41. *Competitive Enter. Inst.*, 970 F.3d at 389 (Sentell, J., dissenting).
42. *See id.* at 388.
43. *Id.*
44. *Id.*
45. *Id.*

based purely upon standing, the resolution adopted by the court, in effect, struck the provisions with the strongest connection to the merit-based objections.

Barr v. American Association of Political Consultants

Bethel Etta

140 S. CT. 2335 (2020)

In *Barr v. American Association of Political Consultants*,[1] the U.S. Supreme Court affirmed the Fourth Circuit's decision to invalidate a 2015 amendment to the Telephone Consumer Protection Act (TCPA), which created an exception to the prohibition against robocalls for calls made to collect a debt owed to the federal government.[2] The Court affirmed that the government-debt exception to the restriction against robocalls was an unconstitutional content-based restriction on speech that failed strict scrutiny.[3] The Court incorporated traditional severability principles to invalidate and sever the government-debt exception amendment of the TCPA.[4]

I. BACKGROUND

In response to several million consumer complaints submitted to the federal government, Congress enacted the Telephone Consumer Protection Act of 1991 to prohibit robocalls to cell and home phones.[5] Congress justified its prohibition against robocalls as "the only effective means of protecting telephone consumers"[6] from the nuisance and invasion of privacy caused by incessant phone calls from automated telemarketers.[7] In 2015, an amendment to the TCPA created an exception to allow robocalls for the purpose of "collect[ing] a debt owed to or guaranteed by the United States."[8]

Plaintiffs are the American Association of Political Consultants and other political organizations that engage in political telemarketing.[9] Plaintiffs operate their organizations by making calls to citizens to "discuss candidates and issues, solicit donations, conduct polls, and get out the vote."[10] Plaintiffs claimed that the prohibition against robocalls to cell phones hindered their outreach; they sought a declaratory judgment in the lower courts against the U.S. Attorney General and the FCC, citing First Amendment violations.[11]

1. Barr v. Am. Ass'n. of Pol. Consultants, 140 S. Ct. 2335 (2020).
2. *Id.* at 2343–44.
3. *Id.* at 2343–45.
4. *Id.* at 2352.
5. *Id.* at 2344.
6. 47 U.S.C. § 227 (2020).
7. *Barr*, 140 S. Ct. at 2344.
8. 47 U.S.C. § 227(b).
9. *Barr*, 140 S. Ct. at 2345.
10. *Id.*
11. *Id.*

The U.S. District Court for the Eastern District of North Carolina ruled that the government-debt exception to robocall restrictions was a content-based restriction, but that it could survive strict scrutiny because of a compelling government interest to collect debt.[12] The U.S. Court of Appeals for the Fourth Circuit vacated the district court and ruled that the government-debt exception was unconstitutional and could not survive strict scrutiny.[13] Following traditional severability principles, the Fourth Circuit further ruled that the government-debt exception is severable from the underlying robocall restriction of the TCPA.[14]

Because the ruling invalidated a part of a federally enacted statute, the Government petitioned for writ of certiorari and plaintiffs supported the petition, believing the Court of Appeals did not provide sufficient relief and the court should have invalidated the entire robocall restriction.[15]

II. ANALYSIS

A. TCPA's Government-Debt Exception is an Unconstitutional Content-Based Restriction

The initial First Amendment question presented is whether the TCPA's robocall restriction, with the government-debt exception, is a content-based restriction.[16] The Court held that it was.[17] A law regulating speech is a content-based restriction if it "on its face draws distinctions based on the message the speaker conveys" and "singles out specific subject matter for differential treatment."[18] The Court noted that § 227(b)(1)(A)(iii), the provision outlining the government-debt exception for robocalls, conditions the legality of robocalls on whether they are made to collect debts owed to the federal government and stated that such preference for the type of permissible robocalls was a clear example of a content-based restriction.[19]

The Government advanced three arguments that the government-debt exception of the TCPA was content-neutral, all of which the Court found unpersuasive.[20] First, the Government suggested that § 227(b)(1)(A)(iii) differentiated speech based on speakers, i.e., authorized debt collectors, not based on the content of the speech.[21] The Court rejected this argument, citing that the text of the statute singles out robocalls "made solely to collect a debt owed to or guaranteed by the United States," not *all* robocalls made from authorized debt collectors. [22] The Court additionally noted that even if the statute's distinction was based on the speaker, it does not "automatically

12. *Id.*
13. *Id.* at 2345.
14. *Id.*
15. *Barr*, 140 S. Ct. at 2346.
16. *See id.*
17. *Id.*
18. *Id.* (quoting *Reed v. Town of Gilbert*, 576 U.S. 155 (2015)).
19. *Id.* at 2347.
20. *See id.* at 2346–47.
21. *Barr*, 140 S. Ct. at 2346–47.
22. *Id.* at 2347 (emphasis added).

render the distinction content neutral."[23] Second, the Government argued that the legality of a robocall does not depend on the content of the speech, but instead on whether the caller engages in a particular economic activity.[24] The Court, again, was unpersuaded because the statute in this case focuses on whether the caller *speaks* about a particular topic.[25] Lastly, the Court rejected the Government's claim that deeming the government-debt exception as an unconstitutional content-based restriction would lead to a slippery slope invalidating most forms of economic regulation.[26] The Court dismissed this concern stating that "the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech."[27] And the Court assured that the judiciary can distinguish between impermissible content based restrictions and ordinary regulations of commercial activity that impose only incidental burdens on speech.[28]

The Court concluded that the government-debt exception was content-based and therefore subject to strict scrutiny review.[29] The Government itself conceded that it could not satisfy strict scrutiny because it could not fully justify the distinction between government debt collection speech and other modes of robocall speech.[30] The Court, therefore, held that the government-debt was an unconstitutional content-based restriction on speech.[31]

B. Severability

Next, the Court turned to the question of whether to strike down the entirety of the 1991 robocall restriction or to only sever the government-debt exception instead. The Court recognized that Congress's competing interests in debt collection as well as consumer privacy can concurrently exist: "Congress's addition of the government-debt exception in 2015 does not cause [the Court] to doubt the credibility of Congress's continuing interest in protecting consumer privacy."[32] So the Court applied traditional principles of severability and only struck the unconstitutional 2015 amendment.[33]

Where a federal statute contains an express severability or non-severability clause, the Court will adhere to the text of the clause.[34] Where Congress does not include such clauses, courts may often presume that an unconstitutional provision is severable from the remainder of the statute.[35] The Court's preference for partial invalidation in its tendency to presume severability stems from its efforts to avoid "judicial policy making or de facto

23. *Id.* (quoting *Reed*, 576 U.S. at 170).
24. *Id.*
25. *Id.* at 2347.
26. *Id.*
27. *Barr*, 140 S. Ct. at 2347 (quoting Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011)).
28. *Id.*
29. *Id*. (quoting *Reed*, 576 U.S. at 165).
30. *Id.*
31. *Id.* at 2347.
32. *Id.* at 2348.
33. *See Barr*, 140 S. Ct. at 2349.
34. *Id.* at 2349.
35. *Id.* at 2350.

judicial legislation in determining just how much of the remainder of a statute should be invalidated."[36] In this case, however, the presumption of severability was unnecessary because the severability clause in the Communications Act covered the TCPA's robocall restriction and its subsequent government-debt exception.[37]

The Court also considered the equal protection principles implicated by the First Amendment violations—in this case, Congress favoring government-debt collection robocalls and discriminating against other robocalls.[38] The Court weighed the possible cures for this unequal treatment and considered either "extending the benefits or burdens to the exempted class" or "nullifying the benefits or burdens for all."[39] The Court chose the latter and severed the government-debt exception to cure unequal treatment and left the longstanding general robocall restriction in place.[40]

III. CONCLUSION

The Court upheld the Fourth Circuit's judgment that the government-debt exception to the TCPA's restrictions against robocalls was unconstitutional and cured the violation by invalidating and severing it from the remainder of the statute.[41]

36. *Id.* at 2352.
37. *Id.*
38. *Barr*, 140 S. Ct. at 2354.
39. *Id.*
40. *Id*. at 2355.
41. *Id*. at 2356.