University of Florida Journal of Law & Public Policy

VOLUME 33 SPRING 2023 ISSUE 2

STATEMENT OF PURPOSE

The *University of Florida Journal of Law & Public Policy* is an interdisciplinary organization whose primary purpose is the publication of scholarly articles on contemporary legal and social issues facing public policy decisionmakers. The *Journal* is composed of two governing bodies: the Advisory Board and the Executive Board. The Advisory Board is comprised of faculty and honorary members who provide independent guidance. The Executive Board, which includes both law and graduate students, is responsible for researching and preparing each volume for publication. The Executive Board also selects the articles that are published. All student members must complete a writing requirement and help research and prepare the *Journal* for publication.

ACKNOWLEDGMENT

This issue of the *University of Florida Journal of Law & Public Policy* is a direct result of the collaboration and hard work of the *Journal* members, staff, advisors, sponsors, and contributing authors.

The *Journal* extends its deep appreciation for the generosity of the University of Florida Fredric G. Levin College of Law and the Huber C. Hurst Fund in supporting and assisting the *Journal* in its publication of this issue and for supporting our interdisciplinary journal concept.

Special thanks to our faculty advisor, Professor Stacey Steinberg, and our staff editor, Lisa-Ann Caldwell.

The *University of Florida Journal of Law & Public Policy* (ISSN# 1047-8035) is published three times per year and is sponsored by the Warrington College of Business Administration and the Levin College of Law, University of Florida. Printed by Western Newspaper Publishing Co., Indianapolis, IN.

Editorial and Business Address: Fredric G. Levin College of Law, University of Florida, P.O. Box 117636, 309 Village Dr., 127 Holland Hall, Gainesville, FL 32611. Phone: (352) 273-0671. Email Address: jlpp@law.ufl.edu.

Subscriptions: $60.00 U.S. domestic per volume plus sales tax for Florida residents and $65.00 U.S. international. Single issues are available for $25.00 U.S. domestic and $30.00 U.S. international.

University of Florida
Journal of Law & Public Policy

VOLUME 33 SPRING 2023 ISSUE 2

FOREWORD

For many years, the Center for Governmental Responsibility at the University of Florida Levin College of Law and the Brechner Center for Freedom of Information at the University of Florida College of Journalism and Communications have hosted the Technology, Media, and Privacy Law (TMPL) Conference. The TMPL Conference provides a forum for discussions by legal professionals, policy experts, and academics on how technology should be regulated and integrated in the United States and around the world. In March 2022, the TMPL Conference placed a special emphasis on emerging issues in artificial intelligence (AI) and privacy. Specifically, the 2022 TMPL Conference explored the legal and ethical concerns raised by AI and assessed the opportunities that automation can offer to society.

Volume 33, Issue 2, of the *University of Florida Journal of Law & Public Policy* is a special issue dedicated to the interaction between technology, privacy, media, and the law. The issue features contributions by the following scholars from the 2022 TMPL Conference: Amy K. Sanders, Jon Mills, Kendra Albert, and Russell Weaver. Authors Jiaying Jiang, Karman Lucero, Hannah Shankman, Caroline Bradley-Kenney, Daxton "Chip" Stewart, Avatara Smith-Carrington, and Lindsey Joost, while not participants in the 2022 TMPL Conference, were selected to be included in this issue because of their innovative academic and policy-oriented insights regarding technology and the law.

This issue is also dedicated to the University of Florida Levin College of Law Class of 2023. Congratulations, and may we all uphold the rule of law and use it as a force for justice in this world of advancing technology.

Jessica R. Pearce, Editor-in-Chief

University of Florida Journal of Law & Public Policy

VOLUME 33 SPRING 2023 ISSUE 2

ARTICLES

NOTE

LET'S NOT BE DUMB: GOVERNMENT TRANSPARENCY, PUBLIC RECORDS LAWS, AND "SMART CITY" TECHNOLOGIES

Amy Kristin Sanders[*] *& Daxton R. Stewart*[**]

Abstract

As the tools to automate our lives become more commonplace, so do the concerns about their use and the data they collect. State and local governments in the United States are increasingly turning to smart city technologies for everything from law enforcement and traffic management to public health monitoring and wastewater testing. Yet often, citizens are left in the dark about the ways in which their elected officials are researching, purchasing, and implementing these technologies. Public records laws represent one mechanism to help improve the public's understanding of smart city technology and its uses in their communities. But not all public records laws are created equal. We argue that public records laws must be updated to ensure the definition of the term "public records" includes the types of records created by these technologies, including audio, video, and large datasets. Additionally, exemptions to public records laws that were designed to prevent invasions of privacy or ensure law enforcement could investigate crime must be narrowly tailored so they cannot be used as an excuse to withhold information that citizens have a right to access. Strong public oversight is crucial to guarantee these technologies are not abused, and most state public records laws are inadequate when it comes to ensuring access to records about, and created by, smart city technology.

* Amy Kristin Sanders, J.D./Ph.D., is an associate professor of journalism and media at the University of Texas at Austin, where she also holds a courtesy appointment in the law school.

** Daxton R. Stewart, J.D./Ph.D., is a professor of journalism at Texas Christian University, where he serves as the assistant provost for research.

INTRODUCTION

Americans heading out to protest the U.S. Supreme Court's summer 2022 decision to overturn *Roe v. Wade* had more to think about than their 1970s predecessors.[1] The rise in smart city technologies means it is more likely that local, state, and federal government agencies can identify them and track their movements. It came to light that Baltimore, Maryland, used facial recognition technology as individuals gathered in protest of the 2015 police killing of Freddie Gray, identifying members of the crowd who had outstanding warrants and arresting them at the protest.[2] Since then, facial recognition has been used by police during protests in other major cities, including New York, Miami, and Washington, D.C.[3] But it is not just facial recognition technology that should concern protestors—the rise of smart city technologies increase the reach of near-constant surveillance.

From cameras to sensors and microphones to mobile phone apps, smart city technologies have become mainstream. State and local governments have become particularly interested in these technologies because of their promises to increase the efficiency of delivering services and to improve the quality of life for residents.[4] "Smart cities . . . collect and analyze data. The cities use this data to improve infrastructure, public

1. *See* Roe v. Wade, 410 U.S. 113, 164 (1973) (holding that the state may not regulate the termination of pregnancy in the first trimester), *overruled by* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022). On June 24, 2022, the Supreme Court, in a 6-1 decision, upheld the constitutionality of Mississippi's Gestational Age Act, which prohibited nearly all abortions after 15 weeks. The majority held there was no constitutional right to an abortion, overruling two previous decisions upholding abortion rights as part of the implied right to privacy. *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022).

2. Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ [https://perma.cc/3ENA-953P].

3. *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, NEW AM. (June 3, 2021), https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/ [https://perma.cc/424V-CJW9].

4. Leon Erlanger, *State and Local Governments Embrace IoT, Including in Smart Cities*, STATE TECH MAG. (July 28, 2016), https://statetechmagazine.com/article/2016/07/state-and-local-governments-embrace-iot-including-smart-cities [https://perma.cc/4FTJ-Q6TG].

utilities and services, and more."[5] The technologies have also piqued the interest of consumers, who are purchasing Internet-connected devices in the form of wearables and smart home devices, including Apple's smart watch and Nest's smart thermostat.[6] Research suggests exponential growth in the sales of these devices, with the total number of smart devices connected to the Internet rising to 3.75 billion by 2025.[7]

But the technology is not without danger. Smart devices and other Internet-connected devices, commonly dubbed the Internet of Things, may offer conveniences, but privacy experts are troubled by the amount of data they collect. Need to turn down the temperature at your home from your office? Your Nest smart thermostat is collecting this information, documenting the patterns of your energy usage. Security Scorecard detailed the threats these smart devices pose in an August 2021 report.[8] Insecure storage and transfer of data were highest among those concerns.[9]

As more and more consumers, businesses, and governments rely on these technologies, they pose more and more potential dangers. In a recent report, Deloitte pointed to concerns about cybersecurity in municipal infrastructure, public transportation, and healthcare services.[10] These concerns are not new. Professors Woodrow Hartzog and Evan Sellinger offered cautionary words about smart technologies as far back as 2016:

---

5. Fariza Sabrina & Julian Jang-Jaccard, *Entitlement-Based Access Control for Smart Cities Using Blockchain*, 21 SENSORS 1, 1 (2021) ("Smart cities use the Internet of Things (IoT) devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities, and services.").

6. *See* Filipe Espósito, *There Are More than 100 Million People Wearing an Apple Watch, Says Analyst*, 9TO5MAC (Feb. 11, 2021, 8:01 PM), https://9to5mac.com/2021/02/11/there-are-more-than-100-million-people-wearing-an-apple-watch-says-analyst/#:~:text=Just%20in%2020 20%2C%20Apple%20sold,already%20own%20an%20Apple%20Watch [https://perma.cc/5HAX-TQAZ] (explaining that as of December 2020, over 100 million people wear an Apple watch); *see also* Parks Associates, *27% of Smart Thermostat Owners Report Owning a Nest Thermostat*, PR NEWSWIRE (Oct. 26, 2022), https://www.prnewswire.com/news-releases/parks-associates-27-of-smart-thermostat-owners-report-owning-a-nest-thermostat-301659852.html [https://perma.cc/3VDQ-PYWY] ("About one in four, equaling roughly 15 million households, report owning a Google Nest thermostat.").

7. *How IoT and Smart City Technology Works: Devices, Applications and Examples*, INSIDER INTEL. (Apr. 15, 2022), https://www.insiderintelligence.com/insights/iot-smart-city-technology/ [https://perma.cc/79N6-XEH2].

8. *7 Internet of Things Threats and Risks to Be Aware of*, SEC. SCORECARD (Aug. 4, 2021), https://securityscorecard.com/blog/internet-of-things-threats-and-risks [https://perma.cc/25T7-39UK].

9. *Id.*

10. *Cyber Risk in an Internet of Things World*, DELOITTE, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html [https://perma.cc/V7BN-KC25] (last visited Apr. 5, 2023).

> While the IoT might be incredibly useful, we should proceed carefully . . . . Each new camera, microphone, and sensor adds another vector for attach and another point of surveillance in our everyday lives . . . . [T]he nature of the "thing" in the IoT should play a more prominent role in privacy and data security law. The decision to wire up an object should be coupled with responsibilities to make sure its users are protected.[11]

Despite this warning, very little has been done to regulate these devices to safeguard users' data.

Not all citizens have embraced a reliance on these technologies. Government use of IoT devices and smart city technologies raises significant concerns given the lack of transparency in how they are adopted and implemented. Eugenie Birch, who directs the Penn Institute for Urban Research, voiced those concerns:

> I also think there is a lack of rules around the use of technology, so that also makes people quite uncomfortable. Some of these complaints are justified because, in the face of an absence of control around the use of the collected data, it can be like the Wild West out there. Even the providers would welcome more transparency and accountability in this area.[12]

Ms. Birch is not alone. Numerous advocacy groups, including the American Civil Liberties Union[13] and Amnesty International,[14] have publicized their concerns about facial recognition technology, noting its impact on citizens' constitutional rights. Another controversial technology known as ShotSpotter purports to detect gunshots.[15] Based on concerns about effectiveness, community organizations have demanded Chicago officials stop using the "smart" microphones, which report

---

11. Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & TECH. 581, 581 (2016) (italics omitted).

12. Eugénie L. Birch, *Why Is There a Backlash to Smart Cities*, BRINK NEWS (Dec. 11, 2019), https://www.brinknews.com/why-is-there-a-backlash-to-smart-cities/ [https://perma.cc/U9JT-LT4G].

13. *The Fight to Stop Face Recognition Technology*, AM. C.L. UNION (July 15, 2021), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance [https://perma.cc/WF56-D5SZ].

14. *Ban Dangerous Facial Recognition Technology that Amplifies Racist Policing*, AMNESTY INT'L (Jan. 26, 2021), https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ [https://perma.cc/7QX3-URG5].

15. Matt Masterson, *Activists Call on Chicago Officials to Dump ShotSpotter Contract*, WTTW (Aug. 19, 2021), https://news.wttw.com/2021/08/19/activists-call-chicago-officials-dump-shotspotter-contract [https://perma.cc/T4TM-G5JU].

directly to the police.[16] Even researchers at Northwestern University's MacArthur Justice Center doubt the value of the technology, documenting more than 40,000 errant reports in twenty-one months.[17]

Public records laws represent one legal tool to improve transparency and accountability for governments implementing smart technologies. In the first part of this Article, we outline the potential benefits and drawbacks of these technologies. Then we argue that citizens have certain rights in a smart city. To advance those rights, we examine the role that public records laws play in providing stronger oversight. We argue that three key aspects of public records laws must be evaluated to ensure they adequately address smart city technologies: the definition of record as well as the scope of the privacy and law enforcement exemptions. We conclude that there is a need for stronger public records laws to ensure stronger oversight as more and more governments adopt smart city technology.

I. THE BENEFITS AND CONSEQUENCES OF SMART CITY TECHNOLOGY

Governments implement these smart technologies for their common core function: monitoring. This monitoring function brings with it both benefits and consequences. These technologies may offer government officials early notification that something is amiss. But these technologies may also increase the frequency of citizens' interactions with government and law enforcement officials. Further, numerous scholars have identified the disparate impact of surveillance technologies, noting they often disadvantage already marginalized groups.[18] Two increasingly popular technologies, both of which have made headlines recently, offer excellent examples of how these technologies raise civil rights concerns. Wastewater surveillance is not a new practice, but U.S. government agencies have increasingly relied on it since the coronavirus pandemic began in 2020.[19] ShotSpotter is a gun-shot detection technology that law

16. *Id.*

17. *ShotSpotter Creates Thousands of Dead-End Police Deployments that Find No Evidence of Actual Gunfire*, MACARTHUR CTR. FOR JUST., https://endpolicesurveillance.com/ [https://perma.cc/6KRD-ZYNS] (last visited Apr. 5, 2023).

18. *See, e.g.*, BARTON GELLMAN & SAM ADLER-BELL, CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE 2 (2017) ("Mass surveillance society subjects us all to its gaze, but not equally so. Its power touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status."); Christopher Jones, *Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation*, 22 N.C. J.L. & TECH. 777, 786 (2021) ("Since human judgment is required for programming and training data, implicit biases present in humans may creep into the machine's processes and produce biased results.").

19. Stephanie Desmon, *How COVID-19 Created a Watershed Moment for Wastewater Surveillance*, JOHNS HOPKINS BLOOMBERG SCH. PUB. HEALTH (May 13, 2022),

enforcement agencies have begun to deploy in cities around the United States.[20] Both are discussed in detail below.

Governments have monitored wastewater outputs to track disease for many decades.[21] By collecting water at select points in a municipality's wastewater system, scientists can determine the concentration of bacteria and viruses present in the samples.[22] But the public's knowledge of this practice, which can detect everything from HIV to COVID-19, was limited prior to the coronavirus pandemic.[23]

Within months of the COVID-19 pandemic taking hold in the United States, the Centers for Disease Control and Prevention (CDC) established the National Wastewater Surveillance System as means of tracking SARS-CoV2, the virus that causes COVID-19.[24] But this technology can be used to monitor far more than just infectious diseases. Some agencies have used it to measure opioid levels, allowing scientists to "track infections at a community level in a population-based way."[25] Taken in the best light, wastewater surveillance may be able to prevent the next public health crisis in the United States, but privacy experts have urged caution. After the CDC's rollout of its national effort, the Government Accountability Office issued this warning in April 2022: "[W]astewater contains not only a pathogen's genetic data that allow public health officials to identify the pathogen, but also human genetic data that could potentially be misused. Additionally, communities may be stigmatized if wastewater surveillance data indicate pathogen spread or illicit drug use."[26] Yet little has been done to address the privacy concerns associated with government surveillance of wastewater.

---

https://publichealth.jhu.edu/2022/how-covid-19-created-a-watershed-moment-for-wastewater-surveillance [https://perma.cc/L9CG-2UV5].

20. *See* Garance Burke et al., *How AI-Powered Tech Landed Man in Jail with Scant Evidence*, AP NEWS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220 [https://perma.cc/MMS5-GG6S] ("Police chiefs call ShotSpotter a game-changer. The technology, which has been installed in about 110 American cities, large and small, can cost up to $95,000 per square mile per year.").

21. *See, e.g.*, T.G. Metcalf et al., *Environmental Virology: From Detection of Virus in Sewage and Water by Isolation to Identification by Molecular Biology—A Trip of Over 50 Years*, 49 ANN. REV. MICROBIOLOGY 461, 463 (1995) (noting that wastewater surveillance of poliovirus occurred in major U.S. cities beginning in the early 1940s).

22. *See id.* at 463–64 (discussing instances of scientists collecting and examining samples of wastewater for detection of viruses).

23. Desmon, *supra* note 19.

24. *National Wastewater Surveillance System*, CDC (Dec. 22, 2022), https://www.cdc.gov/healthywater/surveillance/wastewater-surveillance/wastewater-surveillance.html [https://perma.cc/T9BU-KWP3].

25. Desmon, *supra* note 19.

26. U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105841, SCI. & TECH SPOTLIGHT: WASTEWATER SURVEILLANCE 2 (2022).

Like wastewater surveillance, ShotSpotter technology seems promising on its face. It relies on the installation of microphones in public spaces to detect the sound of gunfire.[27] Proponents argue the technology increases police responsiveness, shaving critical minutes off response times.[28] In theory, cities using ShotSpotter should be able to reduce the number of gun deaths and potentially catch more suspects. In practice, researchers have found the technology, "which has been installed in about 110 American cities . . . . in neighborhoods deemed to be the highest risk for gun violence, which are often disproportionately Black and Latino communities,"[29] does not live up to its promises.[30] "[T]he technology does not reduce firearm violence in the long-term, and the implementation of the technology does not lead to increased murder or weapons related arrests."[31] Regardless of the technology's ineffectiveness in aggregate, ShotSpotter recordings—like those of other smart technologies, including Alexa and Echo—are increasingly being used in criminal trials.[32]

II. CITIZENS' RIGHTS IN A SMART CITY

Citizens in a democratic society have a right to participate in the structuring and maintenance of their communities. Not surprisingly, many scholars have recently turned their focus to the role of citizens in the rise of the smart city. Although governments may envision greater interactions, most projects involve only *de minimis* citizen participation. A deeper relationship might develop if citizens were "valued and trustworthy collaborators in the develop and the governance of public space."[33] However, Els Leclercq and Emiel Rijshouwer's research suggests this is not the case:

> [D]espite the fact that smart city governments and corporations increasingly use a participatory and citizen-centric rhetoric, researchers and activists do not necessarily find that they fundamentally changed the neoliberal and

27. Mitchell L. Doucette et al., *Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: A Longitudinal Analysis, 1999–2016*, 98 J. URB. HEALTH 609, 610 (2021).

28. *Id.*

29. Burke et al., *supra* note 20.

30. *See* Doucette et al., *supra* note 27 (describing the results of various studies on the effectiveness of gunshot detection technology (GDT) and ShotSpotter, including that GDT does not "impact the level of reported gun crimes" and that ShotSpotter does not "improve case closures").

31. Burke et al., *supra* note 20 (internal quotations omitted).

32. *See* Doucette et al., *supra* note 27, at 609 (examining the evidence suggesting that ShotSpotter implementation does not lead to a reduction in firearm related homicides and suggesting policy solutions as more cost-effective measures).

33. Burke et al., *supra* note 20.

> surveilling nature of their projects, or that this contributed to more equal and just cities. [34]

After World War II, Henri Lefebvre argued that democratic participation includes citizen involvement in urban planning and policy in *Le Droit à la Ville*.[35] Lefebvre posited that citizens have a right to shape public spaces in their communities and to help determine their use.[36] Engin Isin colorfully characterized this as "the right to wrest the use of the city from the privileged new masters and democratize its space."[37] Edésio Fernandes advanced Isin's work, noting the importance of "the right to information; the right of expression; . . . the right to self-management, that is, the democratic control of the economy and politics; the right to public and non-public services."[38]

Drawing upon Fernandes' work, we argue that citizens in a smart city have specific rights to information that they should be able to exercise through the use of public records laws:

1. Citizens have a right to know which technologies are being employed.
2. Citizens have a right to know how money is being spent.
3. Citizens have a right to know what data is being collected.
4. Citizens have a right to know how data is being used.
5. Citizens have a right to independent oversight.

A. *Using Public Records Laws to Advance Citizens' Rights*

Open records laws provide the public with the right to access federal and state government records and meetings—including those related to the use of smart city technologies.[39] Access to government information is

---

34. Els M. Leclercq & Emiel A. Rijshouwer, *Enabling Citizens' Right to the Smart City Through the Co-Creation of Digital Platforms*, URB. TRANSFORMATIONS, Mar. 2022, at 2.

35. HENRI LEFEBVRE, LE DROIT À LA VILLE *passim* (1968).

36. *See* Nayeli Riano, *Henri Lefebvre and the Urban Revolution*, IMAGINATIVE CONSERVATIVE (Feb. 21, 2020), https://theimaginativeconservative.org/2020/02/henri-lefebvre-urban-revolution-nayeli-riano.html [https://perma.cc/28YJ-2K9F] (explaining that *Le Droit à la Ville* "argued for a human 'right to the city' where local authorities reclaim the city as a co-created space that is detached from the growing effects that commodification and capitalism have had over social interaction" and "aimed to rectify, through urban planning, the spatial inequalities in cities").

37. ENGIN F. ISIN, DEMOCRACY, CITIZENSHIP AND THE GLOBAL CITY 14 (1st ed. 2001).

38. Edésio Fernandes, *Constructing the 'Right to the City' in Brazil*, 16 SOC. & LEGAL STUD. 201, 208 (2007).

39. *See, e.g.*, 5 U.S.C. § 552b(b) (1976) ("[E]very portion of every meeting of an agency shall be open to public observation."); FLA. STAT. § 286.011(1) (2022) ("All meetings of any board or commission of any state agency or authority or of any agency or authority of any county, municipal corporation, or political subdivision . . . are declared to be public meetings open to the

a fundamental democratic value. U.S. President James Madison once said, "[k]nowledge will for ever [sic] govern ignorance: and a people who mean to be their own Governours, must arm themselves with the power which knowledge gives."[40] By providing the public with access to these documents and proceedings, open records laws help voters hold their governments accountable. Shortly before joining the U.S. Supreme Court, civil rights defender Louis Brandeis noted, "[s]unlight is said to be the best of disinfectants."[41]

The idea behind open records and meetings laws is to provide additional transparency to the carrying out of government duties. As the Texas Public Information Act points out in its opening, "government is the servant and not the master of the people," and that while the people delegate authority to government, they "insist on remaining informed so that they may retain control over the instruments they have created."[42] In no small part, this is because government officials are spending taxpayer money as they govern. Because of the costs and intrusiveness associated with smart city technology, oversight is essential for the protection of our fundamental rights. Often, however, residents know little to nothing about these technologies before they are implemented. Lack of transparency and oversight run counter to our democratic heritage; Judge Damon Keith once wrote that "[d]emocracies die behind closed doors."[43]

The more technologies government agencies employ, the more these agencies become warehouses of public data—and targets for malicious actors. Given the decreasing cost of gathering and storing information, it is not unusual for even municipal governments to possess "an extensive range of personal and sensitive data . . . with relatively few encumbrances from superior levels of government."[44] Much of this data is collected by, stored by, or shared with third-party vendors,[45] raising serious concerns about privacy and security given the weak data protection laws in the United States.

---

public at all times."); TEX. GOV'T CODE ANN. § 552.001(a) (West 2021) ("[I]t is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees.").

40. Letter from James Madison, President of the United States, to William T. Barry, Lieutenant Governor of Kentucky (Aug. 4, 1822), https://founders.archives.gov/documents/Madison/04-02-02-0480 [https://perma.cc/F292-WWDH].

41. Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WKLY., Dec. 20, 1913, at 10.

42. TEX. GOV'T CODE ANN. § 552.001(a) (2021).

43. Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).

44. Ira S. Rubinstein & Bilyana Petkova, *Governing Privacy in the Datafied City*, 47 FORDHAM URB. L.J. 755, 791 (2020).

45. *See id.* at 792 (explaining that data stewardship includes managing third-party vendors "because so many smart city developments depend on public-private partnerships").

Smart city technologies are permeating municipal governance. From smart transportation systems that monitor public and private transit, to smart infrastructure, including water systems and power grids, these Internet-connected technologies allow for ever-increasing amounts of surveillance.[46] The growing use of CCTV in major cities from London to New York also raises issues related to the tracking and monitoring of private individuals.[47]

Smart city technologies thrive on constant, omnipresent data flows captured by cameras and sensors placed throughout the urban landscape. These devices pick up all sorts of behaviors, which can now be cheaply aggregated, stored, and analyzed to draw personal conclusions about city dwellers.[48]

Legal scholarship on smart city technology primarily addresses privacy concerns. But some scholars have raised the issue of government transparency in the use of these technologies. Ira Rubinstein and Bilyana Petkova describe the possibility of "data stewards," functioning as a "hybrid between a public institution seeking to act in the public interest and as a business corporation seeking to maximize profits," noting the opportunity for public-private partnerships engaged in contractual data-sharing arrangements.[49] These partnerships, like all public-private partnerships, often land in the gray area of open records and meetings laws, leaving the public without meaningful oversight.[50] One example: efforts were undertaken to exempt Seattle's dockless bike program from public records laws.[51] Another: despite being a public project, Waterfront Toronto, Google's Sidewalk Labs' attempt to create a smart city, was

46. Kelsey Finch & Omar Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1583–90 (2014).

47. *Id.* at 1598.

48. *Id.* at 1582.

49. Rubinstein & Petkova, *supra* note 44, at 773.

50. *See* Amy Kristin Sanders & Daxton "Chip" Stewart, *Secrecy, Inc.: How Governments Use Trade Secrets, Purported Competitive Harm and Third-Party Interventions to Privatize Public Records*, 1 J. CIVIC INFO. 1 (2019) ("As governments engage in public-private partnerships, they have devised ways to shield the public's business from the traditional level scrutiny offered by citizens and journalists, watchdogs of the public trust.").

51. *See* Amy Kristin Sanders et al., *Is It Just Dumb Luck? The Challenge of Getting Access to Public Records Related to Smart City Technology*, J. CIVIC INFO. (forthcoming 2023) (manuscript at 11), https://www.nfoic.org/wp-content/uploads/2022/10/SmartCities.pdf [https://perma.cc/5Z5R-2UY8] ("The data stewardship examples they [Rubinstein and Petkova] examined, however, did not always play nicely with public records laws, as . . . [there were] efforts to exempt from public records laws . . . data gathered through Seattle's dockless bike program."). *See generally* Rubinstein & Petkova, *supra* note 44, at 811 (discussing how Seattle piloted a program for dockless bikes in 2017).

exempt from public records requests, locking off the public's ability to ensure accountability.[52]

Some have proposed using de-identification to ensure that data in a smart city can be shared with the public while protecting individuals' privacy.[53] But de-identification is not perfect. In critiquing the use of facial recognition technology, Woodrow Hartzog and Evan Selinger argue that it is inadequate to protect individual privacy interests.[54]

Even when information about smart city technologies is available, the algorithms that power their data analyses are often not open source.[55] Such is the case with ShotSpotter, a private company that refuses to release information about its algorithm for gunshot detection.[56] Seemingly a public records gray area, private ownership of algorithmic records of technology used by government entities often allows that information to remain secret.[57] Even the government agencies themselves are unsure whether to release the information. A 2018 study that requested public records related to smart city technology's algorithms from forty-two agencies in twenty-three states received responses across the spectrum: "The barriers we encountered amount to substantial limitations on public access to information about algorithms, even if some of them could be overcome with more time and money."[58]

Given these challenges, it is clear that state public records laws must be amended to ensure better access to information about smart city technology. For the public to engage in appropriate oversight and ensure individuals' rights are being protected anytime government entities purchase and employ these tools, changes must occur. Three key issues must be addressed: (1) defining the term "public records" broadly; (2) defining privacy exemptions narrowly; and (3) narrowing law enforcement exemptions.

---

52. Ellen P. Goodman & Julia Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457, 464 (2019).

53. Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94 N.Y.U. L. REV. 581, 583–84 (2019).

54. Woodrow Hartzog & Evan Selinger, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1754 (2020).

55. *See* Katherine Fink, *Opening the Government's Black Boxes: Freedom of Information and Algorithmic Accountability*, 21 INFO., COMMC'N. & SOC'Y 1453, 1453 (2017) ("[G]overnment operations increasingly involve algorithms. While algorithms can make agency activities and decisions more efficient, they also hide information inside 'black boxes', away from public view. Whether freedom of information laws allow, or should allow, the public to see inside those black boxes is not clear.").

56. Helen Webley-Brown et al., *ShotSpotter and the Misfires of Gunshot Detection Technology*, SURVEILLANCE TECH. OVERSIGHT PROJECT (July 14, 2022), https://www.stopspying.org/shotspotter [https://perma.cc/PBS8-H87L].

57. Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107–09 (2018).

58. *Id.* at 136.

B. *Public Records Laws Must Broadly Define Records*

Most state public records laws include a definition for what constitutes a record within a definitions section in the statute, but those definitions are far from uniform. As we previously found, a majority of states define the term "public records" broadly in a way that encompasses modern recordkeeping.[59] Florida's public records law provides an example of this approach:

> "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.[60]

South Carolina's law represents a similar take on the broad definition, defining "public record" as including "all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of their physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body."[61] For individuals requesting records related to, or produced by, smart city technology, broadly-worded open records laws that demonstrate an understanding of modern recordkeeping technology provide the most support in favor of transparency.

Some states take a much narrower approach that could give requestors headaches. Alabama's public records law includes a lengthy list of records—except they are all paper documents:

> "[P]ublic records" shall include all written, typed or printed book, papers, letters, documents and maps made or received in pursuance of law by the public officers of the state, counties, municipalities and other subdivisions of government in the transactions of public business and shall also include any records authorized to be made by any law of this state belonging or pertaining to any court of record or any other public record authorized by law or any paper, pleading, exhibit or other writing filed with, in or by any such court, office or officer.[62]

---

59. *See* Sanders et al., *supra* note 51, manuscript at 16 ("A majority of states take a relatively modern and wide-reaching approach to defining a record.").

60. FLA. STAT. § 119.011(12) (2022).

61. S.C. CODE ANN. § 30-4-20(c) (2022).

62. ALA. CODE § 41-13-1 (2019).

Obviously, this language is less than ideal for those seeking information about smart city technology. Modern open records laws must embrace modern recordkeeping practices, including electronic and digital storage of information and data. In 2022, it is hard to argue that government information does not include photographs, video recordings, and audio records. Unless these states have useful case law, individuals requesting access to government records and data in these states may find themselves out of luck. Requestors whose state statutes do not include a definition of "public records" at all, however, may benefit from the lack of specificity, depending on the government entity they encounter.

C. *Public Records Laws Must Narrowly Define Privacy Exemptions*

Given the privacy concerns raised about the amount of data collected and stored when governments use smart technology, balancing individual privacy and government transparency proves challenging. But this is not a new challenge. Governments have regularly used privacy exemptions in public records laws to obfuscate the public's access to information.[63] Even with the proliferation of digital records, governments routinely give privacy the upper hand. Professor Benjamin Cramer noted the irony of governments claiming personal privacy, as it is "used increasingly as the justification for withholding government-held documents under FOIA [Freedom of Information Act] . . . thus preventing public knowledge of governmental operations discussed in those documents," yet the public remains "powerless in reducing the secrecy of the surveillance state."[64]

Video records, which could be used for facial recognition, and audio records, possibly used for voice identification, are particularly likely to be withheld under a claim of personal privacy. Vaguely written exemptions allow for broad interpretation by records custodians. In Maryland, for example, any record that would cause "an unwarranted invasion of personal privacy" can be withheld.[65] But statutory language is not the only issue that transparency advocates have to overcome. Not all state public records laws include a personal privacy exemption, but that does not mean adverse case law does not exist. To determine whether records should be released, Iowa courts employ a multi-part balancing test that examines: "(1) the public purpose of the party requesting the information; (2) whether the purpose could be accomplished without the disclosure of personal information; (3) the scope of the request; (4) whether alternative sources for obtaining the information exist; and (5)

63. Benjamin W. Cramer, *Privacy Exceptionalism Unless It's Unexceptional: How the American Government Misuses the Spirit of Privacy in Two Different Ways to Justify Both Nondisclosure and Surveillance*, 16 OHIO STATE TECH. L.J. 306, 307 (2020).

64. *Id.* at 348.

65. MD. CODE ANN., GENERAL PROVISIONS § 4-351(b)(3) (LexisNexis 2022).

the gravity of the invasion of personal privacy."[66] As a result, many records related to, and produced by, smart city technologies are likely to be withheld based on privacy concerns, even when redaction may offer a path forward.

D. *Public Records Laws Must Narrow the Law Enforcement Exemption*

Many of the smart city technologies governments have adopted serve a surveillance function. As a result, it is no surprise that the law enforcement exemption found in many states' open records laws could prove problematic. Overly broad statutory exemptions inhibit transparency. Colorado's law enforcement exemption has this effect: "Any records of the investigations conducted by any sheriff, prosecuting attorney, or police department, any records of the intelligence information or security procedures of any sheriff, prosecuting attorney, or police department, or any investigatory files compiled for any other law enforcement purpose."[67] Colorado is not alone in drafting overly broad exemptions. Nebraska's language is particularly troubling:

> (5) Records developed or received by law enforcement agencies and other public bodies charged with duties of investigation or examination of persons, institutions, or businesses, when the records constitute part of the examination, investigation, intelligence information, citizen complaints or inquiries, informant identification, or strategic or tactical information used in law enforcement training, except that this subdivision shall not apply to records so developed or received:
>
> (a) Relating to the presence of . . . alcohol or drugs in any body fluid of any person; or [a family member's request for investigation into an employee death in the line of duty].[68]

As government entities begin to amass and share information, broad language like this serves as a serious impediment to requestors. Fire departments, for example, make use of thermal imaging cameras when fighting fires.[69] Would sharing that video with law enforcement then permit an agency to withhold it under the law enforcement exemption? What about when the municipal traffic department shares traffic camera data with police? In many states, the answer may be "yes."

Scholars have already noted instances where requests for information from automated license plate readers have been denied based on the law

66. DeLaMater v. Marion Civ. Serv. Comm'n, 554 N.W.2d 875, 879 (Iowa 1996).

67. COLO. REV. STAT. ANN. § 24-72-204(2)(a)(I) (West 2022).

68. NEB. REV. STAT. § 84-712.05(5) (2012).

69. Ann Szajewska, *Development of the Thermal Imaging Camera (TIC) Technology*, 172 PROCEDIA ENG'G 1067, 1607 (2017).

enforcement exemption.[70] Similarly, police body cameras and dash cameras offer the promise of government transparency, but only if that footage is made publicly available.

Visibility is a critical element of democratic oversight by elected officials, legislative bodies, and communities affected by surveillance. The proliferation of new technologies should prompt us to ask not just what rules ought to constrain the police, but what we need to know in order to decide what the rules ought to be.[71]

Although some agencies are engaging in affirmative disclosures, more often than not, government entities are employing "the reactive model embraced by FOIA."[72] As a result, if citizens do not request the video, it may never see the light of day.

As law enforcement officers increasingly rely on drones, facial recognition, and other smart technology to engage in surveillance of protestors and others engaged in lawful activity, it is likely we will see an increase in requests for these records. As they currently stand, many states' public records laws do not provide adequate transparency with regard to these types of records.

CONCLUSION: THE ESSENTIAL ROLE OF PUBLIC RECORDS LAW IN UPHOLDING CITIZENS' RIGHTS

Public records laws will undoubtedly play a central role in protecting citizens' rights in a smart city. Given the massive amounts of data collected by smart city technologies, public oversight is necessary to ensure governments are not infringing on individual rights. But public records laws may come up short in supporting that oversight. In spirit, these laws are designed to ensure the public can hold government officials and entities accountable. But in practice, they are riddled with outdated language and vague exemptions that could limit access to records related to, and produced by, smart city technologies. As our reliance on artificial intelligence, facial recognition, and other forms of surveillance and monitoring technologies in the provision of government services evolves, so too must our public records laws.

70. The Authors note some exceptions, including Montana and Arkansas. *See* Kearston Wesner & Katie Blevins, *Restraining the Surveillance Society: Comparing Privacy Policies for Automated License Plate Readers in the United States and the United Kingdom*, 18 OHIO STATE TECH. L.J. 99, 138 (2021).

71. Hannah Block-Wehba, *Visible Policing, Technology, Transparency, and Democratic Control*, 109 CAL. L. REV. 917, 978 (2021).

72. *Id.* at 965.

SURVEILLANCE AND POLICING TODAY: CAN PRIVACY AND THE FOURTH AMENDMENT SURVIVE NEW TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND A CULTURE OF INTRUSION?

Jon L. Mills & Caroline S. Bradley-Kenney[*]

Abstract

We are on the verge of a surveillance state. New technologies enable intrusions unimagined two decades ago. Our current culture voluntarily provides intimate personal details that are available to the world and to law enforcement. Current interpretations of Fourth Amendment privacy protections are failing to protect individuals from this brave new world. This Article describes the current state of technology, culture, and deficiencies in the law. We propose a specific test that can provide a workable approach to current and emerging intrusions. That test expands upon existing theories, like the mosaic theory and a reformation of the third-party doctrine, but also relies on the basic Fourth Amendment tenets to protect against unreasonable searches and a potential dragnet state. This Article considers how the test can apply to six intrusive technologies currently in use.

* Jon L. Mills is a Professor of Law, Dean Emeritus, and Co-Director of the Center for Governmental Responsibility at the University of Florida Fredric G. Levin College of Law. Caroline S. Bradley-Kenney was a judicial law clerk for Judge Anthony N. Lawrence III at the Mississippi Court of Appeals. She currently works as a judicial law clerk for Justice David Ishee at the Mississippi Supreme Court. She received a J.D. from the University of Florida Fredric G. Levin College of Law. We would like to thank Kyler Gray for his excellent work researching and revising this Article.

INTRODUCTION

In the contemporary world, personal safety and security are a top priority. Post-9/11 American society traded privacy for security, but this trade-off carries significant risks as technology continues to evolve. Our culture routinely exposes personal information including locations, reading lists, and even what people had for lunch. However, there is a concern about whether the totality of the current technology and our current data driven way of life have incrementally allowed the creation of a surveillance society. The ability of police and security officials to ensure public safety is greatly enhanced by a culture of sharing personal information, the availability of legal, warrantless surveillance tools, and artificial intelligence (AI). But along with greater safety, this new reality and specific surveillance tools can intrude on our private lives. These tools include tower dumps, automatic license plate readers (ALPRs), social media searches, geofencing, closed-circuit television (CCTV) surveillance, and Stingrays.[1] All information law enforcement gathers using these tools can be aggregated and analyzed by AI that can then create an in-depth profile of an individual and identify suspects.[2]

New technologies changed the playing field for law enforcement and security officials. In earlier times, obtaining detailed information on potential suspects might take law enforcement weeks or months of investigating. Now, information is available almost instantly from modern technologies and the Internet. A combination of the culture of disclosure and intrusion, new technologies available for surveillance, and AI to put all that information together creates an environment that places personal privacy at great risk. The Authors believe that these circumstances, taken together, have formed an ecosystem that is

1. For more on tower dumps, *see* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. 109 (2020). For more on ALPRs, *see Street-Level Surveillance: Automated License Plate Readers (ALPRS)*, ELEC. FRONTER FOUND. (Aug. 28, 2017) [hereinafter *Street-Level Surveillance*], https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/2P6L-V8YU]. For more on geofencing, *see* Sarah K. White, *What Is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017, 12:43 PM), https://www.cio.com/article/288810/geofencing-explained.html [https://perma.cc/56MV-Q8ST]. For more on CCTV surveillance, *see What Is CCTV and How Does It Work? Your Questions, Answered*, SECURE IT SEC. CORP. (Dec. 8, 2020) [hereinafter *What Is CCTV*], https://www.secureitsecurities.com/blog/what-is-cctv-and-how-does-it-work-your-questions-answered [https://perma.cc/4L9F-GW62]. For more on Stingrays, *see* Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020, 7:00 AM), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [https://perma.cc/6WWH-WDEQ].

2. However, even with all these modern tools and information, sometimes the wrong person is identified. Consider the story of Zachary McCoy who became the prime suspect for a burglary based on his geolocation during a bike ride. His fate is discussed more fully below.

dangerously close to creating what the Supreme Court might term a "too permeating police surveillance" state.[3]

To note, this Article does not suggest that law enforcement can never use technology to investigate future and current crimes. Some investigations logically occur before a warrant is necessary. With proper warrants and safeguards, technologies can be used to fight crime without burying individual rights. This Article argues that such safeguards must be placed on law enforcement's use of intrusive new technologies to ensure that personal and private information is protected.

Technologies have consistently outrun constitutional protections. The law has simply not kept up with new means of intrusion and the consequences of the current culture of intrusion and disclosure.[4] For example, the Fourth Amendment is designed to protect each of us from unreasonable search and seizure,[5] but determining what constitutes a search grows more challenging as search tools grow more sophisticated. Whether by warrantless wiretapping or warrantless GPS tracking, it is fair to say warrantless information gathering went on for some time before the Supreme Court determined that a particular practice of "gathering" was required to obtain a warrant.[6] The Fourth Amendment is not a declaration of national policy; it is a protection of individual rights against the government.[7] Nevertheless, enforcement of Fourth Amendment rights in specific cases does build a national policy brick by brick. Sometimes, those individual decisions may lead to broader prohibitions or standards. However, this policy is a patchwork, leaving gaps where protections are still needed. Pointedly, at this stage, the Fourth

3. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotations omitted).

4. "The Digital Era is characterized by technology which increases the speed and breadth of knowledge turnover within the economy and society." Jill Shepherd, *What Is the Digital Era?*, *in* SOCIAL AND ECONOMIC TRANSFORMATION IN THE DIGITAL ERA 1 (Georgios Doukidis et al. eds., 2004).

5. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

6. *See Carpenter*, 138 S. Ct. at 2221 ("Having found that the acquisition of Carpenter's [cell-site location information] was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records."); *see also* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that attaching a GPS tracking device to a vehicle and using the device to monitor the vehicle's movements constitutes a search within the meaning of the Fourth Amendment).

7. *See What Does the Fourth Amendment Mean?*, U.S. COURTS, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 [https://perma.cc/8DSP-RSWP] (last visited Feb. 15, 2023) ("On one side of the scale is the intrusion on an individual's Fourth Amendment rights. On the other side of the scale are legitimate government interests, such as public safety.").

Amendment protects information from being used against an individual at trial, but it does not protect that information from being collected.[8]

Law enforcement has always gathered and stored information, but today new technology provides unprecedented reams of data and analytical capacity. In the digital era, information is more readily available than ever, and law enforcement can use AI to aggregate and source all of it. AI can categorize and flag information that would have taken weeks to process manually, even when manual processing would have been altogether impractical.[9] AI utilizes "machine learning" to process and sort gathered information.[10] AI takes a large quantity of information and sorts it—looking for patterns, making predictions, and organizing the information it has sorted.[11] Accordingly, AI profiling is a powerful tool in criminal investigations. Law enforcement can use a person's AI-generated profile to obtain a probable cause search warrant, allowing them to use even more invasive surveillance.[12]

Law enforcement has access to various modes of legal warrantless surveillance tools that gather information that is then sorted through AI to identify suspects in criminal investigations.[13] Many uses of these technologies *could* be considered searches. This Article considers six technologies that have been used in warrantless surveillance: tower dumps, ALPRs, social media, geofencing, CCTV, and Stingrays. Of these six tools, the U.S. Supreme Court has not ruled that any of them require a search warrant, although some state legislatures and some state courts have started regulating their use.[14] Additionally, the Court has not ruled

8. *See* Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, WASH. POST (Apr. 26, 2021, 6:00 AM), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/GGB2-9CHA] (explaining that voluntarily disclosed information can be collected and that the warrant requirement in *Carpenter* can be evaded by buying data through intermediaries).

9. Steven Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Sept. 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 [https://perma.cc/MW2B-CXND].

10. Ed Burns et al., *What Is Artificial Intelligence (AI)?*, TECHTARGET, https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence [https://perma.cc/AB4F-TLL2] (last visited Mar. 5, 2023).

11. Steven Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 555, 589 (2014).

12. *See* T.J. Benedict, Note, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 852 (2022) ("Courts provide little to no supervision over [facial recognition technology] in policing, especially when police use [facial recognition technology] to establish probable cause.").

13. KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 1 (2020).

14. *See* E. Barlow Keener, *Facial Recognition: A New Trend in State Regulation*, WOMBLE BOND DICKINSON (Apr. 29, 2022), https://www.womblebonddickinson.com/us/insights/alerts/

on whether using AI data-sorting to identify a suspect constitutes a search. Arguably, AI's analysis of the information gathered by law enforcement is not a search but rather an evaluation of data. However, as this Article will discuss, there are troubling indications that available technology could facilitate the creation of a surveillance society. Consequently, it is essential to scrutinize warrantless gathering of information and to evaluate at what point the use of these tools should require a warrant.

To better understand the potential for intrusive surveillance, one should understand the various roles and duties that law enforcement and security officials play. As citizens, we want a law enforcement system that prevents crime, and when crime occurs, we want that system to identify the criminals for prosecution. To that end, law enforcement relies on various forms of technology to gather and process information efficiently. One form of criminal investigation is law enforcement gathering information on its own and storing it in various databases.[15] The gathered information can then be input into an analytical system that uses AI to sort the information and identify potential suspects.[16]

The information that law enforcement provides to the system can come in the form of fingerprints, photographs, DNA, and criminal records—all information that is usually already part of law enforcement's records. However, data can also be easily obtained by law enforcement through technologies like CCTV and ALPR cameras, which capture individuals' daily movements.[17] Some information is also readily available to law enforcement through the third-party doctrine.[18] Information from cell service providers and websites can be obtained through requests to the third-party vendors.[19] Regardless of the mode of information-gathering, law enforcement is not required to obtain a probable cause search warrant before obtaining these types of valuable, and often personal, information.[20]

---

facial-recognition-new-trend-state-regulation [https://perma.cc/BPG6-2L92] ("Several states and municipalities are seeking to protect persons from abuse of biometrics by private companies and by law enforcement.").

15. For example, CODIS is a database that local, state, and federal agencies can use to access DNA records. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/LM3E-DLDY] (last visited Mar. 8, 2023).

16. *See* Benedict, *supra* note 12, at 854 ("For example, law enforcement agencies use [facial recognition technology] to try to match an image of a suspect against databases of driver's license photos or mugshots.").

17. *What Is CCTV*, *supra* note 1; *Street-Level Surveillance*, *supra* note 1.

18. H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 CARDOZO L. REV. 1549, 1550 (2020).

19. *Id.* at 1596–97.

20. *Id.* at 1573.

If a threat occurs, law enforcement can input the vast collection of information it has gathered through various modes of surveillance technology into a system using AI.[21] After quickly sorting through the information, the system will identify a potential suspect or suspects. Once a target is identified, information-gathering strategies change; with probable cause, warrants can be issued for specific in-depth searches[22] because data has produced a probable suspect. A second scenario occurs when general data about the specific crime area may be useful. Instead of going to the scene and questioning witnesses, law enforcement can rely on technologies like CCTV, geofencing, tower dumps, ALPRs, and Stingrays to gather all information about a given location on a specific date. That information can be input into AI to quickly identify all potential suspects. Finally, if a specific person is a suspect, substantial data can be gathered about him or her without a search warrant,[23] using all of the technologies discussed in this Article.

Regardless of the scenario, if an incident occurs, law enforcement will seek information. The question is whether it is reasonable to obtain that information using the six technology tools that this Article will discuss. The tools are just examples of the multiple technologies that law enforcement uses, but these six provide excellent insight. It is likely that the initial gathering of information using these tools is so broad that there are not Fourth Amendment protections. However, once the use of those tools gets more specific—when a particular individual's information becomes the target—the Fourth Amendment is implicated.

Technology-facilitated investigations may become so comprehensive that they provoke policy questions about whether we are building a surveillance society. Allowing law enforcement to acquire and keep a database that contains individual citizens' information, obtained through sophisticated and opaque technologies, searchable on demand and without restrictions, may indeed give rise to a "too permeating police

21. *See Does the Fourth Amendment Block Cops from Using Artificial Intelligence?*, CRIME REP. (Nov. 6, 2018), https://thecrimereport.org/2018/11/06/does-the-fourth-amendment-block-cops-from-using-artificial-intelligence/ [https://perma.cc/B558-GGFG] ("The police today enjoy a surfeit of data that can be collected, stored, mined, and sifted through easily and cheaply: license plate data, social media posts, social networks, and soon our own faces.").

22. *See* Michael J. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886–87 (2016) (noting that probable cause, rather than reasonable suspicion, is required for more intrusive searches).

23. *See* Bryan McMahon, *How the Police Use AI to Track and Identify You*, GRADIENT (Oct. 3, 2020), https://thegradient.pub/how-the-police-use-ai-to-track-and-identify-you/ [https://perma.cc/YWG2-G7JK] ("Technology and lax data and privacy laws have enabled the rise of dragnet surveillance systems that regularly search and seize critical data and devices from Americans without a warrant.").

surveillance" state.[24] Therefore the situation is two-fold: the law must protect individuals from intrusions by law enforcement, and our policies should ensure that investigations do not create a permeating surveillance state.

In this Article, we apply the traditional test of reasonable expectation of privacy from *Katz v. United States* to the various surveillance techniques and technologies that law enforcement can access in this digital world. Any location-related information derived from tower dumps, ALPRs, social media, geofencing, CCTV, and Stingrays may be judged based on the duration and detail of the information obtained. In other words, this Article critiques how much of a person's life is tracked by these technologies to reveal personal information that law enforcement would otherwise not be able to ascertain. The aggregate of the information is intrusive. There is a difference between a snapshot and a movie. The movie tells an entire story and presents a mosaic. The aggregation of mundane information can create an intimate profile. Intrusion can also occur based on acquisition of intimate information not acquired over a long period of time. One snapshot can be intrusive. If law enforcement obtains information about a person's health or financial data through cell phone data obtained from a tower dump, that information is not location data, but it is personal data.[25]

The first test we apply throughout this Article is the traditional two-part test from *Katz*.[26] Justice Harlan articulated the *Katz* test in his concurrence: to determine whether law enforcement's actions are a search, a court must look at (1) whether an individual has an actual, subjective expectation of privacy and (2) whether that expectation is one society is prepared to recognize as reasonable.[27] Determining an individual's subjective expectation of privacy means considering things like phone settings, social media privacy settings, and the policy implications of preventing a permeating police state.[28] The objective

24. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotations omitted).

25. Overlying these concerns is the third-party doctrine, how it is applied, and the need for it to be reworked.

26. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

27. *Id.*

28. *Reasonable Expectation of Privacy*, LAW SHELF EDUC. MEDIA, https://lawshelf.com/shortvideoscontentview/reasonable-expectation-of-privacy [https://perma.cc/G7A2-UFWQ] (last visited Mar. 3, 2023). Social media in particular presents unique questions regarding users' expectations of privacy. United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012). In the context of Facebook, the court in *Meregildo* explained:

> Facebook users may decide to keep their profiles completely private, share them only with "friends" or more expansively with "friends of friends," or disseminate

prong of this test concerns society's expectations, the third-party doctrine, and the public nature of some information.[29] Applying this test to modern technology and police surveillance tools is no easy task. To apply this test, we must look at the totality of the circumstances and the intimate nature of the information being obtained. It is likely that the general gathering of anonymized information is not a search, but when that general search turns specific and certain individuals become targets of legal warrantless surveillance, a search occurs.[30]

The second test we will apply is the mosaic theory, which will help us prove the subjective and objective prongs of *Katz*. The mosaic theory requires government action to be considered as a whole.[31] Specifically, instead of "asking if a particular act is a search, the mosaic theory asks whether a series of acts that [may not be] searches in isolation amount to a search when considered as a group."[32] The Massachusetts Supreme Judicial Court recently articulated how it applies the mosaic theory: to determine if government action constitutes a search that requires a warrant under the mosaic theory, the court must determine "whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's

---

> them to the public at large. Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, *inter alia*, on the user's privacy settings.
>
> When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.

Id. (emphasis in original). Thus, the social media privacy settings that an individual selects can be an indicator of the individual's subjective expectation of privacy. *Id.*

29. Caitlin Campbell, *Mixed Signals: An Analysis of the Third-Party Doctrine as Applied to Warrantless Collection of Historical Cell Site Location Information*, ARK. J. SOC. CHANGE & PUB. SERV. (Apr. 4, 2018), https://ualr.edu/socialchange/2018/04/04/mixed-signals-analysis-third-party-doctrine-applied-warrantless-collection-historical-cell-site-location-information/ [https://perma.cc/53M7-52K6].

30. To note, the new technology doctrine from *Kyllo v. United States* should not be applicable to the digital era and law enforcement's use of surveillance technologies. That doctrine stands for the premise that law enforcement's warrantless use of technology that is not in "general public use" in order to search a home is unlawful. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001). However, applying this doctrine would mean that law enforcement could still use highly invasive technologies if they just wait a few months or years. This suggests that *Kyllo* may no longer be good law and is becoming obsolete in its applicability.

31. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2010).

32. Commonwealth v. Perry, 184 N.E.3d 745, 757 (Mass. 2022) (quoting Kerr, *supra* note 31, at 320) (internal quotations omitted).

life."[33] Further, the Massachusetts court explained that there are three concerns to consider when making this determination.[34] First, there is the concern of how much of an individual's public movement is revealed by the surveillance.[35] The second concern is what kind of information is obtained through the search, and the third concern is whether law enforcement could have achieved the same kind of surveillance and gathering using "traditional law enforcement techniques."[36] The mosaic theory guides our approach to each of the law enforcement technologies discussed below.

The challenge begins when attempting to prove the subjective prong of *Katz*. Under the subjective prong, it must be shown that an individual has an actual, subjective expectation of privacy.[37] Individuals do not voluntarily disclose information revealed by blanket surveillance such as health issues, relationships, and political preferences. For the objective prong, the issue is whether society views an intrusion as a violation of a reasonable expectation of privacy.[38] As the *Perry* court suggests, an intrusion becomes unreasonable when the surveillance reveals "otherwise unknowable details of a person's life."[39] That level of constitutionally unconstrained data gathering and searching may signal a permeating surveillance state. Therefore, the mosaic theory of the Fourth Amendment should be considered as a limitation on data gathering from tower dumps, ALPR imaging, social media, geofencing, CCTV footage, Stingrays, or the aggregation of information through AI. With these tests in mind, this Article moves to the first mode of surveillance technology: tower dumps.

I. TOWER DUMPS

Any time a cell phone is turned on, it connects to a cell tower every seven seconds,[40] and each connection to a cell tower registers the cell phone user's location.[41] Tower dumps allow law enforcement to gather data about the identity, activity, and location of any cell phone that

33. *Id.* (quoting Commonwealth v. Mora, 150 N.E.3d 297, 310 (Mass. 2020)) (internal quotations omitted).

34. *Id.* at 758.

35. *Id.*

36. *Id.*

37. *Id.* at 756; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

38. Commonwealth v. Perry, 184 N.E.3d 745, 756 (Mass. 2022); *Katz*, 389 U.S. at 361.

39. *Perry*, 184 N.E.3d at 757.

40. *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Priv., Tech. & L. of the S. Comm. on the Judiciary*, 112th Cong. 228 (2011) (statement of the Am. Civ. Liberties Union), https://www.judiciary.senate.gov/imo/media/doc/CHRG-112shrg86775.pdf [https://perma.cc/BL85-R4NR].

41. *Id.*

connects to a specific cell tower during a one or two hour time frame.[42] To access this information, law enforcement must request records of every cell phone that connected to a cell tower in a certain area.[43] Law enforcement must make these requests to "cellular telephone providers" who have "detailed historical records" of their cell phone users.[44] Law enforcement's use of tower dumps as a legal warrantless surveillance tool poses a significant threat to an individual's reasonable expectation of privacy.

The danger of tower dumps was made clear during the summer of 2020 when thousands of Americans participated in the Black Lives Matter Protests.[45] Many protesters brought their cell phones with them, but most did not realize the risk that came with bringing their phones.[46] Throughout the summer, privacy experts warned protesters that law enforcement agencies had surveillance tools capable of tracking cell phones.[47]

Law enforcement's use of tower dumps is analogous to law enforcement's use of cell site location information (CSLI). In *Carpenter v. United States*, the Supreme Court ruled that the collection of an individual's CSLI was an unconstitutional warrantless search.[48] In *Carpenter*, law enforcement gathered CSLI information on a single person for 127 days.[49] The *Carpenter* Court ultimately held that the warrantless gathering of seven days of CSLI on a specific person was

42. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Aug. 11, 2015, 11:51 AM), https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ [https://perma.cc/HW8Y-ALSC].

43. Wendy J. Wagner, *Tower Dump Production Orders: Restricting Police Access to Cellular Records in R v. Rogers Communications*, GOWLING WLG (Jan. 18, 2016), https://gowlingwlg.com/en/insights-resources/articles/2016/tower-dump-production-orders-restricting-police-a/ [https://perma.cc/SFD8-WDFJ].

44. Hon. Brian L. Owsley, *The Fourth Amendment's Implication of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CON. L. 1, 5 (2013).

45. *See* Keeanga-Yamahtta Taylor, *Did Last Summer's Black Lives Matter Protests Change Anything?*, NEW YORKER (Aug. 6, 2021), https://www.newyorker.com/news/our-columnists/did-last-summers-protests-change-anything [https://perma.cc/8QNL-ATRT] ("On June 1st last year, a week after George Floyd was murdered, more than three hundred fires blazed across Philadelphia . . . . By that Saturday, June 6th, tens of thousands of people clogged the streets of downtown, demanding justice, proclaiming that Black Lives Matter.").

46. Thomas Germain, *How to Protect Phone Privacy and Security During a Protest*, CONSUMER REPS. (June 3, 2020), https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest-a5990476708/ [https://perma.cc/YCV2-WTHP].

47. *Id.* This phenomenon is not unique to the Black Lives Matter Protests, but these protests are a manifestation of this risk. "Protests in the United States and elsewhere have been monitored in the past, and information gathered through digital surveillance has been introduced in situations where protesters have been prosecuted." *Id.* (internal quotations omitted).

48. Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

49. *Id.* at 2212, 2217.

unconstitutional,[50] but the Court did not answer whether a shorter amount of time would be violative of someone's reasonable expectation of privacy.[51] Tower dumps involve the gathering of CSLI over a short amount of time and gathering data about hundreds of individuals in a specific area rather than one individual.[52] The question is whether there is a material difference between tower dumps and targeted CSLI collection as in *Carpenter*.

The tower dump is not targeted at an individual and covers a shorter period.[53] No warrant is required before law enforcement requests the information.[54] Because a warrant is not required, a law enforcement agency might seek to use a tower dump to investigate an incident in a particular area by identifying multiple individuals in the area. Part of the justification for allowing warrantless collection via tower dumps is the third-party doctrine, which is becoming a highly criticized area of law.[55] A tower dump is obtained through the third-party cell tower provider.[56]

Both the subjective and objective prongs of *Katz* are implicated in law enforcement's use of tower dumps. The process of using tower dumps to obtain vast amounts of information on hundreds of cell phones at a given location and during a certain period of time must be broken down to best understand the intrusive nature of this mode of surveillance. First, the whole of an individual's public movement at certain locations can be revealed by tower dumps.[57] With a tower dump, law enforcement

50. *See id*. at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

51. *See* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. 109, 113 (2020) ("[*Carpenter*] explicitly left open the question of whether governmental acquisition of historical CSLI for shorter periods of time, like tower dump CSLI, also triggers Fourth Amendment protections.").

52. *See* Mason Kortz & Christopher Bavitz, *Cell Tower Dumps*, BOSTON BAR ASS'N (Mar. 18, 2019), https://bostonbar.org/journal/cell-tower-dumps/ [https://perma.cc/VYZ7-8E43] ("A tower dump, by its nature, involves access to more users' data than historical CSLI does . . . . That said, a typical tower dump is confined in the sense that it covers both a small area and a relatively short time period—often a few hours or even a few minutes.").

53. *Id.*

54. *See id.* (explaining that a majority of courts have held that a warrant is not required to obtain a cell tower dump).

55. The third-party doctrine stands for the principle that whatever an individual discloses to a third party can be accessed by law enforcement without a warrant. RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014).

56. Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, AM. CIV. LIBERTIES UNION (Mar. 27, 2014), https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique [https://perma.cc/ANJ6-MLGB].

57. *See id.* ("This is a cell tower dump: the practice of demanding an enormous amount of cell phone location information—anywhere from hundreds to hundreds of thousands of data points—in an effort to identify just a few suspects."); *see also* Kelly, *supra* note 42 (explaining

accesses the identity, activity, and location of cell phones that connected to a specific tower at a specific date.[58] In fact, a "tower dump . . . provides officers with CSLI from every device that connected to a particular cell site within a specified period; allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time."[59]

Additionally, law enforcement can potentially access very specific, identifying information about an individual. Individuals take their cell phones everywhere, so depending on which cell towers law enforcement is requesting information from, they could obtain deeply personal and private information about a user. People bring cell phones into public places, like grocery stores and schools, but also into private places like doctors' offices, their homes, and churches, to name a few. With tower dumps, intimate details of a cell phone user's life could be in law enforcement's hands in a matter of minutes.

Finally, this level of surveillance is not something law enforcement could achieve with traditional law enforcement techniques. Prior to tower dumps, law enforcement officers would have to identify suspects by questioning witnesses at the scene of a crime. Law enforcement did not have the ability to "secretly monitor and catalogue every movement of an individual."[60] By using tower dumps, law enforcement is able to quickly gather identifying information on thousands of people in a short amount of time. This identifying information provides information on a cell phone user's life, "revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[61]

The Court has yet to determine whether tower dumps are unconstitutional. However, in other contexts such as GPS monitoring, the wide-scale blanket collection of information over a period of time is considered intrusive.[62] If law enforcement is to collect that vast amount of location information over a specific period of time on cell phones, they should be able to state a reason. Indeed, there may be reasons such as a

---

that tower dumps give police officers the location of any phone that connects to a targeted cell phone tower).

58. Kelly, *supra* note 42.

59. Commonwealth v. Perry, 184 N.E.3d 745, 754 (Mass. 2022).

60. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). Notably, the *Carpenter* Court explained how society at one time did not expect law enforcement to be able to track every movement of an individual's car. *Id.* This logic applies the same to tracking individuals themselves. Prior to the digital era, society did not expect law enforcement to have the ability to secretly track the movements of individuals. *Id.*

61. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

62. *See* United States v. Jones, 565 U.S. 400, 403–04 (2012) (finding that the government's use of a GPS tracking device on a suspect's vehicle for twenty-eight days constituted a search within the meaning of the Fourth Amendment).

shooting or terrorist event that would justify a tower dump. Regardless of the reason, law enforcement should be prohibited from such unrestricted access to a cell phone user's personal information through the use of tower dumps over an extended period of time.

II. AUTOMATIC LICENSE PLATE READERS

ALPRs are devices that use "high-speed cameras designed to capture a photograph of each and every passing license plate, combined with software that analyzes those photographs to identify the license plate number."[63] Law enforcement uses both their own ALPR devices and devices owned by vendors that have contracts with law enforcement.[64] These contracts allow officers to "access . . . private databases containing scans from private ALPRs and from other local and federal law enforcement agencies."[65] The U.S. Supreme Court has never addressed whether a warrant is required for law enforcement to obtain historical ALPR data.[66] However, some appellate courts have started deciding cases on this very issue.

The Ninth Circuit has held that a defendant lacked standing to challenge law enforcement's warrantless accumulation of ALPR data to determine where the defendant went after he kept a rental car past its return date.[67] The Massachusetts Supreme Judicial Court found that a limited use of ALPRs in a specific location did not violate a defendant's reasonable expectation of privacy.[68] Notably, the Massachusetts court implied that an extended use of ALPRs to constantly monitor someone's movements with more than four cameras, in more than one location, would violate a defendant's reasonable expectation of privacy.[69]

States have different rules for how long a specific piece of ALPR data can be stored. New Hampshire mandates that data on a vehicle that is not

63. AM. CIV. LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 4 (July 2013).

64. Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations#:~:text=Law%20enforcement%20use%20of%20ALPR,and%20federal%20law%20enforcement%20agencies [https://perma.cc/H4YB-G9FW].

65. *Id.*

66. *Id.*

67. United States v. Yang, 958 F.3d 851, 859 (9th Cir. 2020).

68. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1106 (Mass. 2020).

69. *See id.* ("While we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections, it is not that produced by four cameras at fixed locations on the ends of two bridges.").

associated with a crime be deleted in three minutes.[70] Arkansas requires that the data be deleted after 150 days.[71] ALPR data in California must be deleted after sixty days if it is not related to a felony case.[72] Georgia mandates that ALPR data be deleted after thirty months unless it is related to a "law enforcement purpose."[73] This means that the state in which an individual drives determines how long their personal information is stored.

Law enforcement having unfettered access to a long term, searchable, organized database containing photographs of individuals driving on a highway is concerning. Specifically, these images reveal the vehicle make and model, the license plate number, and the vehicle's location on a certain date and time.[74] In other words, the database creates a mosaic of the driver's movements. As courts have recognized, an unlimited record of vehicle movements can be intrusive,[75] which is why time limits make sense. If this type of information gathering is turned into targeted, individualized surveillance, the question is whether it violates the *Katz* standard and the mosaic theory. When the gathering of information becomes the action of law enforcement searching an ALPR database for a specific driver's movements, such gathering violates those standards.

Even though the collection and storage of images in ALPR databases is not a search, when law enforcement accesses the database to identify and track the movements of a specific driver, a search does occur. First, using ALPRs for this individualized surveillance implicates a subjective expectation of privacy, as it creates the potential for a permeating police state and permits law enforcement to track the daily movements of any driver they target.[76] ALPRs allow agencies to collect images of vehicles as they travel on specific roads and highways, revealing a driver's

---

70. Dave Davies, *Surveillance and Local Police: How Technology Is Evolving Faster Than Regulation*, NPR (Jan. 27, 2021, 12:51 PM), https://www.npr.org/2021/01/27/961103187/surveillance-and-local-police-how-technology-is-evolving-faster-than-regulation [https://perma.cc/6CNS-PY6J].

71. ARK. CODE ANN. §§ 12-12-1804(a) (2023).

72. *Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 3, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/8UFC-7X2V]; CAL. VEH. CODE § 2413(b) (West 2022).

73. *Automated License Plate Readers: State Statutes*, *supra* note 72; *see also* GA. CODE ANN. § 35-1-22(b) (2022).

74. *ALPR FAQs*, IACP (Aug. 8, 2018), https://www.theiacp.org/resources/alpr-faqs#:~:text=ALPR%20systems%20typically%20capture%20the,unit%20that%20captured%20the%20image [https://perma.cc/HQ5G-4C3N].

75. *See* United States v. Jones, 565 U.S. 400, 403–04 (2012) (holding that the police conducted a search within the meaning of the Fourth Amendment by using a GPS tracking device on a vehicle for twenty-eight days and collecting more than two thousand pages of data).

76. Yash Dattani, *Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces*, 24 VAND. J. ENT. & TECH. L. 749, 764 (2022).

movements on public roads.[77] Not only does this information provide a log of a driver's movements but it can also reveal intimate details of a driver's location or whereabouts at any specific time.[78] Justice Sotomayor even explained that giving law enforcement the ability to create a precise, comprehensive record of a person's movements threatens reasonable expectations of privacy.[79] Specifically, she stated, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of her familial, political, professional, religious, and sexual associations."[80] Although Justice Sotomayor was writing about the use of GPS, her analysis can also apply to personal location data obtained through use of ALPRs. The major difference is that a GPS is attached to a car while an ALPR is not. But the resulting tracking information can result in the same location data. This is the type of intimate information that the mosaic theory prohibits. Notably, the Supreme Court has stated, "A person *does not surrender all Fourth Amendment protections* by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[81]

Further, law enforcement has not always had this surveillance technology. Until the advent of ALPRs, law enforcement did not have the technology to gather a vast amount of information about every driver on a highway at a given location, date, and time. They also lacked the ability to obtain specific information on the location of drivers from months or years prior to their investigation. Now, that is possible. Although some states restrict ALPRs,[82] there is no Supreme Court determination that constant ALPR surveillance is an intrusion. The mosaic theory could well apply to continuous surveillance through ALPRs, depending on the facts. As it stands now, there is no consistent national policy on ALPRs.

77. *Id.* at 769.

78. *Id.* at 774.

79. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

80. *Id.* at 415.

81. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)) (emphasis added) (brackets in original).

82. *See, e.g.*, ME. STAT. tit. 29-A, § 2117-A (2022) (explaining that ALPRs are prohibited except when used by law enforcement in Maine to "provid[e] public safety, conduct[] criminal investigations and ensur[e] compliance with local, state and federal laws"); MD. CODE ANN., PUB. SAFETY § 3-509(c) (LexisNexis 2022) (setting forth specific procedures for law enforcement in Maryland to follow in using ALPRs); VT. STAT. ANN. tit. 23, § 1607(c)(1)(A) (2022) ("Deployment of ALPR equipment by Vermont law enforcement agencies is intended to provide access to law enforcement reports of wanted or stolen vehicles and wanted persons and to further other legitimate law enforcement purposes. Use of ALPR systems by law enforcement officers and access to active data are restricted to legitimate law enforcement purposes.").

III. SOCIAL MEDIA

Seventy-two percent of Americans use at least one form of social media.[83] Social media allows users to share in real time what they are doing, where they are located, and how they are feeling while making new friends online. Unfortunately, this shared information has also become a treasure trove for law enforcement investigations. Seventy-three percent of law enforcement agencies believe "social media helps solve crimes more quickly."[84] Much of this information is available without a warrant.[85]

The third-party doctrine allows law enforcement to obtain information on social media sites without a warrant.[86] The doctrine states that when people voluntarily give information to third parties like banks, Internet service providers, and phone companies, they have no reasonable expectation of privacy in the information they provide.[87] However, with the evolving technologies in the digital era, the broad application of this doctrine is outdated and ignores the realities of contemporary society.

The logic of this doctrine was questioned as early as 1979. In fact, Justice Thurgood Marshall criticized this doctrine in his dissent in *Smith v. Maryland*: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[88] Justice Sotomayor also expressed her frustrations with the doctrine in her *United States v. Jones* concurrence and argued that it is time to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[89] Justice Sotomayor also went on to say that the third-party doctrine was "ill-suited" for the digital era because individuals share a "great deal of information about themselves

---

83. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/2DTF-UKAV].

84. LEXISNEXIS, SOCIAL MEDIA USE IN LAW ENFORCEMENT: CRIME PREVENTION AND INVESTIGATIVE ACTIVITIES CONTINUE TO DRIVE USAGE 3 (2014), https://centerforimprovinginvestigations.org/wp-content/uploads/2018/11/2014-social-media-use-in-law-enforcement-pdf.pdf [https://perma.cc/8TNF-JC5K].

85. *See id.* at 8 ("Social media information used to help establish probable cause for a search warrant continues to be widely accepted.").

86. *See id.* (explaining that social media information can be gathered by law enforcement before obtaining a search warrant, in order to establish probable cause); *see also* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter?*, 26 B.U. J. SCI. & TECH. L. 286, 288 (2020) (emphasizing that, by relying on the third-party doctrine, the government can "liberally glean the most intimate details" from communicative content, including social media messages).

87. THOMPSON II, *supra* note 55.

88. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

89. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

to third parties in the course of carrying out mundane tasks."[90] Justice Sotomayor explained the dangers of the third-party doctrine in the digital age perfectly. Technology dominates all aspects of modern life. Individuals surrender vast amounts of personal information to third parties in the course of a normal day, but that surrender should not be considered a waiver of Fourth Amendment rights.

Nonetheless, courts continue to hold that individuals have no reasonable expectation of privacy in their social media posts. A New York court held that a Twitter user had no reasonable expectation of privacy in his tweets.[91] The U.S. District Court for the Southern District of New York found that law enforcement can constitutionally access a Facebook user's private profile through friends' profiles.[92] The court noted that having more secure privacy settings on a profile may reflect users' intent to protect their personal information, providing some constitutional protections.[93] The Connecticut Supreme Court suggested that posting personal information on social media waives any expectation of privacy in that information.[94] The Pennsylvania Court of Common Pleas held that communications on social media are not protected: "[N]o person choosing MySpace or Facebook as a communications forum could reasonably expect that his communications would remain confidential, as both sites clearly express the possibility of disclosure."[95] The U.S. District Court for the Northern District of Ohio held that the Fourth Amendment did not protect defendants from law enforcement adding them as friends on music sites to gather evidence.[96] The U.S. District Court of New Jersey held that a defendant's privacy rights were not

90. *Id.*

91. *See* People v. Harris, 949 N.Y.S.2d 590, 593 (N.Y. Crim. Ct. 2012) ("There can be no reasonable expectation of privacy in a tweet sent around the world.").

92. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment.").

93. *Id.* at 525.

94. *See* State v. Bruhl, 138 A.3d 868, 878 n.10 (Conn. 2016) ("The Appellate Court reasoned that the Facebook posts had to be exhibited in a 'public place,' . . . in order to be publicly exhibited . . . . [T]he Appellate Court concluded that to be publicly exhibited, the Facebook posts had to be accessible by the general public, and not only to 'Tasha Moore's' friends. Because we conclude that the trial court reasonably could have concluded that the posts were accessible to the general public on the facts of the present case, we need not decide whether a Facebook post that is accessible only to a user's network of friends is publicly exhibited . . . . We leave that question for another day.").

95. McMillen v. Hummingbird Speedway, Inc., No. 113-2010, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010) (trial order op.).

96. United States v. Sawyer, 786 F. Supp. 2d 1352, 1356–57 (N.D. Ohio 2011).

violated when an officer followed the defendant on Instagram and discovered incriminating evidence.[97]

In evaluating law enforcement's access to social media, it is important to determine if an individual takes actions that demonstrate a desire to limit access to their information. For example, when a social media user chooses a private profile, that action can be an expression of an expectation of privacy.[98] In *Commonwealth v. Carrasaquillo*, the court evaluated whether the defendant had a reasonable expectation of privacy in a video he posted on Snapchat.[99] A law enforcement officer used a randomly generated username and requested to be Carrasaquillo's friend on Snapchat.[100] Carrasaquillo added the officer, and the officer recorded a video Carrasaquillo posted, which was later used against him at trial.[101] The court ultimately concluded that Carrasaquillo did not have a subjective expectation of privacy because he did not know what his privacy settings were and because he accepted more requests than those of people he knew.[102] The court also explained that there may be a subjective expectation of privacy in social media posts if the user has taken actions to "purposefully engage[] in conduct aimed at ensuring privacy."[103] Clearly, Carrasaquillo's actions were not taken to ensure his privacy.

Based on the logic of *Carrasaquillo*, a user who takes specific, intentional steps to protect their personal information can establish an expectation of privacy. For instance, a person may take intentional steps to program privacy settings to prevent Facebook friends from sharing their statuses or pictures.[104] In other platforms, individuals can also express an intent to protect their privacy. An individual can prevent their tweets from getting retweeted or can prevent their Instagram post from being shared by other profiles and limit viewing to specific people. There are not yet Supreme Court precedents on these various privacy options, but there is a reasonable argument that personal conversations, even if

97. United States v. Gatson, No. 13-705, 2014 WL 7182275, at *22 (D. N.J. Dec. 16, 2014), *aff'd*, 744 F. App'x 97 (3d Cir. 2018).

98. *See Meregildo*, 883 F. Supp. 2d at 525 ("[P]ostings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.").

99. Commonwealth v. Carrasquillo, 179 N.E.3d 1104, 1108 (Mass. 2022).

100. *Id.* at 1110.

101. *Id.* at 1120.

102. *Id.* at 1117.

103. *Id.*

104. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (explaining that Facebook users may "decide to keep their profiles completely private, share them only with 'friends' or more expansively with 'friends of friends,' or disseminate them to the public at large" and that because the defendant "maintained a Facebook profile in which he permitted his Facebook 'friends' to view a list of all of his other Facebook 'friends,'" the government did not violate the Fourth Amendment by viewing the defendant's profile through his friend's profile).

conducted over social media, can be limited. There are longstanding expectations of privacy in conversation and association[105]—two things that are prominent features of social media. Capturing social media posts can be highly intrusive. The nature of social media does not usually manifest a desire for privacy, but it can. If posts allow for large numbers of observers, it is difficult to argue that the user has a reasonable expectation of privacy. But intentional privacy limits may provide arguments against warrantless access. There is something disquieting about a law enforcement officer creating a fake profile to gain access to a social media profile.

Notably, the mosaic theory also provides some guidance. As a reminder, there are three concerns to consider when applying the mosaic theory to potential searches by law enforcement: how much of someone's public movement is revealed, the nature of the information revealed, and whether law enforcement could obtain this information using traditional techniques.[106] It is undeniable that a law enforcement officer looking at someone's social media profile is able to see a detailed mosaic of that person's life. In fact, part of social media posting involves sharing where a user has been—implicating the first concern of the mosaic theory. Social media allows law enforcement to see a great deal of someone's public movement by browsing photograph location tags, status updates, and location pins. Additionally, people share their thoughts on religion, politics, and current events on social media. They post photographs of family, for birthdays, and while on vacation. All of this information is very intimate in nature. Finally, social media provides law enforcement with an unprecedented amount of information on users—information that would never be achieved through traditional law enforcement techniques.

Ultimately, the protection of social media disclosures may well be decided around the evolution of the third-party doctrine in the digital age. As it stands, social media is a vast unprotected trove of personal information that law enforcement can easily access without a warrant. A rethinking of the third-party doctrine in the digital era may serve to create the best protections from social media intrusions by law enforcement.

IV. GEOFENCING

Geofencing is a "location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a

105. *See Carrasquillo*, 179 N.E.3d at 1114 ("Government surveillance of [social media] activity therefore risks chilling the conversational and associational privacy rights that the Fourth Amendment . . . seek[s] to protect.").

106. Commonwealth v. Perry, 184 N.E.3d 745, 758 (Mass. 2022).

geofence."[107] When law enforcement is unable to identify a suspect for a potential crime, officers can obtain a geofence warrant to get valuable location information from certain apps.[108] These warrants are different from search warrants. To obtain a geofence warrant, a law enforcement officer only needs to provide a specific place and time to a judge. Once that officer obtains judicial approval, companies will conduct searches of their databases to provide a list of cell phone numbers that were in that specific location at that specific time.[109]

Zachary McCoy, a University of Florida student, learned first-hand how law enforcement's use of geofencing warrants can lead officers to identifying a suspect, and in his case, the wrong suspect. In March 2019, McCoy was riding his bike in Gainesville, Florida, and tracking his ride on RunKeeper, a Google fitness app.[110] Months later, in January 2020, Google emailed McCoy and notified him that his data was being released to law enforcement because he had become a suspect in a burglary.[111] McCoy became a suspect after law enforcement obtained his location information from Google through a geofencing warrant.[112] McCoy ultimately fought to keep Google from releasing his personal information and won.[113]

Many states have allowed law enforcement to use geofence warrants to gain large amounts of personal location information.[114] These warrants "rely on the vast trove of location data that Google collects from Android users—approximately 131.2 million Americans—and anyone who visits a Google-based application or website from their phone, including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others."[115] This is extremely concerning as most Americans use at least one Google

107. Sarah K. White, *What Is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017), https://www.cio.com/article/288810/geofencing-explained.html [https://perma.cc/5QPT-82MA]. RFID stands for radio-frequency identification.

108. Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021) [hereinafter *Geofence Warrants*].

109. *Id.*

110. *Id.* at 2508.

111. *Id.*

112. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-buke-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/Z5ZN-TAF5].

113. *Id.*

114. *Geofence Warrants*, *supra* note 108 (stating that Arizona, Florida, Maine, Minnesota, New York, North Carolina, Texas, Virginia, Washington, D.C., Wisconsin, and other states have embraced the use of "sweeping geofence warrants").

115. *Id.* at 2512.

application: YouTube.[116] In fact, between 2017 and 2018, law enforcement's request for geofenced information from Google increased 1,500%, and it increased 500% between 2018 and 2019.[117] While Google is the most common corporation to receive these requests, Apple, Snapchat, Lyft, and Uber also receive them.[118]

Google has attempted to protect some of this information by implementing a three-step plan to prohibit "overly broad requests" from being fulfilled.[119] The first step Google takes is searching its location history database and producing an anonymized list of accounts, which contains "relevant coordinate, timestamp, and source information—present during the specified timeframe in one or more areas."[120] Next, law enforcement informs Google regarding which accounts it wants additional information on.[121] Finally, Google will provide "account-identifying information, such as first names, last names, and email addresses" of those users.[122]

It is harder to argue that an individual has an expectation of privacy in the *anonymized* account information that Google provides to law enforcement than when Google provides identifiable personal information. At that point, the Fourth Amendment becomes relevant for the following reasons, in accordance with the mosaic theory.

First, geofencing reveals the locations of any individuals in a given area at a given time.[123] Once that information is targeted toward a certain user, law enforcement knows when that individual was in a public space, allowing officers to have a better understanding of someone's public movements. Second, as explained above, after a simple request, law enforcement can obtain personal information on any anonymized account that may be deemed suspicious or that is in a suspicious location, turning this massive search of anonymized accounts into an investigation into a single individual.[124] This personal information contains highly intimate

116. *See* Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ [https://perma.cc/293B-7SUA] (finding that eighty-one percent of Americans report that they use YouTube).

117. Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022, 11:04 AM), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html [https://perma.cc/65JR-EFXE]. "In 2019, Google received about 9,000 geofence requests." *Id.*

118. *Geofence Warrants*, *supra* note 108, at 2512–13.

119. *Id.* at 2515.

120. *Id.*

121. *Id.*

122. *Id.*

123. Seltzer, *supra* note 117.

124. *Geofence Warrants*, *supra* note 108, at 2514–15.

content and includes email addresses, first names, and last names of users, at minimum.

Finally, geofencing technology allows law enforcement to obtain information that it normally would not be able to obtain through traditional law enforcement techniques like speaking to witnesses who were at the scene.[125] Law enforcement has not always had the ability to effortlessly obtain personal, identifying details about a person's whereabouts through the Internet, but geofencing provides them with this ability. In other words, geofencing now provides law enforcement with the ability to aggregate information on a person's whereabouts over a period of time, creating a mosaic of their life.

V. CLOSED-CIRCUIT TELEVISION

CCTV cameras that record activity in real time are in use across the world for security and law enforcement purposes. The U.S. Justice Department conducted a survey in 2001 indicating that sixty-three percent of participants say CCTV helps in criminal investigations, fifty-four percent say CCTV helps gather evidence, and twenty percent say CCTV helps in crime prevention.[126] Fifty million CCTV cameras are stationed throughout the United States as of 2020.[127]

Courts have started to establish when law enforcement's use of CCTV cameras constitutes a search. If CCTV covers public spaces, and the camera records activity in public, there is generally no broad expectation of privacy.[128] But there are exceptions. For example, in *United States v. Moore-Bush*, a federal judge granted a defendant's motion to suppress CCTV video footage of the defendant and her mother.[129] The CCTV camera was placed on an utility pole outside of the defendant and her mother's home, and the camera filmed their movement for eight months.[130] The camera could pan to numerous parts of the property, and

125. *Id.* at 2515–18.

126. Laura J. Nichols, *Use of CCTV/Video Cameras in Law Enforcement, Executive Brief*, U.S. DEP'T OF JUST., https://www.ojp.gov/ncjrs/virtual-library/abstracts/use-cctvvideo-cameras-law-enforcement-executive-brief [https://perma.cc/AXY7-PX3U] (last visited Mar. 17, 2023).

127. Sidney Fussell, *When Private Security Cameras Are Police Surveillance Tools*, WIRED (Aug. 11, 2020, 3:27 PM), https://www.wired.com/story/private-security-cameras-police-surveillance-tools/ [https://perma.cc/NP7Z-R5C9].

128. United States v. Knotts, 460 U.S. 276, 277 (1983).

129. United States v. Moore-Bush, 381 F. Supp. 3d 139, 141 (D. Mass. 2019), *rev'd*, 36 F.4th 320 (1st Cir. 2022). Although the district court's decision in *Moore-Bush* was reversed, other courts have applied the district court's reasoning to support similar decisions. *See, e.g.*, People v. Tafoya, 494 P.3d 613, 615, 621 n.8 (Colo. 2021) (holding that "police use of [a] pole camera to continuously video surveil Tafoya's fenced-in curtilage for three months, with the footage stored indefinitely for later review, constituted a warrantless search in violation of the Fourth Amendment" and explaining that the reversal of *Moore-Bush* did not change the court's decision).

130. *Moore-Bush*, 381 F. Supp. 3d at 141.

it could zoom in on activities occurring on the property.[131] Through this footage, law enforcement created a searchable log of the family's activities in and around their home.[132] The government did not have a warrant before it installed this camera, and it could not show probable cause for this surveillance.[133] The government argued that the video taken from the pole did not constitute a search under the Fourth Amendment.[134] The district court judge disagreed.[135]

The judge stated that there were two "basic guideposts" to shape society's understanding of an unreasonable search: "First, that the [Fourth] Amendment seeks to secure the 'privacies of life' against 'arbitrary power.' Second . . . that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[136] The court found that the defendant and her mother's actions of living in a residential neighborhood and in a house obstructed by a large tree showed "that they did not subjectively expect to be surreptitiously surveilled with meticulous precision each and every time they or a visitor came or went from their home."[137] The court also found the expectation to be reasonable based on *Carpenter*, stating that they had a reasonable expectation of privacy in their movements and their visitor's movements around the house for eight months.[138] The court also noted that those alive during the creation of the Fourth Amendment would be outraged if they discovered law enforcement "had managed to collect a detailed log of when a home's occupants were inside and when visitors arrived and whom they were."[139]

The *Moore-Bush* decision draws a logical line. When law enforcement uses CCTV to conduct twenty-four-hour surveillance of a home, that action constitutes an unreasonable search.[140] CCTV targeted at a home seems to be a clear overreach under the Fourth Amendment. Not only is the target specific, but also the continuous nature reeks of permeating surveillance. As the *Carpenter* Court explained, in drafting the Fourth

131. *Id.* The camera could not see into the home, but it could see license plates of vehicles that came and went from the home. *Id.*

132. *Id.* at 149–50.

133. *Id.* at 142.

134. *Id.*

135. *Id.* at 150.

136. *Moore-Bush*, 381 F. Supp. 3d at 142.

137. *Id.* at 144.

138. *Id.* at 146.

139. *Id.* at 148.

140. *See* People v. Tafoya, 490 P.3d 532, 542 (Colo. App. 2019) (finding that the police violated the Fourth Amendment when they used a video camera on a utility pole to continuously surveil defendant's house for three months), *aff'd*, 494 P.3d 613 (Colo. 2021). The Colorado appellate court nevertheless noted that "many of the courts to address the issue have concluded that continuous, long-term video surveillance of a private home via a non-trespassory pole camera does *not* constitute a 'search' under the Fourth Amendment." *Id.* at 538 (emphasis added).

Amendment, the Framers sought to prevent a "too permeating police" state.[141] Allowing law enforcement to have unlimited access to monitor a home and who visits it permits the permeating police surveillance that the Court warned of, and it provides an intimate look into the home—a constitutionally protected area. In sum, a subjective expectation of privacy exists when residents have taken specific actions to ensure their home will not be "surreptitiously surveilled with meticulous precision."[142]

Society expects privacy at home and is prepared to recognize it as reasonable. There is a long history of Supreme Court cases stating that the most protected sphere of privacy for an individual is their home.[143] Additionally, constant CCTV monitoring of a home reveals a deeply intimate mosaic of an individual's private life. First, it tracks the movement of all residents of a home and of all visitors of a home.[144] It also reveals extremely intimate information concerning private family life[145]—religion, political affiliations, and health, to name a few. Finally, it allows law enforcement to use cameras to get a closer look at a home that they otherwise would not be able to see into through traditional law enforcement techniques.[146] Arguably, law enforcement's use of CCTV to

141. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

142. *Moore-Bush*, 381 F. Supp. 3d at 150.

143. *See* Mapp v. Ohio, 367 U.S. 643, 660 (1961) (holding that the Fourth Amendment is made applicable to the states through the Due Process Clause, such that state residents are protected from unreasonable searches and seizures in their home by state police); Chimel v. California, 395 U.S. 752, 768 (1969) (establishing that the warrantless search of an individual's entire home is unconstitutional under the Fourth Amendment); Payton v. New York, 445 U.S. 573, 576 (1980) ("[T]he Fourth Amendment . . . prohibits the police from making a warrantless and nonconsensual entry into a suspect's home in order to make a routine felony arrest."); Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."); Florida v. Jardines, 569 U.S. 1, 11–12 (2013) ("The government's use of trained police dogs to investigate the home and its immediate surroundings is a 'search' within the meaning of the Fourth Amendment.").

144. *See* Brief of Amici Curiae Elec. Frontier Found. et al. in Support of Petitioner at 16, Tuggle v. United States, 142 S. Ct. 1107 (2022) (No. 21-541) ("[C]onstant and secret long-term surveillance makes it possible to learn intimate details about the lives of everyone in the household. For example, the police could identify everyone who visits the home by tracking the license plate of every car that parks in the driveway.").

145. *See, e.g.*, *id.* ("[Police] could deduce whether the occupants were expecting a baby, merely by the large boxes delivered to the home, and whether the occupants later lost that baby, by those same boxes being returned.").

146. *See id.* at 14–15 ("Although 'lawful conventional surveillance techniques,' such as a stakeout, might allow police to watch a suspect's activities for limited periods from public vantage points, digitally enabled surveillance is 'ever alert,' and its 'memory is nearly infallible.'").

monitor a home over any period of time is a search that requires a warrant.[147]

Additionally, the Fourth Amendment could be implicated when a public CCTV camera identifies a person on footage through law enforcement's use of facial recognition software.[148] Once an image has been captured by CCTV or otherwise, facial recognition technology can be used to personally identify an individual.[149] Then that image may be used to track multiple other images.[150] Applications like Clearview software say they have billions of images from the Internet and other locations.[151] Interestingly, Clearview has been limited in certain locations such as Canada and Australia.[152] Law enforcement frequently uses facial recognition, and some public opinion polls indicate that Americans think it is a good way to stop crime.[153] However, the combination of broad

147. Notably, the general surveillance of a public space through CCTV footage may not have the same protections. Additionally, modern technology can make CCTV monitoring even more dangerous with insect-size drones. In fact, a micro air vehicle, also called the bug drone, is being developed for future use by the U.S. Military for "in-the-open surveillance, aerial swarm operations, and battlefield situational awareness." Bruce Crumley, *Bug Off: US Military Planning Winged, Insect-like Microdrone*, DRONEDJ (June 18, 2021, 4:26 AM), https://dronedj.com/2021/06/18/bug-off-us-military-planning-winged-insect-like-microdrone/ [https://perma.cc/Z8DJ-EJ27]. Another danger of CCTV is the way it interacts with facial recognition technology. A single image of a person on a public street taken by a CCTV camera can be put into a facial recognition database, and large amounts of personal data can be gathered. *Facial Recognition: Who's Tracking You in Public?*, CONSUMER REPS. (Dec. 30, 2015), https://consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1-a7157224354/ [https://perma.cc/6N68-9KB8].

148. Theodore Claypoole, *A Clear Solution to Police Surveillance Creep: Warrants Needed for Biometric Analysis*, AM. BAR ASS'N (Aug. 3, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/08/police-surveillance/ [https://perma.cc/P4G8-67JH].

149. *See* Benedict, *supra* note 12, at 854 ("This technology attempts to match one image of a face against a collection of facial images.").

150. *See id.* ("[L]aw enforcement agencies use [facial recognition technology] to try to match an image of a suspect against databases of driver's license photos or mugshots. Some [facial recognition technology] databases contain images gathered from social media or other sources without the consent of those photographed.").

151. *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/ [https://perma.cc/JR4M-SZ77] (last visited Mar. 18, 2023).

152. *Announcement: Clearview AI Ordered to Comply with Recommendations to Stop Collecting, Sharing Images*, OFF. OF PRIV. COMM'R OF CANADA (Dec. 14, 2021), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/ [https://perma.cc/4GWS-THRN]; Byron Kaye, *Australia Says U.S. Facial Recognition Software Firm Clearview Breached Privacy Law*, REUTERS (Nov. 3, 2021), https://www.reuters.com/business/cop/australia-says-us-facial-recognition-software-firm-clearview-breached-privacy-2021-11-03/ [https://perma.cc/AEL9-YZXM].

153. Lee Rainie et al., *Public More Likely to See Facial Recognition Use by Police as Good, Rather Than Bad for Society*, PEW RSCH. CTR. (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-

CCTV surveillance, individual facial recognition, and gathering of other images with AI can create what reasonably can be termed a permeating surveillance state. One example is the proposed use of Amazon's Rekogniton software program in Orlando, Florida; the program uses CCTV, facial recognition, and AI to aide law enforcement.[154]

VI. STINGRAYS

A Stingray is a tool used by law enforcement to collect cell phone data.[155] These devices are able to "mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect's cell phone, they also gather information about the phones of countless bystanders who happen to be nearby."[156] To note, Stingrays and tower dumps share similarities. However, Stingrays can gather a larger volume of cellphone data over an extended period of time.[157] States vary on whether Stingrays can be used without a warrant, but in 2015, the Department of Justice announced a new policy that requires federal agents to obtain a search warrant before using a Stingray.[158] While the federal government has taken an encouraging step in preventing warrantless police surveillance,

---

than-bad-for-society/ [https://perma.cc/K39L-YNQ4]; Geoff Kohl, *Extensive New Poll Finds Most Americans Support Facial Recognition*, SEC. INDUS. ASS'N (Oct. 7, 2020), https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/ [https://perma.cc/85NX-RM44].

154. Rekognition is a program that Amazon and the city of Orlando considered implementing that would conduct real-time facial recognition on a city-wide basis. The information generated by the software would be available to law enforcement. *See* Dawn Kawamoto, *Orlando Police to Launch Round of Two Facial Recognition Testing*, GOV'T TECH., https://www.govtech.com/public-safety/orlando-police-to-launch-round-two-of-facial-recognition-testing.html [https://perma.cc/X7LP-APJK] (last visited Mar. 18, 2023). Fortunately, Rekognition is no longer being piloted for use by Orlando police. *See* Nick Statt, *Orlando Police Once Again Ditch Amazon's Facial Recognition Software*, VERGE (July 18, 2019, 8:30 PM), https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended [https://perma.cc/3UYN-2TCR].

155. Zetter, *supra* note 1.

156. *Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them#:~:text=Stingrays%2C%20also%20known%20as%20%22cell,their%20locations%20and%20identifying%20information [https://perma.cc/YKG9-MA4V].

157. ADAM BATES, CATO INST., STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE 5 (2017).

158. U.S. DEP'T OF JUST., DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY *passim* (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/SLM3-QWRD]; *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T OF JUST. (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/GM24-BMXM].

we cannot overlook that prior to this 2015 order, federal agents were using Stingrays without a warrant since 1995.[159]

Some states do require law enforcement to obtain a warrant before using a Stingray. Those states are Washington, D.C.,[160] Florida,[161] New York,[162] California,[163] Maryland,[164] Virginia,[165] Minnesota,[166] Utah[167] and Washington.[168] However, all other states allow the warrantless use of Stingrays to gather information on potential suspects.

United States v. Ellis specifically evaluated the use of Stingray surveillance to determine whether the warrantless search and seizure of historical cell phone records revealing CSLI violates the Fourth Amendment.[169] Law enforcement used a Stingray to locate and arrest Ellis for shooting a police officer.[170] Ellis argued that the use of a Stingray to locate him constituted a warrantless search.[171] The district court ultimately concluded that Ellis had a reasonable expectation of privacy in his real-time cell location, stating "cell phone users have an expectation of privacy in their cell phone location in real time and that society is prepared to recognize that expectation as reasonable."[172] The court continued to say that cell phone users have "an even stronger privacy

159. *STINGRAYS: The Most Common Surveillance Tool the Government Won't Tell You About*, AM. CIV. LIBERTIES UNION N. CAL. (June 24, 2014), https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about [https://perma.cc/FBB3-CYRN].

160. Jones v. United States, 168 A.3d 703, 717 (D.C. 2017).

161. Ferrari v. Florida, 260 So. 3d 295, 307 (Fla. 4th DCA 2018); Florida v. Sylvestre, 254 So. 3d 986, 992 (Fla. 4th DCA 2018).

162. N.Y. CIV. LIBERTIES UNION, MEMORANDUM: WARRANT REQUIREMENT FOR THE USE OF STINGRAYS IN NEW YORK 1 (2015), https://www.nyclu.org/sites/default/files/memo_stingrayuse_NY_201508_final.pdf [https://perma.cc/3NGP-9GQ4].

163. Cyrus Farivar, *California Cops, Want to Use a Stingray? Get a Warrant, Governor Says*, ARS TECHNICA (Oct. 8, 2015, 7:32 PM), https://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/#:~:text=On%20 Thursday%2C%20California%20Governor%20Jerry,intercept%20calls%20and%20text%20messages [https://perma.cc/425J-G73Z].

164. State v. Andrews, 134 A.3d 324, 346–47 (Md. App. Ct. 2016).

165. VA. CODE ANN. § 19.2-70.3 (2022).

166. MINN. STAT. § 626A.28(3) (2022).

167. 2022 Utah Laws 77-23c-101.1.

168. WASH. REV. CODE § 9.73.260(1)–(6) (2022). The provisions require law enforcement to request an ex parte order authorizing the use of the device. *See id.* § 9.73.260(3)–(4). The request must include the type of data being collected, and law enforcement must take "all steps necessary" to permanently delete any information or metadata collected from any party not specified in the court order. *See id.* § 9.73.260(3), (6)(c). Additionally, law enforcement must delete the data from the target within thirty days if there is no longer probable cause to support the belief that such data is evidence of a crime. *See id.* § 9.73.260(6)(c).

169. United States v. Ellis, 270 F. Supp. 3d 1134, 1144 (N.D. Cal. 2017).

170. *Id.* at 1139.

171. *Id.*

172. *Id.* at 1145.

interest in real time location information associated with their cell phones, which act as a close proxy to ones' actual physical location because most cell phone users keep their phones on their person or within reach."[173]

Today, there is an actual subjective expectation of privacy in real-time location information from cell phones gathered over a period of time by law enforcement. As of 2022, seventy-seven percent of Americans own cell phones.[174] In other words, seventy-seven percent of the American population carries a device that can be accessed by a Stingray at any moment. This is concerning because, as the *Riley v. California* Court explained, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[175] This allows law enforcement to build a mosaic of an individual's life, contributing to a permeating surveillance state.

This expectation in real-time location information from cell phones over a period of time is one society is prepared to recognize as reasonable. Law enforcement can use a Stingray to continuously monitor an individual's movements, and that data can be compiled to create a vast database of location information, tracking the public and private movements of individuals.[176] Additionally, the information from Stingrays provides a "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[177] Further, the information gathered is information that law enforcement would not usually have access to if they relied on traditional police surveillance techniques, as it would take weeks or months to gather the same kind of information from interviewing witnesses or subpoenaing camera footage from businesses. Therefore, law enforcement's use of Stingrays constitutes unreasonable searches that should require warrants.

CONCLUSION

The technologies discussed above all raise concerns that law enforcement's use of data-gathering technologies and AI can create a permeating police surveillance state. New technologies must be subjected to the *Katz* test. First, the individual must have an actual, subjective

173. *Id.*

174. Deyan Georgiev, *67+ Revealing Smartphone Statistics for 2022*, TECHJURY (Feb. 26, 2022), https://techjury.net/blog/smartphone-usage-statistics/#gref [https://perma.cc/7UQQ-AJWN].

175. Riley v. California, 573 U.S. 373, 394 (2014).

176. Jones v. United States, 168 A.3d 703, 708 n.7 (D.C. 2017).

177. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

expectation of privacy in the information obtained by law enforcement.[178] Second, the violation must violate society's reasonable expectation of privacy.[179] An individual's reasonable expectation of privacy is violated through the use of these surveillance tools when a search yields data that is objectively intrusive. Surveillance is considered objectively intrusive based on the type of information or locations obtained, the intimate nature of the information that would be otherwise unknowable, and the aggregate of information that creates a detailed and intrusive mosaic of an individual's life.[180]

We cannot say that law enforcement's initial investigation using location-based technologies and other technologies available to investigate or prevent a criminal activity requires a search warrant. However, when technologies are combined to produce a comprehensive surveillance of all citizens, limitations are necessary. Also, when a general investigation converts to a specific investigation on an individual, the use of these technologies becomes a critical issue because they reveal a great deal of personal, intimate, and private intrusive information that law enforcement would not otherwise be able to access. To note, law enforcement does have databases like CODIS, which provide information about individuals.[181] However, the Authors' objection is to the government's use of technology to profile every citizen—an earmark of a surveillance state. Legislatures have already taken steps to limit some of these technologies, especially Stingrays, but there are not enough protections in place. In fact, private corporations like Clearview have databases to aid law enforcement with facial recognition.[182] There must be a policy that draws the line on the government gathering information on citizens, who may or may not have committed a crime. These policies are the best way to prevent the permeating surveillance society the Fourth Amendment was intended to protect us from.

The sum of tower dumps, ALPRs, social media, geofencing, CCTV, Stingrays, and AI provide the potential for collecting, analyzing, and creating a dossier without a warrant that then justifies a warrant. The new technology creates an information matrix that rivals or exceeds the abilities of the "thought police" from George Orwell's *1984* or the "precogs" from Philip K. Dick's *The Minority Report*. We have the Fourth Amendment for a reason. The Supreme Court has stated that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to

178. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

179. *Id.*

181. Commonwealth v. Perry, 184 N.E.3d 745, 757–58 (Mass. 2022).

181. *See Frequently Asked Questions on CODIS and NDIS*, *supra* note 15 (explaining that CODIS is a database that agencies can use to access DNA records).

182. *Company Overview*, *supra* note 151.

'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[183] In this Article, the Authors have provided guidance for where the courts can establish protections for individuals and their information. Additionally, the Authors have found that *Kyllo* is obsolete when new technologies are becoming publicly available so rapidly,[184] and the Authors have argued that the third-party doctrine must be limited in this new digital age. Further, a search warrant must be required when law enforcement's investigations become targeted and intrusive. There is a realm of privacy and individuality that must be protected from the government unless the government shows a good reason to intrude—that is, obtaining a warrant. The speed of technological innovation has outpaced the law, and it is time to draw a line.

183. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27 (2001)) (brackets in original).

184. *See supra* note 30.

BOMB BODY POLITICS: ON THE TSA'S ALGORITHIMIC POLICING OF GENDER

Kendra Albert and *Avatara Smith-Carrington*[*]

Abstract

Long before modern discussions of algorithmic policing, the Department of Homeland Security was using sexist and racist algorithms to determine which individuals to subject to additional screening. The algorithms are built into the Transportation Safety Administration's advanced imaging technology, and they are used to justify the systems of policing already in place. In this Article adapted from remarks delivered at the Technology, Media, Privacy, and the Law Conference in 2022, the TSA's discriminatory practices against transgender people serve as a cautionary tale for surveillance reformers who risk entrenching violence against the "wrong" bodies to protect the "right" ones.

INTRODUCTION

When technology law and policy scholars talk about algorithmic policing, there are archetypal examples that we return to: Shotspotter, LASER, COMPAS, and whatever Palantir is marketing this week. I am not a scholar of policing, and my work on algorithmic harms focuses in areas quite different from those examples. But I do have a cautionary tale about how we think about this space, and it involves millimeter wave body scanners.

I. THE TSA AND ALGORITHMIC POLICING

If you were flying to attend a conference like the one that this Article was first presented at, you would have likely gone through a millimeter wave body scanner as part of a TSA screening. Many folks have had this experience—you put your hands up in cactus arms and then you stand in the tube. If you are lucky, you come out the other side and are given the "all clear," and you walk to your gate.

---

* This Article is an adaptation of remarks prepared for the 2022 Technology, Media, & Privacy Law Conference at the University of Florida College of Law by Kendra Albert. Avatara Smith-Carrington is listed as a co-author because of their substantial contributions to the underlying theories and knowledge, but the words are Kendra's. Thank you to Afsaneh Rigot for her valuable feedback, and Jessica Fjeld and Apryl Williams for the title.

Now, what some people may not know is how the advanced imaging technology of the type used in these tools works. As the Transportation Safety Administration says, it uses automated target recognition (ATR) technology to "eliminate passenger specific imagery and auto-detect[] potential threats."[1] When you approach a TSA scanner, a TSA agent looks at you and makes a decision about what button to push—blue if they think you are a man, and pink if they think you are a woman.[2] That button determines the algorithm that your body is matched against.[3] The algorithm then determines what is normal, and that which is not shows up as an anomaly on the screen, causing further screening—including potentially invasive pat-downs.[4] The development of such algorithms was proprietary. We do not know who developed them, or what training data they used to produce the ultimate equations, or whether that data is up to date. What we do know is that these systems discriminate.

If you are a Black woman with natural hair, your hair may be an anomaly, as Simone Browne discussed in her book, *Dark Matters*.[5] If you are Sikh or Muslim and wear religious headwear, like a turban or a hijab, you may be subjected to an additional pat-down, just because.[6] God forbid if you exercise your right to religious expression under the First Amendment and wear a burqa.[7] But that pink or blue button does a lot of

1. *TSA to Begin Testing New Advanced Imaging Technology Software at Select U.S. Airports to Further Enhance Passenger Privacy*, PR NEWS WIRE (Feb. 1, 2011, 12:34 PM), https://www.prnewswire.com/news-releases/tsa-to-begin-testing-new-advanced-imaging-technology-software-at-select-us-airports-to-further-enhance-passenger-privacy-115022109.html [https://perma.cc/AY7E-M6YU].

2. TOBY BEAUCHAMP, GOING STEALTH: TRANSGENDER POLITICS AND U.S. SURVEILLANCE PRACTICES 50 (2019).

3. *Id.*

4. *Id.* at 50–51.

5. SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 161–62 (2015); *see* Gaby Del Valle, *How Airport Scanners Discriminate Against Passengers of Color*, VOX (Apr. 17, 2019), https://www.vox.com/the-goods/2019/4/17/18412450/tsa-airport-full-body-scanners-racist [https://perma.cc/K6NG-ZGB4] ("[B]lack passengers who wear their hair naturally—or who wear it in styles typically associated with black culture, like braids or dreadlocks—seem to be disproportionately targeted.").

6. *See* SIKH COALITION, KNOW YOUR RIGHTS AT THE AIRPORT 2 (2018), https://www.sikhcoalition.org/wp-content/uploads/2018/11/tsa-know-your-rights-2018-1.pdf [https://perma.cc/8NC6-VWBQ] ("Travelers wearing turbans may be subject to additional security screening."). TSA harassment of women wearing hijabs is well-documented. *See, e.g.*, Nicole Rojas, *Fourteen Women Are Claiming TSA Harassed Them for Wearing Hijabs at Newark Airport*, NEWSWEEK (June 8, 2018), https://www.newsweek.com/fourteen-women-claim-tsa-harassed-them-wearing-hijabs-newark-airport-967771 [https://perma.cc/69KD-VQ4U] (discussing fourteen Muslim women who wore hijabs to the airport and were subject to two hours of pat-downs, causing them to miss their flight).

7. *See* U.S. CONST. AMEND. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof."); *see also* Tatiana Walk-Morris, *What to Do If You Face Anti-Muslim Discrimination at Airport Security*, VICE (Sept. 10, 2021),

work. If the TSA agent reads you as a woman but you have a penis, that will present an anomaly.[8] If you are white and non-binary and TSA agents cannot quite figure out what you are, or how to fit you into a literal pink or blue box, good luck—you are getting patted down for sure, and have fun finding a TSA agent that shares your gender identity to do so. (A promise that the TSA makes, in albeit oblique terms.[9]) Of course, if you are Black and trans, or Black and non-binary, or Muslim and trans, or Muslim and non-binary, the chances that this "routine" process will result in extensive questioning and invasive procedures increase quite significantly.[10]

Advanced imaging technology is not "artificial intelligence" or "machine learning," but it is algorithmic policing, in the most literal sense.[11] Long before "FAccT,"[12] or ProPublica's Correctional Offender

---

https://www.vice.com/en/article/epnwjz/what-to-do-if-you-face-anti-muslim-discrimination-islamophobia-at-airport-security [https://perma.cc/XZ9K-LSEN] ("According to TSA basic training documents . . . trainees are . . . . made aware that hijabs and burqas are non-form fitting headwear that could conceal prohibited items, but travelers aren't required to remove them for religious reasons.").

8. *See* Dawn Ennis, *Goodbye, "Anomaly"—TSA's New Word for Trans Bodies Is "Alarm"*, ADVOCATE (Dec. 23, 2015, 9:37 PM), http://www.advocate.com/transgender/2015/12/23/goodbye-anomaly-tsas-new-word-trans-bodies-alarm [https://perma.cc/D2KU-2K3S] (explaining that the TSA previously used the word "anomaly" whenever screening machines detected a transgender traveler).

9. *See What Can I Expect During Pat-Down Screening?*, TRANSP. SEC. ADMIN., https://www.tsa.gov/travel/frequently-asked-questions/what-can-i-expect-during-pat-down-screening [https://perma.cc/8TAR-JYWC] (last visited Mar. 23, 2023) ("The screening is conducted by a TSA officer of the same gender.").

10. *See* Lucas Waldron & Brenda Medina, *When Transgender Travelers Walk into Scanners, Invasive Searches Sometimes Wait on the Other Side*, PROPUBLICA (Aug. 16, 2019, 5:00 AM), https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches-often-wait-on-the-other-side [https://perma.cc/5W83-ASEB]; *Perspectives on TSA's Policies to Prevent Unlawful Profiling: Hearing Before the Comm. on Homeland Sec.*, 116th Cong. 6, 11, 13, 17, 28, 37, 39 (2019) (statement of Hon. Shelia Jackson Lee, Cong. Rep. of Tex.; statement of W. William Russel, Acting Dir., Homeland Sec. & Just. Team; statement of Sim J. Singh, Senior Manager of Pol'y & Advoc., The Sikh Coal.; statement of Janai S. Nelson, Assoc. Dir.-Couns., NAACP Legal Def. & Educ. Fund, Inc.).

11. *See* MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 89 (2018) ("[C]omputer scientists know that machine 'learning' is more akin to a metaphor in this case: it means that the machine can improve at its programmed, routine, automated tasks. It doesn't mean that the machine acquires knowledge or wisdom or agency, despite what the term *learning* might imply. This type of linguistic confusion is at the root of many misconceptions about computers."); *see also* Emily Tucker, *Artifice and Intelligence*, CTR. ON PRIV. & TECHN. GEO. L. (Mar. 8, 2022), https://medium.com/center-on-privacy-technology/artifice-and-intelligence%C2%B9-f00da128d3cd [https://perma.cc/V8ZA-QPL7] ("Whatever the merit of the scientific aspirations originally encompassed by the term 'artificial intelligence,' it's a phrase that now functions in the vernacular primarily to obfuscate, alienate, and glamorize.").

12. "FAccT" is the Association for Computing Machinery (ACM) Conference on Fairness, Accountability, and Transparency which "brings together researchers and practitioners interested

Management Profiling for Alternative Sanctions (COMPAS) reporting,[13] or Andrew Ferguson's book,[14] the Department of Homeland Security was using sexist, racist algorithms to determine who would be subject to additional screening. The algorithms that are built into these technologies are used to justify the systems of policing already in place. These algorithms mirror the systems that I and others, most prominently Sasha Constanza-Chock, have written about, in that they assume a binary of gender and bodies, a concordance between sex and appearance, and punish those who may not conform.[15] It is the algorithmic decision of what bodies are normal, acceptable, and safe versus which ones are deviant.[16] It is the production of the tools of policing that are algorithmically incapable of respecting the diversity of the people who encounter them. Forms of violence are targeted by algorithms, albeit on a level different than drone strikes or additional police stops.[17]

It is easy to pretend that debiasing these algorithms could somehow fix them. As a result of years of activism, the TSA announced on Transgender Day of Visibility in 2022 that they were developing an algorithm that does not require a pink or blue box checking exercise.[18] In my work with Maggie Delano on medical devices, I have called such

---

in fairness, accountability, and transparency in socio-technical systems." It was founded in 2018. *See* ACM CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY, https://facctconference.org [https://perma.cc/CQC6-PJNQ] (last visited Mar. 23, 2023).

13. *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=TiqCeZIj4uLbXl91e3wM2PnmnWbCVOvS [https://perma.cc/QF6E-3TAW] (reporting that the risk assessment tool COMPAS is intended for use by judges to determine which criminal defendants are eligible for probation or treatment programs but that the tool disproportionately identifies Black individuals as being a high risk to the community).

14. ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT *passim* (2017).

15. SASHA COSTANZA-CHOCK, DESIGN JUSTICE: COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED 1–5 (2020); *see* Kendra Albert & Maggie Delano, *Sex Trouble: Sex/Gender Slippage, Sex Confusion, and Sex Obsession in Machine Learning Using Electronic Health Records*, 3 PATTERNS 1, 1 (2022) (discussing how machine learning datasets used for healthcare applications can ignore the complexities of gender).

16. For more on the construction of social deviance through these systems, *see* Merav Amir & Hagar Kotef, *In-Secure Identities: On the Securitization of Abnormality*, 36 ENV'T & PLAN. D: SOC'Y & SPACE 236 *passim* (2018).

17. *Compare* Angwin et al., *supra* note 13 (describing an algorithm used to predict the likelihood an individual will commit another crime), *with* ALASDAIR MCKAY ET AL., REMOTE WARFARE: INTERDISCIPLINARY PERSPECTIVES 187 (2021) (describing an algorithm used to choose where to launch drone strikes), *and* NAT'L ACADS. OF SCIS., ENG'G, & MED., PROACTIVE POLICING: EFFECTS ON CRIME AND COMMUNITIES 109–10 (David Weisburd & Malay K. Majmundar eds., 2018) (describing an algorithm used to identify neighborhoods as crime hotspots for increased policing).

18. Arli Christian, *Four Ways the TSA Is Making Flying Easier for Transgender People*, AM. CIV. LIBERTIES UNION (Apr. 5, 2022), https://www.aclu.org/news/lgbtq-rights/four-ways-the-tsa-is-making-flying-easier-for-transgender-people [https://perma.cc/C3CD-T8YP].

fixes "rainbow band-aids" because they fail to actually disrupt the normative assumptions about gender, sex, and bodies that algorithmic designers make.[19] In policing contexts, I am not sure a "rainbow band-aid" covers it, unless we imagine an adhesive bandage placed over a gaping, festering wound. As Toby Beauchamp argued in his book, *Going Stealth*, it is easy to use such technologies to foreground "questions of gender, vulnerability, and individual privacy rather than [those] of citizenship and structural racism."[20] In fact, that is partly how we ended up with advanced imaging technologies in the first place. The widespread backlash to millimeter wave scanners and their ability to produce detailed "naked" images of travelers, which invaded their privacy, explains the move to the algorithmic anomaly standard, ATR, and the requirement of TSA-assigned gender based on presentation.[21] In short, the urge to reform the system to fit the privacy needs of White, upper middle class, cisgender Americans created forms of targeted violence against others.[22]

That is why transgender folks like me must resist the urge to make this a conversation about how the TSA's security apparatus can become more welcoming or friendly to just us. As Avatara Smith-Carrington has pointed out, such proposals by White transgender people end up reinforcing the hold of policing systems. Here, I also builds on the arguments of Stop LAPD Spying and the Carceral Tech Resistance Network, who have pointed out that those arguing for the reform of surveillance technologies often end up legitimating their use.[23] As Stop

19. Kendra Albert & Maggie Delano, *"This Whole Thing Smacks of Gender": Algorithmic Exclusion in Bioimpedance-Based Body Composition Analysis*, YOUTUBE (May 5, 2021), https://www.youtube.com/watch?v=JcLvBFqjqo4&list=PLXA0IWa3BpHkdkCkbcUpm2im-rjoVvji4&index=35 [https://perma.cc/CBT7-VRM3]; *see* Kendra Albert & Maggie Delano, *"This Whole Thing Smacks of Gender": Algorithmic Exclusion in Bioimpedance-Based Body Composition Analysis*, 2021 FACCT '21: PROC. 2021 ACM CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY 342, 349 (explaining that eliminating the use of sex or gender as a proxy in bioelectrical impedance analysis equations does not remove the "pervasive assumptions about sex and gender" in clinical research).

20. BEAUCHAMP, *supra* note 2, at 64.

21. *See* Scott Neuman, *TSA: No More Graphic, Full-Body Airport Scans*, NPR (May 30, 2013, 7:19 PM), https://www.npr.org/sections/thetwo-way/2013/05/30/187376559/tsa-no-more-graphic-full-body-airport-scans [https://perma.cc/P37D-BZS4] ("[A]s of May 16, [2013,] all U.S. airport scanners that had been equipped with the offending Advanced Imaging Technology, or AIT, have been loaded with software called [ATR], which shows only generic images of the passengers."). The Author is grateful to the research efforts of Zoe Kaiser and Arabi Hassan, who helped them fully understand the relationship between the privacy backlash and ATR, albeit for a different context.

22. *See generally* Christian, *supra* note 18 (discussing how harassment and mistreatment of trans individuals in the airport led the TSA to develop new policies that move away from assumptions about the binary of gender and bodies).

23. Stop LAPD Spying Coal., *Co-Optation and Counterinsurgency in Surveillance Reform*, LPE PROJECT (Mar. 15, 2022), https://lpeproject.org/blog/co-optation-and-counterinsurgency-in-surveillance-reform/ [https://perma.cc/T3SA-FURS]; *Our Practice // Our Community*

LAPD Spying articulated in a recent piece on the Law and Political Economy (LPE) blog, "[t]his ecosystem of nonprofit reform advocacy must be understood as a form of counterinsurgency, helping the state absorb the shocks generated by abolitionist organizing."[24]

As we play around the margins, rather than pointing out the fundamental racism of American efforts to police "terrorism," we provide cover for policing the "right" people (read: Muslim, Black, Brown, radical, mad, poor, disabled) instead of the wrong ones. The choice of which bodies to normalize and proclaim safe is not an accident—it is the system working as intended. White transgender people's fight for the right to be seen as part of that body politic comes at the rejection of a solidarity with those who will never be "safe" enough.

CONCLUSION

The use of ATR is a cautionary tale for privacy advocates and others who see the use of algorithmic technologies as a panacea against the vagaries and harm of human judgment. Although there are undoubtedly forms of bias and harm that have been eliminated by the shift to millimeter wave scanners with ATR algorithmic tools, they come at the cost of engraining forms of discrimination into the literal code of the tools that are theoretically meant to protect certain people. The failure to meaningfully center the most impacted in discussions of how to change the TSA's practices, as my colleague Afsaneh Rigot has described in her work on "design from the margins," results in algorithms that fundamentally cannot ever be fair, even aside from the illegitimate context of American imperialist views on terrorism.[25]

We already know the future of algorithmic policing. To quote William Gibson, "[d]ystopia is already here, it's just not . . ."[26] evenly distributed.

Commitments, CARCERAL TECH RESISTANCE NETWORK, https://www.carceral.tech/practice [https://perma.cc/W5BA-MKR7] (last visited Mar. 25, 2023).

24. Stop LAPD Spying Coal., *supra* note 23. *See generally* Sarah T. Hamid, *Community Defense: Sarah T. Hamid on Abolishing Carceral Technologies*, LOGIC MAG. (Aug. 31, 2020), https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishing-carceral-technologies/ [https://perma.cc/R4TJ-X6ES] ("There was an intentional move . . . to push back on these technologies by presenting surveillance as a generalized harm . . . . This was a well-intentioned move. But it muted much of what directly impacted communities needed to talk about.").

25. AFSANEH RIGOT, BELFER CTR. FOR SCI. & INT'L AFFS., DESIGN FROM THE MARGINS *passim* (2022).

26. William Gibson (@GreatDismal), TWITTER (Aug. 22, 2015, 4:26 PM), https://twitter.com/greatdismal/status/635186310550962176 [https://perma.cc/8YLA-Z9J7].

PRIVACY IN AN ERA OF ADVANCING TECHNOLOGY

Russell L. Weaver[*]

Abstract

This Article examines the privacy implications of new technologies, in particular facial recognition technology (FRT), which uses biometric software to recognize a person's facial features. When used in conjunction with closed-circuit television (CCTV) or drones, FRT has allowed governments to continuously monitor public places and has helped law enforcement officials to locate and apprehend criminals. But many are uneasy regarding the privacy implications of FRT technology, which can often be unreliable. The difficulty is that the Fourth Amendment imposes few meaningful limits on governmental use of modern technologies in public places, although some states have imposed limitations by statute.

INTRODUCTION

Technology has made it increasingly difficult for individuals to maintain their privacy.[1] When the United States was founded in the eighteenth century, the government had only crude means for spying on the citizenry. For example, the police might have eavesdropped on their fellow citizens in taverns or other public settings or listened outside a suspect's window. However, without the advanced technologies that

* Professor of Law and Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law. Professor Weaver wishes to thank the University of Louisville's Distinguished University Scholar program for supporting his research. Portions of this Article are drawn from a prior publication, Russell L. Weaver, *The Constitutional Implications of Drones, Facial Recognition Technology and CCTV*, 6 PUB. GOVERNANCE, ADMIN. & FINS. L. REV. 53–65 (2021). Reprinted with permission.

1. *See* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1136 (2011) ("The steady onslaught of technology has raised troubling implications for individual privacy.").

exist today, the opportunities for successful eavesdropping were very limited.

The situation is dramatically different today. Surveillance technologies have gone high tech, creating Orwellian possibilities for snooping. As one commentator observed, "rapid technological advances and the consequent recognition of the 'frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society' have underlined the possibility of worse horrors yet to come."[2]

Electricity was a transformative invention because it made possible the creation of super-sensitive microphones with the ability to overhear conversations from far away, as well as through walls, and led to the invention of facial recognition and CCTV systems, which allow the government to maintain continuous surveillance of public places.[3] Electricity also led to the creation of GPS monitoring systems, which allow the police to monitor the location and movements of individuals and things; X-ray technology, which enables the police to peer through walls and into the privacy of homes by using drive-by X-ray vans; and devices that allow people to monitor the computer key strokes of individuals from distant places.[4]

---

2. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 386 (1974).

3. *See* Silverman v. United States, 365 U.S. 505, 506–07 (1961) (demonstrating that advanced surveillance technologies were already available in the 1960s); *see also* Katz v. United States, 389 U.S. 347, 348 (1967) (involving the attachment of an electronic listening device to the outside of a phone booth so that the police could overhear what was being said inside the phone booth); Goldman v. United States, 316 U.S. 129, 131–32 (1942) (involving the use of a listening device that allowed the police to overhear what was being said in Goldman's office even though the police were located in an adjoining office); Dina Temple-Raston & Robert Smith, *U.S. Eyes U.K.'s Surveillance Cameras*, NPR (July 8, 2007, 8:00 AM), http://www.npr.org/templates/story/story.php?storyId=11813693 [https://perma.cc/L4ZN-4FUN] (discussing how police in Great Britain have been using CCTV cameras to combat terrorism since the 1990s).

4. *See* Devega v. State, 689 S.E.2d 293, 299–300 (Ga. 2010) (finding no violation of the Fourth Amendment when investigators requested that the defendant's cell phone provider "ping" the defendant's phone and used GPS to locate the defendant in his vehicle); Andy Greenberg, *Scanner Vans Allow Drive-By Snooping*, FORBES (Sept. 9, 2010, 12:40 PM), http://www.forbes.com/forbes/2010/0927/technology-x-rays-homeland-security-aclu-drive-by-snooping.html?feed=rss_technology [https://perma.cc/J6VB-YQGB] ("American Science & Engineering . . . has sold U.S. and foreign government agencies more than 500 backscatter X-ray scanners mounted in vans that can be driven past neighboring vehicles or cargo containers to snoop into their contents."); Rania M. Basha, *Kyllo v. United States: The Fourth Amendment Triumphs over Technology*, 41 BRANDEIS L.J. 939, 939 (2003) ("[T]here are some devices, such as x-ray systems and radar flashlights, which enable officers to see through walls."); Alan F. Blakley et al., *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 4 DUKE L. & TECH. REV. 1, 4 n.18 (2005) (explaining the capabilities of spyware, including the monitoring of key strokes). *See generally* City of Ontario v. Quon, 130 S. Ct. 2619, 2625 (2010) (discussing how a city reserved the right to monitor all network activity on pagers issued to the city's police); Jason Broberg,

This Article focuses on one of these new technologies: governmental monitoring of citizens in public places through devices such as drones, FRT, and CCTV. As will be seen, in the United States, there are few restrictions on governmental use of these technologies.

I. THE DEVELOPMENT OF NEWER TECHNOLOGIES

U.S. government organizations monitor what happens in public spaces using technologies that only have increased in sophistication and reach over time. By 2018, some 910 state and local public safety agencies, including 599 law enforcement agencies, were using drones.[5] Drones can be equipped with high-powered cameras that allow them to magnify images on the ground by 180 times, thereby making them effective spies that can take detailed pictures of what is happening below.[6] As a result, drones can observe activities that may not be observable from ground level, including things that are happening in individuals' backyards.[7]

FRT "uses biometric software to map a person's facial features from a video or photo."[8] The technology can then identify a person by pinpoint matching his or her facial features with information contained in existing databases.[9] CCTV is also being used to monitor what goes on in public places.[10] For example, in the London Underground, there is a pervasive CCTV system that includes some 15,516 cameras.[11] The United States is

---

From CALEA to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretap Digital Telecommunications, 77 N. DAKOTA L. REV. 795, 795 (2001) (describing the Communications Assistance for Law Enforcement Act (CALEA), which mandated that phone carriers "assist law enforcement in obtaining the content of digital telephone calls and information that may identify a call, such as a telephone number"); Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 447 (2007) ("Over the past decade, the amount of personal information collected, stored, and shared by private companies has skyrocketed due to the rise of internet communication, decreased cost of data storage, and the emergence of data brokerage companies.").

5. Jake Laperruque & David Janovsky, *These Police Drones Are Watching You*, PROJECT ON GOV'T OVERSIGHT (Sept. 25, 2018), https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/ [https://perma.cc/LSV4-DKUT].

6. *Id.*

7. *Id.*

8. Terry Collins, *Facial Recognition: Do You Really Control How Your Face Is Being Used*, USA TODAY (Dec. 23, 2019, 3:30 PM), https://www.usatoday.com/story/tech/2019/11/19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/ [https://perma.cc/9FNW-LS99].

9. *Id.*

10. *Privacy in Public*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/surveillance-oversight/privacy-in-public/ [https://perma.cc/Z6ZW-GP32] (last visited Mar. 29, 2023).

11. *Which London Underground Station Has the Most CCTV Cameras?*, AAI SEC. SYS., https://www.aaisecurity.co.uk/news/cctv-london-underground/#:~:text=There%20is%20a%20total%20of,visitors%20to%20London's%20underground%20maze [https://perma.cc/Z3K8-JVNR] (last visited Mar. 29, 2023).

awash in CCTV systems, with Atlanta having 15.56 cameras per 1,000 people, and Chicago having 35,000 cameras or 13.06 cameras per 1,000 people.[12] Indeed, six U.S. cities (Atlanta, Chicago, Washington, D.C., San Francisco, San Diego, and Boston) made the list of the most surveilled cities in the world.[13]

II. THE BENEFITS OF DRONES, FRT, AND CCTV

Unquestionably, drones, CCTV, and FRT can offer enormous benefits to governmental officials in their efforts to serve the public. For example, when hikers are lost in remote areas, drones can help locate the hikers.[14] Likewise, following hurricanes, drones can "assess damage, locate victims, and deliver aid."[15] In an effort to prevent forest fires, drones equipped with thermal imaging cameras can survey forests.[16] Drones can also monitor the health and well-being of wild animals.[17]

CCTV and FRT also are enormously helpful in locating and apprehending criminal suspects.[18] CCTV can provide continuous, recorded video monitoring of public areas, so that the police can review tape recordings and identify suspects after a crime has been committed.[19] Following the London subway bombings in July 2005, during which fifty-two people were killed and another 700 were injured, the bombers were identified through police review of London Underground CCTV footage.[20] Similarly, the Boston Marathon bombers, who killed three people and injured hundreds of others, were found and apprehended using

12. Jason Plautz, *6 US Cities Top List of World's Most Surveilled*, SMART CITIES DIVE (Sept. 23, 2019), https://www.smartcitiesdive.com/news/6-us-cities-top-list-of-worlds-most-surveilled/563438/ [https://perma.cc/72D8-2F5E].

13. *Id.*

14. Hailey Higgins, *Search and Rescue Teams Use Drone to Help Injured Hiker in Southern Utah*, FOX 13 SALT LAKE CITY (Jan. 20, 2020, 9:29 PM), https://www.fox13now.com/2020/01/20/search-and-rescue-teams-use-drone-to-help-injured-hiker-in-southern-utah/ [https://perma.cc/75S9-R5RA].

15. *38 Ways Drones Will Impact Society: From Fighting War to Forecasting Weather, UAVs Change Everything*, CB INSIGHTS (Jan. 9, 2020), https://www.cbinsights.com/research/drone-impact-society-uav/ [https://perma.cc/UU6M-7NBV].

16. *Id.*

17. *Id.*

18. *See* Collins, *supra* note 8 ("Police departments regularly use facial recognition to find potential crime suspects and witnesses by scanning through millions of photos.").

19. *Role of CCTV Cameras: Public, Privacy and Protection*, IFSEC GLOB. (Jan. 1, 2021) [hereinafter *Role of CCTV Cameras*], https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/ [https://perma.cc/2HVK-PTU7].

20. *July 7 2005 London Bombings Fast Facts*, CNN (June 23, 2021, 7:38 AM), https://www.cnn.com/2013/11/06/world/europe/july-7-2005-london-bombings-fast-facts [https://perma.cc/XF6H-EHM9]; *7 July Bombers Spotted on CCTV After Exhaustive Hunt*, BRITISH BROAD. CORP. (Oct. 13, 2010), https://www.bbc.com/news/uk-11534951 [https://perma.cc/ULM2-2T2Z].

CCTV images captured on government and private cameras.[21] The bombers stood out on the video because of the way they acted: while the crowd was fleeing the scene, the Tsarnaev brothers lingered around or walked away casually.[22] In tracking down those who attacked the U.S. Capitol Building on January 6, 2021, the FBI used CCTV images and FRT, among other techniques.[23]

III. PRIVACY CONCERNS

As FRT, CCTV, and drones have proliferated, major privacy concerns have arisen. As one writer noted: "[P]rivacy advocates and other citizens are uneasy with the idea that Big Brother is monitoring their every public move."[24] For example, when New York City announced that it was going to deploy fourteen drones, purportedly to assist in emergencies, civil libertarians complained that the drones could "easily be used to track . . . those who speak out against City Hall and police."[25] As one commentator noted, "The NYPD's drone policy places no meaningful restrictions on police deployment of drones in New York City and opens the door to the police department by building a permanent archive of drone footage of political activity and intimate private behavior visible only from the sky."[26]

Similar concerns have been raised regarding FRT. The dimensions of modern FRT are truly staggering:

> [W]ith a single high-resolution snap shot, FRT, has the ability to map out a biometric profile that is as individually

21. *See* Heather Kelly, *After Boston: The Pros and Cons of Surveillance Cameras*, CNN BUS. (Apr. 26, 2013, 7:03 PM), https://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/index.html [https://perma.cc/A2UX-6R9D] ("After last week's bombings at the Boston Marathon, authorities had to sift through a mountain of footage from government surveillance cameras, private security cameras and imagery shot by bystanders on smartphones. It took the FBI only three days to release blurry shots of the two suspects, taken by a department store's cameras."); *see also Role of CCTV Cameras*, *supra* note 19 ("The potential value of public surveillance technology was well demonstrated all the way back in April, 2013 when investigators identified the two suspects in the Boston Marathon bombing after sifting through video images captured by the city's cameras.").

22. *Surveillance and Solving the Boston Bombing*, NCAVF, https://ncavf.com/press/surveillance-and-solving-the-boston-bombing/ [https://perma.cc/VV3E-JWKH] (last visited Mar. 29, 2023).

23. Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/7KQB-72NH].

24. Kelly, *supra* note 21.

25. Dennis Romero, *NYPD to Deploy Drone Fleet, Stoking Fears of Big Brother*, U.S. NEWS (Dec. 4, 2018), https://www.nbcnews.com/news/us-news/nypd-deploy-drone-fleet-stoking-fears-big-brother-n943876 [https://perma.cc/6CW7-ALBG].

26. *Id.*

> unique as a human fingerprint. With images sharing the same binary 1 and 0 sequences as text, the source noted that big data software and storage capacity currently exists to construct a truly three-dimensional profile of, well, anyone with a digital image online.[27]

One source denounced FRT as "an unreliable, biased and dystopian threat to privacy."[28] The American Civil Liberties Union summarized the impact of FRT as follows: "Face recognition offers governments a surveillance capability unlike any other technology in the past. The powerful capability can enable the government to identify who attends protests, political rallies, church, or AA meetings on an unprecedented scale."[29] Despite the concerns, FRT use seems to be expanding and is now used by U.S. Customs and Border Patrol.[30]

CCTV raises similar concerns. As one commentator argued, "[t]he advent of sophisticated technology that allows the government to watch, zoom in on, track, and record the activities of anyone, anywhere in public, twenty-four hours a day, demands regulation."[31] CCTV is particularly potent when it is combined with FRT. CCTV accumulates a mountain of facial images that can then be fed into an FRT system to identify people.[32]

The difficulty is that current drones, FRT, and CCTV technology provide only a glimpse of what is to come. The FBI is spending more than a billion dollars to expand its Next Generation Identification (NGI) system.[33] That system will include huge amounts of information about

---

27. Gavin P. Sullivan, *Big Brother's Tracking Shines Light on Emerging Facial Recognition Technology*, FORBES (July 9, 2013, 11:22 AM), https://www.forbes.com/sites/mergermarket/2013/07/09/big-brothers-tracking-shines-light-on-emerging-facial-recognition-technology/?sh=714dae3c40f0 [https://perma.cc/B882-2KWK].

28. Sean O'Brien, *Time to Face Up to Big Brother*, NEW HAVEN INDEP. (Mar. 9, 2020), https://www.newhavenindependent.org/index.php/archives/entry/facial_recognition/ [https://perma.cc/WBY8-D86M].

29. Abdullah Hassan, *2019 Proved We Can Stop Face Recognition Surveillance*, AM. C.L. UNION (Jan. 17, 2020), https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/ [https://perma.cc/VN9N-S8F8].

30. *State Facial Recognition Policy*, ELEC. PRIV. INFO. CTR., https://epic.org/state-policy/facialrecognition/ [https://perma.cc/MYC5-X9AF] (last visited Oct. 27, 2022).

31. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and Right to Anonymity*, 72 MISS. L.J. 213, 215 (2002).

32. *See* Kelly, *supra* note 21 ("[F]acial-recognition software and other technologies are making security-camera images more valuable to law enforcement. Now, software can automatically mine surveillance footage for information, such as a specific person's face, and create a giant searchable database.").

33. *See Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/6HEL-D9SX] (last visited Mar. 29, 2023) ("This new system, the Next Generation Identification (NGI), provides the criminal justice community with the world's largest and most efficient electronic repository of biometric and criminal history information.").

people, including iris scans, photos, palm prints, gait and voice recordings, scars, tattoos, and DNA.[34]

IV. LEGAL LIMITATIONS

There are few meaningful limits on governmental use of these modern technologies in public places. There have been isolated attempts by individual jurisdictions to limit or control the use of FRT and CCTV in public spaces.[35] The Electronic Privacy Information Center notes that several U.S. cities (for example, San Francisco, California, Somerville, Massachusetts, and Oakland, California) have banned the use of FRT, and that the State of California has imposed a moratorium on its use.[36] However, there are few restrictions on governmental use of CCTV.

There are some restrictions on government's use of drones. For example, many states have provisions governing the flying of drones by private citizens, but these laws place few restrictions on governmental use.[37] The federal government does impose some limitations on drone pilots. For example, governmental "pilots" must either comply with Federal Aviation Administration (FAA) Rule 107 waiver requirements or obtain a federal certificate.[38] In addition, drones cannot be flown within

34. *Next Generation Identification - FBI*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/fbi/ngi.html [https://perma.cc/ST9E-EWSK] (last visited Mar. 30, 2023).

35. For example, Boston, Massachusetts, and Portland, Oregon, have banned the use of FRT. *See* Natasha G. Kohne et al., *Portland City Council Passes Strongest Ban on Facial Recognition in US*, AKIN (Sept. 29, 2020), https://www.akingump.com/en/insights/blogs/ag-data-dive/portland-city-council-passes-strongest-ban-on-facial-recognition-in-us#:~:text=Other%20cities%2C%20such%20as%20San,businesses%20from%20using%20facial%20recognition [https://perma.cc/YZ3U-3JJ8]. In 2020, IBM announced that it would "no longer offer facial recognition products." *See* Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress.*, VOX (June 11, 2020, 5:02 PM), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police [https://perma.cc/9TL5-LP4G]. Similarly, Microsoft announced that it would not sell facial recognition to the police until the federal government passes a law regulating its use, and Amazon instituted a one-year moratorium on the use of its facial recognition software by police. *Id.*

36. *State Facial Recognition Policy*, *supra* note 30.

37. For a comprehensive list of state drone laws, *see Master List of Drone Laws (Organized by State & Country)*, UAV COACH, https://uavcoach.com/drone-laws/ [https://perma.cc/M2RU-N36U] (last visited Mar. 30, 2023).

38. *See Part 107 Waiver*, FED. AVIATION ADMIN. (July 14, 2022), https://www.faa.gov/uas/commercial_operators/part_107_waivers/ [https://perma.cc/U56C-T8J5] ("You do not need a waiver to fly a drone following part 107 rules. You do need a waiver when you want to operate a drone contrary to the rules in part 107."); *see also Certificated Remote Pilots Including Commercial Operators*, FED. AVIATION ADMIN., https://www.faa.gov/uas/commercial_operators/ [https://perma.cc/NRP8-X3VT] (last visited Mar. 30, 2023) (explaining the steps to obtain certification to fly under FAA Rule 107).

400 feet of the ground or over venues such as military bases or public landmarks.[39]

One might think that the U.S. Constitution would limit the use of surveillance technologies, but it imposes relatively few restrictions on governmental uses of advanced technologies in public places. The most obvious constitutional limitation is the Fourth Amendment to the U.S. Constitution, which prohibits "unreasonable searches and seizures."[40] Historically, the Fourth Amendment has prohibited only "trespassory" invasions into "constitutionally protected areas."[41] That approach provided few protections against the use of advanced technologies.[42] For example, in *Olmstead v. United States*, when the police wiretapped phone calls made from the defendant's home, the Court held that there was no "search" within the meaning of the Fourth Amendment because the police did not trespass or intrude into a constitutionally protected area.[43] In other words, the wiretapping was permissible because it was conducted from a public place.[44] Likewise, in *Goldman v. United States*, when the police held a "detectaphone" against an office wall, thereby allowing them to overhear what was being said in an adjoining office, the Court again held that there was no search because the police did not trespass into the adjoining office.[45]

---

39. *Critical Infrastructure and Public Venues*, FED. AVIATION ADMIN., https://www.faa.gov/uas/critical_infrastructure/ [https://perma.cc/U8KH-HCRW] (last visited Mar. 30, 2023).

40. U.S. CONST. amend. IV.

41. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134–35 (1942) (explaining that use of a detectaphone was not an illegal trespass and not a violation of the Fourth Amendment), *abrogated by* Katz v. United States, 389 U.S. 347, 353 (1967); Olmstead v. United States, 277 U.S. 438, 466 (1928) ("Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."), *abrogated by* Katz v. United States, 389 U.S. 347, 353 (1967); *ex parte* Jackson, 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.").

42. *See* Weaver, *supra* note 1, at 1150 ("While the concepts of 'trespassory invasions' and 'intrusions into constitutionally protected areas' may have made sense as applied to a house, a car or a briefcase, those concepts did not produce satisfactory results as advancing technology provided police investigators with ever more sophisticated surveillance technologies.").

43. *Olmstead*, 277 U.S. at 465 ("The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.").

44. *Id.*

45. *Goldman*, 316 U.S. at 135. The *Goldman* Court noted:

It took many decades before the Court started to come to grips with the reality of advancing technologies. The Court's landmark decision in *Katz v. United States* involved a man who the police suspected was involved in illegal bookmaking operations.[46] Police, anticipating that Katz would make a call from a particular phone booth, placed an electronic bug on the outside of the booth which allowed them to record Katz's incriminating statements and to use them against him in a subsequent prosecution.[47] Based on decisions like *Olmstead* and *Goldman*, the government argued that the police did not engage in a "search" when they bugged the phone booth since there was no "intrusion" into the phone booth and there was doubt about whether the booth would qualify as a "constitutionally protected area."[48] The electronic bug placed by the police had done nothing more than passively collect sounds that emanated from a public phone booth.[49]

The *Katz* Court disagreed with the government and held that police use of the listening device to overhear Katz's conversation constituted a "search" within the meaning of the Fourth Amendment.[50] In reaching that result, *Katz* departed from *Olmstead's* focus on whether there had been an intrusion into a constitutionally protected area[51] and held that a search occurs when governmental officials violate an individual's "expectation of privacy" (EOP).[52] In doing so, the Court purported to shift the focus under the Fourth Amendment from places to persons.[53] As the Court

> The suggested ground of distinction is that the Olmstead case dealt with the tapping of telephone wires, and the court adverted to the fact that, in using a telephone, the speaker projects his voice beyond the confines of his home or office and, therefore, assumes the risk that his message may be intercepted. It is urged that where, as in the present case, one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone's use of a delicate detector in the next room. We think, however, the distinction is too nice for practical application of the Constitutional guarantee and no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the Olmstead case.

Id.

46. Katz v. United States, 389 U.S. 347, 348 (1967).

47. *Id.* at 349.

48. *Id.* at 351.

49. *Id.* at 352.

50. *Id.* at 352–53.

51. *See id.* at 353 ("Thus, although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested.").

52. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

53. *See id.* at 351 (majority opinion) ("For the Fourth Amendment protects people, not places.").

stated: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[54] Justice Harlan, concurring, agreed with the Court that the focus should be on whether Katz had an EOP, but he argued that the expectation must be one that society was prepared to recognize as "reasonable."[55] Ultimately, Justice Harlan's requirement of "reasonableness" was integrated into the EOP test so that the final inquiry became whether the police have intruded upon an individual's "reasonable expectation of privacy" (REOP).[56]

Thus, after *Katz*, the Court used two tests to determine whether a "search" occurred under the Fourth Amendment. In addition to the REOP test, the Court continued to apply the old trespass test, which had been the governing test for many decades. For example, in the Court's later decision in *United States v. Jones*, the police attached a GPS tracking device to the undercarriage of the defendant's car.[57] Instead of deciding the case under the *Katz* test, the Court relied on the trespass test and invalidated the warrantless attachment of the device—and its use to monitor the defendant's car on public streets.[58]

Unfortunately, in the decades since the *Katz* test was announced in the 1960s, that test has not provided a workable or reliable test for evaluating Fourth Amendment claims.[59] The REOP test could have led to a

54. *Id.*

55. *See id.* at 361 (Harlan, J., concurring) ("As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

56. United States v. Jones, 565 U.S. 400, 406 (2012).

57. *Id.* at 403, 409.

58. *Id.* at 406–07. The *Jones* Court explained, "[F]or most of our history, the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates. *Katz* did not repudiate that understanding." *Id.* The Court continued, "*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id.* at 407 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)). The Court added, "What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted." *Id.* at 411 (emphasis in original). Finally, the Court concluded, "[W]e do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* (emphasis in original).

59. *See* Weaver, *supra* note 1, at 1225 ("The one thing that remains clear, some three decades after the *Katz* decision was rendered, is that the Court is still struggling to determine what the REOP test means, and there are continuing disputes between the Justices about how to apply the REOP test.").

significant expansion of the Fourth Amendment's scope of protection. That is exemplified by *Katz*. In that case, under the trespass test, there would have been no search. Yet, under the REOP test, the Court held that the Fourth Amendment protected an individual who made a phone call from a phone booth because the police intruded upon his REOP.[60] As a result, the REOP test expanded the Fourth Amendment's reach and provided Katz with protection against the government's seizure of the contents of his conversation.

Despite the promise of *Katz*, the REOP test has not been applied expansively in subsequent cases, and the Court has held that many activities that occur in public are not protected against government surveillance. For example, in *United States v. Knotts*, the Court held that the police may monitor a beeper (placed in a bottle of chloroform) to determine where Knotts was traveling.[61] Knotts argued that police use of the beeper constituted a "search" because the police obtained information from the beeper—in particular, the location of a remote cabin where Knotts was manufacturing drugs—that they could not have easily obtained otherwise.[62] Had they tried to follow Knotts, he may have noticed them and either tried to elude them or not gone to the cabin. However, the Court construed the situation very narrowly, concluding that an individual has a diminished expectation of privacy in an automobile, especially when he is traveling on a public highway, and concluded that the beeper simply allowed the police to monitor things that they could have observed from the highway with their own eyes.[63] In other words, had the police been on the road, they could have seen Knotts drive from the city to his remote cabin.[64] Although Knotts had an EOP in

60. *Katz*, 389 U.S. at 359.

61. United States v. Knotts, 460 U.S. 276, 285 (1983).

62. *Id.* at 277.

63. *See id.* at 281 ("'One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.'" (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion))). The *Knotts* Court explained:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen [a codefendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id. at 281–82.

64. *Id.* at 285. The *Knotts* Court went on:

> A police car following Petschen at a distance throughout his journey could have

the interior of his cabin (which was not infringed), he could not claim a REOP for his drive to the cabin: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[65]

Likewise, in *Florida v. Riley*, even though the Court had previously placed great emphasis on protecting the curtilage surrounding a home and a homeowner's EOP associated with the curtilage, the Court held that there was no search when the police flew a helicopter at low altitude over the defendant's property, thereby allowing them to peer down onto the property.[66] From the fly-over, the police were able to see that the defendant, Riley, was growing marijuana inside a greenhouse.[67] In the Court's view, Riley had no expectation of privacy because "[a]ny member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more."[68]

In *California v. Greenwood*, the Court upheld a police search of a defendant's garbage.[69] The Court emphasized that, while the trash was lying by the curb, it was accessible to "animals, children, scavengers, snoops, and other members of the public," and the trash had been placed by the curb "for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."[70] As a result, since the Greenwoods left their trash by the curb, "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,"[71] the Court concluded

---

> observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car. This fact, along with others, was used by the government in obtaining a search warrant which led to the discovery of the clandestine drug laboratory. But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.

Id.

65. *Id.* at 281. The Court added that "no such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway, nor to movements of objects such as the drum of chloroform outside the cabin in the 'open fields.'" *Id.* at 282 (quoting Hester v. United States, 265 U.S. 57, 59 (1924)).

66. Florida v. Riley, 488 U.S. 445, 449–52 (1989).

67. *Id.* at 448.

68. *Id.* at 451.

69. California v. Greenwood, 486 U.S. 35, 37 (1988).

70. *Id.* at 40.

71. *Id.* at 40–41 (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)) (internal quotations omitted).

that the Greenwoods could not have maintained a "reasonable expectation of privacy in the inculpatory items that they discarded."[72]

In general, the Court has only reined in governmental surveillance when the government has infringed on someone's home or private space. For example, in *United States v. Karo*, a case that is similar to *Knotts* in that the police used a beeper to track the defendant's movement to a remote location, the Court held that the use of a tracking beeper violated a homeowner's REOP because police continued to monitor the location of the beeper even after it was taken inside a dwelling and were thereby able to know when the bottle containing the beeper was moved to another location.[73] The Court reasoned that a search occurs when the government

> [S]urreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched.[74]

Thus, the beeper revealed "a critical fact about the interior of the premises" that the government "could not have obtained without a warrant."[75] By contrast, the beeper in *Knotts* "told the authorities nothing about the interior of Knotts' cabin."[76] The information obtained in *Knotts* was "voluntarily conveyed to anyone who wanted to look,"[77] whereas in *Karo*, "the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified."[78]

Likewise, in *Kyllo v. United States*, the Court concluded that the police conducted a search when they pointed an Agema Thermovision 210 thermal imager (essentially, a forward-looking infrared detection device) to scan Kyllo's home to detect and measure the heat that was being emitted.[79] They did so because they believed (correctly, as it turns out) that Kyllo was growing marijuana in his attic using special lighting

---

72. *Id.* at 41.

73. *See* United States v. Karo, 468 U.S. 705, 714 (1984) ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does.").

74. *Id.* at 715.

75. *Id.*

76. *Id.*; *see* United States v. Knotts, 460 U.S. 276, 285 (1983) ("[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

77. *Karo*, 468 U.S. at 715 (quoting *Knotts*, 460 U.S. at 281) (internal quotations omitted).

78. *Id.*

79. Kyllo v. United States, 533 U.S. 27, 29, 40 (2001).

(which gave off heat to simulate the effects of the sun) to help the plants grow.[80] Even though the heat might have been observed from the street (for example, by watching how quickly snow melted on Kyllo's house versus the surrounding houses, or by watching how quickly rain dried), the Court held that police use of the device constituted a search within the meaning of the Fourth Amendment because it could have revealed intimate details regarding the interior of the home (for instance, the time at which the lady of the house takes her bath).[81]

Perhaps the only real restraint on the use of surveillance technologies in public spaces was rendered in the case of *Carpenter v. United States*.[82] In *Carpenter*, the police used cell site sector information to ascertain a suspect's whereabouts at the time that certain robberies were committed.[83] Through the use of that data, they were able to ascertain that Carpenter was in close proximity to the robbery sites at the time of the robberies.[84] Thus, the police were able to pinpoint Carpenter's public movements using technology. One could argue that there was no search in this case. After all, the cell site data revealed nothing more than Carpenter's location, and the police were particularly interested in knowing about Carpenter's movements in public (similar to what they were seeking in *Knotts*).[85] Moreover, although the Court had previously suggested that information that individuals share with others (as they do when their cell phones reveal their locations to cell site towers) does not come with an EOP, the Court nonetheless held that Carpenter held a REOP in his cell site data.[86] The Court noted "society's expectation . . . that law enforcement agents and others would not—and indeed could not—secretly monitor and catalogue every movement of an individual's car for a very long period."[87] The Court concluded:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts . . . . [T]he time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[88]

The difficulty is that the Court's existing precedent imposes few other limits on the ability of the government to observe what happens in public

80. *Id.* at 29–30.
81. *Id.* at 34–35, 38–39.
82. *See* Carpenter v. United States, 138 S. Ct. 2206, 2206 (2018).
83. *Id.* at 2212.
84. *Id.* at 2213.
85. *Id.* at 2214–15; United States v. Knotts, 460 U.S. 276, 281 (1983).
86. *Carpenter*, 138 S. Ct. at 2217.
87. *Id.*
88. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

places, to capture that information with CCTV or drones, or to use FRT to help police analyze the images that they have captured. On the contrary, the Court has made it clear that there is a very low EOP for activities that take place in public. Several of the decisions discussed above illustrate that principle. *Riley* suggests that the government can fly over private property and peer down into the curtilage surrounding a home, and *Knotts* suggests that the government can monitor activities that take place in private places.[89] Thus, CCTV and drone monitoring of public places may be permissible. Moreover, the U.S. Supreme Court has not rendered any decisions regarding governmental use of FRT, so there is no indication that this technology will be prohibited. *Carpenter* is the only decision that suggests any limits on the government's ability to monitor what happens in public places.[90] However, in that case, the Court did nothing more than limit the government's ability to access historical cell site data.[91]

CONCLUSION

Modern technologies have enhanced the ability of governments to spy on the citizenry. Although there has been significant controversy regarding the use of surveillance technologies in countries like China, the problem exists in most Western countries as well.[92] In the United States, the government is increasingly using technologies like drones, CCTV, and FRT to spy on people. While these surveillance technologies can serve many important and benign governmental purposes (for example, to locate lost hikers or help ascertain the level of damage in a disaster), as well as to apprehend criminal perpetrators, there is a fear that new technologies can create an Orwellian level of surveillance for everything that occurs outside the home.

Some state and local governments have placed significant limitations on the ability of private individuals and companies to use surveillance devices. For example, Illinois' Biometric Information Privacy Act (BIPA), sets forth various notice requirements for private entities that collect "biometric identifiers" and "biometric information."[93] BIPA also places restrictions on the ability of private employers to collect biometric

89. Florida v. Riley, 488 U.S. 445, 449–52 (1989); *Knotts*, 460 U.S. at 284–85.

90. *Compare Carpenter*, 138 S. Ct. at 2220–21 (holding that the warrantless access of a person's cell phone location history violated the Fourth Amendment), *with Knotts*, 460 U.S. at 281–85 (holding that the use of a radio transmitter in a suspect's car was not a search or seizure under the Fourth Amendment), *and Riley*, 488 U.S. at 451–52 (holding that police do not need a warrant to observe a home's curtilage from navigable airspace).

91. *Carpenter*, 138 S. Ct. at 2223.

92. *See generally Mass Surveillance in China*, HUM. RTS. WATCH (Oct. 10, 2022), https://www.hrw.org/tag/mass-surveillance-china# [https://perma.cc/DS9D-JW6C] (listing news reports describing various instances of mass surveillance in China).

93. 740 ILL. COMP. STAT. § 14/15(b) (2008).

information regarding their employees.[94] Likewise, the California Consumer Privacy Act (CCPA), places limitations on the ability of businesses to collect information, including biometric data.[95] But even in the private arena, the protections are far from comprehensive. For example, the Brookings Institution estimates that private actors will soon have as many drones as the government.[96] One potential restriction is that some companies have indicated that they will limit their sale, research, and development of FRT.[97]

If governmental use of technology like CCTV, drones, and FRT is going to be controlled and limited, Congress will have to exert control through legislation. It is unlikely that courts will do so through their decisions. The U.S. Supreme Court's search-related jurisprudence has evolved very slowly. In its early decisions regarding technology, the Court was relatively unwilling to rein in governmental use of advanced technologies.[98] *Katz* was the first decision to explicitly acknowledge and attempt to deal with that problem, and it took the Court nearly half-a-century to get to that point. However, as noted, the *Katz* test has proven difficult to apply and has not provided consistent or reliable protections to the citizenry. In more recent decisions, such as *Karo*, *Kyllo*, and *Carpenter*, the Court has expanded Fourth Amendment protections on a piecemeal basis, and perhaps the Court will expand its jurisprudence even further in an effort to deal with the implications of technologies like CCTV, FRT, and drones. But the Court has struggled with the problem of advancing technology for nearly a century, and jurisprudential changes have come slowly and haltingly.

It seems unlikely that Congress will deal with the problem either. Congress has been stuck in gridlock for years, and it matters not which party is in power. So, change may have to come at the state and local levels, but those changes will vary by state and will inevitably be piecemeal. Just as some jurisdictions have sought to limit the use of FRT in police investigations, they have the power to impose limitations on governmental use of drones and CCTV. Of course, there is a push-pull

94. *Id.* § 14/15(b)(3).

95. CAL. CIV. CODE § 1798.100(b) (West 2022).

96. Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, BROOKINGS INST. (Sept. 4, 2014), https://www.brookings.edu/research/civilian-drones-privacy-and-the-federal-state-balance/ [https://perma.cc/UW4Z-2BGS].

97. *See, e.g.*, Jay Peters, *IBM Will No Longer Offer, Develop, or Research Facial Recognition Technology*, VERGE (June 8, 2020, 8:49 PM), https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software [https://perma.cc/2XSH-Q75L] (explaining that IBM is no longer offering, developing, or researching FRT).

98. *See* Weaver, *supra* note 1, at 1137 ("[E]arly United States Supreme Court decisions dealing with technology and the Fourth Amendment tended to adhere to more traditional views of the Fourth Amendment and were virtually unresponsive (except in the dissents) to the problems presented by new technologies.").

here. The public has a strong interest in controlling crime and in protecting itself against criminals, and drones, FRT, and CCTV help the police achieve that objective. The trick for state and local governments is to find an acceptable balance between crime control and privacy protections. Undoubtedly, these are issues that society will debate for many years to come.

BACKGROUND AND IMPLICATIONS OF CHINA'S E-CNY*

*Jiaying Jiang** and *Karman Lucero***

Abstract

The People's Republic of China is a leading experimenter in central bank digital currencies (CBDCs). This Article explores the current background, deployment, features, potential impacts, challenges, and legal concerns of China's CBDC: the electronic yuan, or E-CNY. This Article explains the potential significance of what is known and not known about E-CNY with a particular focus on how E-CNY might fit into existing legal and economic systems, both within China and internationally. On the surface, E-CNY looks transformative. When you dig a little deeper, however, most of the potential changes or transformations turn on broader institutional, political, and legal changes that, so far, have not accompanied the deployment of E-CNY. Without those broader changes, the impact of E-CNY will likely remain limited, and E-CNY may not be able to achieve its policy goals.

* If you would like to contact the Article's authors, please email them at jiang@law.ufl.edu and karman.lucero@yale.edu respectively. The Authors are grateful to participants at the workshops of Information Law Institute at NYU Law School and Paul Tsai China Center at Yale Law School for their generous comments and suggestions. The Authors also appreciate many conversations with experts from People's Bank of China and the Federal Reserve.

** Assistant Professor of Law, University of Florida Levin College of Law.

*** Fellow, Paul Tsai China Center, Yale Law School.

INTRODUCTION

China's central bank digital currency (CBDC), the electronic yuan or E-CNY, is the digital version of fiat currency issued by the China's central bank—the People's Bank of China (PBOC)—operated by authorized financial institutions and tech companies. China is one of the first major economies to issue a CBDC that could have global implications. Many forms of CBDC are possible, such as a wholesale CBDC or a retail CBDC. A wholesale CBDC is used between financial institutions to settle trades in financial markets; a retail CBDC is used by individuals to pay businesses, shops or each other (like cash).[1] Various design choices are available for the development of a CBDC—examples include direct, two-tier, or hybrid models, with token or account access models.[2] This list of categories in not exhaustive; a great deal of complexity underlies the choices in access, intermediation, institutional roles, and data retention in CBDC design that have different implications for the technical, institutional, or social infrastructure of how a CBDC is

1. *BIS Innovation Hub Work on Central Bank Digital Currency (CBDC)*, BIS, https://www.bis.org/about/bisih/topics/cbdc.htm [https://perma.cc/D9UL-NTHJ] (last visited May 18, 2023).

2. *Project Hamilton Phase 1 Executive Summary*, FED. RSRV. BANK BOSTON (Feb. 3, 2022), https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx [https://perma.cc/W96E-PXC3].

designed, implemented, and used.[3] Design choices are complex, multilayered, and multifaceted.[4]

This Article introduces the development, initial deployments, and implications of China's E-CNY. It analyzes China's motivations for issuing a CBDC and explores the potential impacts and challenges of E-CNY. Currently, it appears that China's pioneering the creation of E-CNY is driven mainly by the hopes of advancing domestic policy goals, such as reducing costs, combatting money laundering, improving financial inclusion, transforming to a cashless economy, responding to the duopoly of the mobile payment market, and generally increasing government insight into and capacity to intervene in the Chinese economy.[5] Externally, China's experimentation with E-CNY has been sped up by Diem[6] due to the threat that Diem could potentially undermine the monetary sovereignty of the yuan (RMB). It is also arguable that China has an agenda to use E-CNY to circumvent U.S. and international sanctions[7] and even to internationalize the RMB, though whether it could succeed in doing so is debatable.

E-CNY may also impact China's domestic financial system as well as the global financial system. First, E-CNY may reduce transaction costs and increase efficiency by shifting to a free digital currency for individuals and businesses. Second, E-CNY may impact the payment and mobile payment duopoly held by Alibaba and Tencent.[8] Third, E-CNY could impact monetary and economic policy by, in theory, offering more affordances and greater oversight over the currency. Fourth, E-CNY may also impact the relationship between Belt and Road Initiative (BRI)[9]

---

3. *Id.*

4. *Id.*

5. *See* Andrew Urquhart, *Should Central Banks Develop Their Own Digital Currencies?*, ECONOMICS OBSERVATORY (Jan. 11, 2022), https://www.economicsobservatory.com/should-central-banks-develop-their-own-digital-currencies [https://perma.cc/2HN2-RRXN]; *see also infra* note 8.

6. Diem "is built on blockchain technology to enable the open, instant, and low-cost movement of money. People will be able to send, receive, and spend their money, enabling universal access to financial services." *Vision*, DIEM, https://www.diem.com/en-us/vision/#how_it_works [https://perma.cc/3BNV-EVD5] (last visited May 18, 2023); *see* Scott Jeffries, *Diem Coin: What You Need to Know*, GOBANKINGRATES (Oct. 31, 2022), https://www.gobankingrates.com/investing/crypto/what-is-diem-coin/ [https://perma.cc/B474-EGY4].

7. Aditi Kumar & Eric Rosenbach, *Could China's Digital Currency Unseat the Dollar?*, FOREIGN AFFS. (May 20, 2020), https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar [https://perma.cc/K32A-9FHX].

8. Alibaba and Tencent are two leading multinational Internet and technology companies with headquarters in China.

9. Andrew Chatzky & James McBride, *China's Massive Belt and Road Initiative*, COUNCIL ON FOREIGN AFFS. (Jan. 28, 2020), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative [https://perma.cc/4MB3-SN64].

countries and China since countries that have increasingly interconnected relationships with China, but do not have a strong and established domestic financial infrastructure, may be drawn to mobile payment systems. Last, one possible goal of E-CNY may be to impact international settlements by creating circumstances where international governments (including China), businesses, and other actors are more able to use a Chinese-backed SWIFT[10] alternative.

Besides E-CNY's impact on financial systems, E-CNY raises many concerns. For one, there is the uncertainty which state and non-state actors have access to information generated by and related to the deployment and use of E-CNY. Similarly, there are questions concerning how state agencies will guarantee due process rights regarding access to and use of data. Another challenge is how state agencies and intermediaries will protect users' privacy. Last, the lack of technological transparency and cybersecurity threats present further challenges.

This report proceeds as follows. Part I discusses the development of E-CNY, including known technical features, institutional framework, and E-CNY's intended role in China's domestic monetary system. Part II explores China's motivations for developing and deploying E-CNY, most of which are focused on domestic concerns, though there are important international dynamics as well. Part III outlines several potential impacts of E-CNY, including domestic impacts on online payment platforms such as Alipay and WeChat Pay and commercial banks as well as impacts on international settlements and BRI countries. Part IV addresses key challenges and concerns around E-CNY, particularly as it pertains to information access and sharing, privacy protections, due process rights, cybersecurity threats, and intermediaries. Part V examines E-CNY in the context of additional legal paradigms, including taxation, antitrust, anti-money laundering, and fraud prevention.

I. THE DEFINITION, DEVELOPMENT, AND KEY FEATURES OF E-CNY

The exact technical and institutional parameters of E-CNY are not public; any "definition" of E-CNY therefore must be based on statements by government officials about E-CNY and observations about how E-CNY is used in practice. Some sources have described E-CNY as "based on broad accounts, loosely coupled with bank accounts and has its system of value."[11] However, E-CNY is fundamentally different from existing mobile payment systems and cryptocurrencies. That said, China has been

10. SWIFT is a network that banks use worldwide to securely send and receive messages for transferring funds between accounts.

11. WORKING GRP. ON E-CNY RSCH. & DEV. OF THE PEOPLE'S BANK OF CHINA, PROGRESS OF RESEARCH & DEVELOPMENT OF E-CNY IN CHINA 6 (2021) [hereinafter WORKING GRP.], http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf [https://perma.cc/Q9V4-FTL3].

one of the main pioneers in exploring the implications that a CBDC may bring. China has conducted pilots in at least ten regions, as well as during the 2022 Beijing Winter Olympics, over the past eight years.[12] From these studies, others have examined some key features of E-CNY, including its operating structure, institutional background, issuance and redemption process, technical designs, and financial characteristics.

A. *Definition*

The PBOC defines E-CNY as the digital version of China's fiat currency.[13] E-CNY has all the basic functions of money, i.e., it is a unit of account, medium of exchange, and store of value.[14] As with the physical form of RMB, E-CNY is legal tender.[15] The PBOC also defines E-CNY as mainly a substitute for cash in circulation (M0) that will coexist with physical RMB.[16]

E-CNY is different from existing mobile payment systems such as Alipay and WeChat Pay. First, E-CNY is legal tender, but Alipay and WeChat Pay are payment tools—they are intermediaries that still have to operate through commercial banks, and they do not issue their own currency.[17] Although Alipay and WeChat Pay have been widely used in China, one can still legally refuse to accept payment made via WeChat Pay or Alipay but cannot legally refuse to accept E-CNY because E-CNY, just like cash, is a legal tender backed by the state. Second, technological and operational differences exist between them. For instance, E-CNY allows for offline transactions while Alipay and WeChat Pay heavily rely on an Internet connection to process transactions.[18] E-CNY does not need to be associated with a bank account to make payments while Alipay and WeChat Pay do.[19] These differences are further addressed in the section about E-CNY features.

E-CNY is also fundamentally different from cryptocurrencies such as Bitcoin and Ethereum. E-CNY is a fiat currency issued and governed by the central bank. The technical details of how it works are not public, but PBOC officials have stated that it does not run on a blockchain. By contrast, cryptocurrencies are a type of privately-issued money running

12. *Id.*
13. *Id.* at 3.
14. *Id.*
15. *Id.*
16. *Id.* at 4.
17. Zhang Xuan (张宣) & Wang Tuo (王拓), Shuzi Huobi, he Zhifubao, Weixin Zhifu Youshenme Qubie? (数字货币，和支付宝、微信支付有什么区别?) [What Is the Difference Between Digital Currency, Alipay, and WeChat Pay?], Xinhua Ribao (新华日报交汇点) [XINHUA DAILY INTERSECTION] (Aug. 27, 2020, 9:02 AM), http://blockchain.people.com.cn/n1/2020/0827/c417685-31838908.html [https://perma.cc/CEV9-DL2K].
18. *Id.*
19. *Id.*

either on a blockchain, which is produced by solving complex mathematical proofs and governed by disparate online communities instead of a centralized body, or some other kind of privately run, generally centralized, clearing system.[20] E-CNY is a legal tender, but cryptocurrencies are not; their worth is not backed by a state directly and one can reject cryptocurrencies as a form of payment.[21] The value of E-CNY, like existing fiat currency, is influenced by policymakers and the vicissitudes of micro and macroeconomics but ultimately guaranteed, and to an extent controlled, by the state, whereas the value of cryptocurrencies is determined by the market, the expectations of the network, and adverse policy making,[22] and thus is highly volatile.

B. *The Timeline of E-CNY Development*

China is a pioneer in exploring CBDC. The early-stage research started in 2014 when a group of experts started to examine the feasibility of establishing a CBDC.[23] In 2016, the PBOC held a seminar on CBDC in Beijing and recognized the positive practical significance and far-reaching historical impacts of CBDC.[24]

A series of discussions then focused on the design of E-CNY. In an interview with Caixin, Zhou Xiaochuan, then Governor of the PBOC, stated that digital currency could be account based or non-account based.[25] Fan Yifei, Deputy Governor of the PBOC, suggested that E-CNY should be within the scope of money in circulation and he discussed two possible operating frameworks of E-CNY: a one-tier (in which users have accounts directly with the PBOC) and two-tier (in which commercial banks and other entities serve as the main intermediaries) distribution model.[26] Yao Qian, then Vice Director-General of the

20. *Id.*; Anshu Siripurapu, *Cryptocurrencies, Digital Dollars, and the Future of Money*, COUNCIL ON FOREIGN RELS. (Sept. 24, 2022, 12:55 PM), https://www.cfr.org/backgrounder/cryptocurrencies-digital-dollars-and-future-money [https://perma.cc/RGN6-ZZZE].

21. Lorand Laskai, *Let's Start with What China's Digital Currency Is Not*, DIGICHINA (Mar. 8, 2022), https://digichina.stanford.edu/work/lets-start-with-what-chinas-digital-currency-is-not/ [https://perma.cc/5VTX-H464].

22. Alun John et al., *China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling*, REUTERS (Sept. 24, 2021, 1:49 PM), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/ [https://perma.cc/J83R-QK48].

23. WORKING GRP., *supra* note 11, at 1.

24. *Id.*

25. Wang Shuo (王烁) et al., Zhuanfang Zhou Xiaochuan (专访周小川) [Interview with Zhou Xiaochuan], Caixin Xin Zhoukan (財新周刊) [CAIXIN WEEKLY] (Feb. 15, 2016), https://weekly.caixin.com/2016-02-12/100908570.html [https://perma.cc/H2RA-WW9W].

26. Fan Yifei (范一飞), Fan Tifei: Shuzi Renminbi M0 Dingwei de Zhengce Yiyi Fenxi (范一飞：數字人民幣 M0 定位的政策意義分析) [Fan Yifei: Analysis of the Policy Meaning of the Positioning of Digital RMB M0], Zhongguo Jinrong Xinwen Wang (中國金融新聞網)

Technology Department of the PBOC, proposed the concepts of an account-based and wallet-based E-CNY, and he further put forward a two-tier model of E-CNY distribution.[27]

In 2016, the PBOC formally established the Digital Currency Research Institute with Yao Qian as its first director.[28] In the same year, with the approval of the State Council, the PBOC formally began working on E-CNY. In January 2018, Fan Yifei confirmed the benefits of the two-tier distribution model and emphasized that E-CNY should be released in a loosely coupled manner and adhere to centralized (not distributed) governance.[29]

In May 2019, Mu Changchun, then Deputy Director of the Payment and Settlement Department of the PBOC, further elaborated the two-tier distribution model of E-CNY—to ensure that the central bank does not overissue E-CNY, commercial banks should pay 100% of the reserve to the central bank.[30] E-CNY is still a central bank liability guaranteed by the central bank's credit, and, like other central banks, it has unlimited legal indemnity.[31] Mu Changchun also emphasized that E-CNY has intentionally remained technologically neutral, meaning the PBOC does not have a fixed technological architecture for the E-CNY.[32] A fixed architecture would likely only limit potential business cases in the future.[33] The PBOC did not adopt blockchain but did borrow associated

---

[CHINA FIN. NEWS NETWORK] (Sept. 9, 2020), https://www.yicai.com/news/100770937.html [https://perma.cc/NZB3-V8BJ]; Robert Greene, *What Will Be the Impact of China's State-Sponsored Digital Currency?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 1, 2021), https://carnegieendowment.org/2021/07/01/what-will-be-impact-of-china-s-state-sponsored-digital-currency-pub-84868#:~:text [https://perma.cc/E8R7-ML9A].

27. Yao Qian Fenxiang Yanghang Fading Shuzi Huobi "Shuang Ceng Jiagou": Jiyu Zhanghu he Qianbao de Fen Ceng (姚謙分享央行法定數字貨幣"雙層架構"：基於賬戶和錢包的分層) [Yao Qian Shared the "Double-Layer Architecture" of the Central Bank's Legal Digital Currency: Based on the Stratification of Accounts and Wallets], Yodong Zhifu Wangluo (移動支付網絡) [MOBILE PAYMENT NETWORK] (Aug. 6, 2018, 10:14 AM), https://www.mpaypass.com.cn/news/201808/06103010.html [https://perma.cc/2UXK-2BU8].

28. WORKING GRP., *supra* note 11.

29. Yanghang Shuzi Huobi Yanjiu Suo: Zhashi Kaizhan Shuzi Renminbi Yanfa Shidian Gongzuo (央行數字貨幣研究所：紮實開展數字人民幣研發試點工作) [Central Bank Digital Currency Research Institute: Solidly Carry Out Digital RMB Research and Development Pilot Work], Xinlang Caijing (新浪財經) [SINA FIN.] (Oct. 12, 2022, 4:02 PM), https://finance.sina.com.cn/money/bank/bank_hydt/2022-10-12/doc-imqqsmrp2326411.shtml [https://perma.cc/G55L-CR88].

30. Qukuailian Xingqiu (区块链星球), Yanghang Shuzi Huobi Sheji Bingcheng Zhongxin Hua Guanli Moshi (央行數字貨幣設計秉承中心化管理模式) [The Central Bank's Digital Currency Design Adheres to the Centralized Management Model], Qu Kuai Lian Xingqiu (區塊鏈星球) [BLOCKCHAIN PLANET] (Aug. 16, 2019, 6:08 AM), https://www.qklplanet.io/2019/08/16/135128/ [https://perma.cc/BAL5-YQUA].

31. WORKING GRP., *supra* note 11, at 3.

32. *Id.* at 10–11.

33. *Id.* at 10.

concepts such as peer-to-peer payment and traceability.[34] The PBOC is maintaining a flexible position so that it can adapt to different architectures and remain compatible with technologies adopted by commercial banks. Of course, it is impossible to critically assess this claim as the E-CNY's underlying architecture, however flexible or malleable, is not public.

Later in November 2019, Fan Yifei confirmed that the major work of E-CNY, such as the high-level design, standard formulation, and functional research and testing, had been completed.[35] The next step would be to select pilot areas to test and optimize E-CNY, following the principles of stability, safety, and controllability.[36] In April 2020, China launched trials of E-CNY in four cities: Shenzhen, Suzhou, Chengdu, and Xiong'an.[37] In May, the PBOC was in talks with private companies to expand its test run. Major firms such as China's largest ride-hailing company Didi Chuxing (China's Uber or Lyft), and food delivery giant Meituan Dianping were among the candidates to roll out E-CNY on a large scale through their wide-reaching platforms.[38] As a part of the trials, in October 2020, the PBOC distributed ten million E-CNY (1.4 million in U.S. dollars) in digital "red pockets" to 50,000 Shenzhen residents.[39]

---

34. *Id.*

35. *Digital Currency Research Institute of the People's Bank of China: The Online DC/EP Information Is the Test Content, Which Does Not Mean That the Digital RMB Is Officially Issued*, PEOPLE'S BANK CHINA: SHENZHEN CENT. SUB-BRANCH (Apr. 24, 2020, 3:26 PM), http://shenzhen.pbc.gov.cn/shenzhen/122787/4013185/index.html [https://perma.cc/GC4W-CJMP].

36. *Id.*

37. Chen Xin (陳欣), Shuzi Renmibi Laile! Chengdu, Suzhou, Xiong'an Xinqu Deng di Shuaixian Kaizhan Shidian (數字人民幣來了！成都、蘇州、雄安新區等地率先開展試點) [Here Comes the Digital RMB! Chengdu, Suzhou, Xiong'an New Area and Other Places Took the Lead in Carrying Out Pilot], Nanfang Dushi Bao (南方都市報) [S. METROPOLIS DAILY] (Aug. 14, 2020), https://m.mp.oeeee.com/a/BAAFRD000020200814354576.html [https://perma.cc/VR7P-YNV6].

38. Didi yu Yanghang Shuzi Huobi Yanjiu Suo Dacheng Zhanlue Hezuo, Tansuo Zhihui Chuxing Changjing Yingyong (滴滴與央行數字貨幣研究所達成戰略合作，探索智慧出行場景應用) [Didi and the Central Bank's Digital Currency Research Institute Reached a Strategic Cooperation to Explore the Application of Smart Travel Scenarios], Lutou She (路透社) [REUTERS] (July 8, 2020), https://www.reuters.com/article/didi-pboc-0708-wedn-idCNKBS2491BT [https://perma.cc/X4EZ-D353]; Si Da Xing Nei Ce Da Fanwei Kaizhan. Yanghang Shuzi Huobi Shenme Shihou Tuichu? (四大行內測大範圍開展。央行數字貨幣什麼時候推出?) [The Internal Test of the Four Major Banks Is Carried Out on a Large Scale. When Will the Central Bank Digital Currency Be Launched?], Xiao Tu (小兔) [BABIT] (Aug. 6, 2020, 10:46 PM), https://www.8btc.com/article/632339 [https://perma.cc/PL3K-7LMB].

39. Shuzi Renminbi Zhen de Yao Laile! Shenzhen Lianshou Yanghang Fafang 1000 Wan ge "Shuzi Hongbao" (數字人民幣真的要來了！深圳聯手央行發放 1000 萬個"數字紅包") [The Digital RMB Is Really Coming! Shenzhen Teamed Up With the Central Bank to Distribute 10 Million "Digital Red Envelopes"], Xinlang Caijing (新浪財經) [SINA FIN.] (Oct. 9, 2020, 12:30 AM), https://finance.sina.com.cn/blockchain/coin/2020-10-09/doc-iivhvpwz0960147.shtml [https://perma.cc/R5YY-QA5R].

Residents could spend it at over 3,300 restaurants and retail stores.[40] The week-long trial ended with 8.8 million E-CNY (1.3 million in U.S. dollars) being spent in over 62,000 transactions.[41]

"Starting from November 2020, Shanghai, Hainan, Changsha, Xi'an, Qingdao, Dalian joined the pilot."[42] According to data published by the PBOC,

> As of June 30, 2021, E-CNY has been applied in over 1.32 million use cases, covering utility payments, catering services, transportation, shopping, and government services. More than 20.87 million personal wallets and over 3.51 million corporate wallets have been opened, with a transaction volume totaling 70.75 million and a transaction value approximating RMB 34.5 billion.[43]

During the 2022 Winter Olympics, China tested the appeal of E-CNY by providing E-CNY's mobile application and payment cards or wristbands to visiting foreigners.[44] The Olympic Games provided an international center stage to test the capabilities of the E-CNY.[45] In fact, top officials from the PBOC reported that E-CNY was being used to make two million yuan payments a day (or more).[46]

These pilot programs tested the business and technological designs as well as whether the E-CNY system is stable, the product is user-friendly, and the scenario is applicable.[47] China has continued these pilot programs at a large scale with more corporate and individual participants, and more use cases throughout 2022. It is still unclear if China will ever officially launch the E-CNY nationally and internationally and not just as pilot programs.

---

40. *Id.*

41. Cissy Zhao, *China Digital Currency: Shenzhen Consumers Spend 8.8 Million Yuan in Largest Trial of Digital Yuan*, S. CHINA MORNING POST (Oct. 20, 2020, 5:00 PM), https://www.scmp.com/economy/china-economy/article/3106265/china-digital-currency-shen zhen-consumers-spend-88-million [https://perma.cc/VL25-ZN6C].

42. WORKING GRP., *supra* note 11, at 13.

43. *Id.*

44. Marc Jones, *Over $315,000 in Digital Yuan Used Every Day at Olympics, PBOC Official Says*, REUTERS (Feb. 16, 2022, 3:16 AM), https://www.reuters.com/technology/around-300-mln-digital-yuan-used-every-day-olympics-pboc-official-says-2022-02-15/ [https://perma.cc/4ADG-5C3S].

45. *Id.*

46. *Id.*

47. *Id.*; *PBC Holds Meeting on Pilot Program of E-CNY R&D*, PEOPLE'S BANK CHINA, http://www.pbc.gov.cn/en/3688110/3688172/4437084/4529973/index.html [https://perma.cc/GBQ9-ZP92] (last updated Apr. 2, 2022); *Chinese Embrace Digital Yuan as China Further Promotes Pilot Program-Xinhua*, ENG. NEWS (May 14, 2022, 7:52 PM), https://english.news.cn/20220514/18c29e06fb264f00a6d85672104d2c31/c.html [https://perma.cc/AHL6-X2JG].

C. *Key Features of E-CNY*

This section addresses some key features of E-CNY, including its operating structure, institutional background, issuance and redemption process, technical designs, and financial characteristics. At this moment, the only available source from the PBOC is the report published in July 2021. Without more details and specific access to technical details, there are many unanswered questions regarding how E-CNY works at a technical and institutional level. As of the beginning of 2023, E-CNY remains "little used," according to former PBOC official Xie Ping.[48]

1. E-CNY and the Existing Monetary System

E-CNY is designed to replace cash, or "M0," which refers to physical currency in circulation and is the most liquid form of money.[49] M1 includes M0 plus money held in checking accounts in banks (including in digital form).[50] M2 includes M1 plus money held in savings accounts and certificates of deposits (CDs).[51] Similar to traditional cash, E-CNY holders will not receive any interest from the central bank for having E-CNY;[52] E-CNY will only earn interest if it is stored in an interest-bearing account in a bank. At this stage, E-CNY is not designed for M1 or M2 replacement because the PBOC believes that significant parts of M1 and M2 have already been digitized. In other words, commercial banks, online payment platforms, and other entities that store money in bank accounts already do so in digital form. Besides, the digitalization of all

48. Xie Ping (谢平)，Xie Ping: Qian xi Shuzi Renminbi Weihe Xian Wei Renzhi (謝平：淺析數字人民幣為何鮮為人知) [Xie Ping: Preliminary Analysis of Why *Digital Yuan Is Little Used*]，Shuzi Jinrong Zichan Yanjiu Zhongxin (數字金融資產研究中心) [DIGITAL FIN. ASSET RSCH. CTR.] (Dec. 29, 2022, 5:46 AM), https://mp.weixin.qq.com/s/WAY6TUSlv4jMVJY2SfH0Iw [https://perma.cc/SMW2-KMGV]; Jason Xue et al., *Former PBOC Official Says China's Digital Yuan Is Little Used – Caixin*, REUTERS (Dec. 29, 2022, 3:54 AM), https://www.reuters.com/technology/former-pboc-official-says-chinas-digital-yuan-is-little-used-caixin-2022-12-29/ [https://perma.cc/3XXB-LEDS].

49. Jiemeng Yang & Guangyou Zhou, *A Study on the Influence Mechanism of CBDC on Monetary Policy: An Analysis Based on E-CNY*, PLOS ONE (July 8, 2022), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0268471 [https://perma.cc/8U3N-JLHB].

50. Evan Tarver, *Money Aggregates: Definition and Examples*, INVESTOPEDIA (Mar. 9, 2021), https://www.investopedia.com/terms/m/monetary-aggregates.asp [https://perma.cc/66CQ-U63B].

51. Pete Rathburn, *M2 Definition and Meaning in the Money Supply*, INVESTOPEDIA (Dec. 18, 2022), https://www.investopedia.com/terms/m/m2.asp#:~:text=M2%20is%20the%20U.S.%20Federal%20Reserve%27s%20estimate%20of,time%20deposits%20above%20%24100%2C000%20are%20omitted%20from%20M2 [https://perma.cc/FX8D-BY6M].

52. Robert Greene, *What Will Be the Impact of China's State-Sponsored Digital Currency?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 1, 2021), https://carnegieendowment.org/2021/07/01/what-will-be-impact-of-china-s-state-sponsored-digital-currency-pub-84868 [https://perma.cc/T37J-7XTL].

parts of M1 and M2 is complex and likely outside of the current capability of the E-CNY design.

Some government actors may have broader ambitions than just positioning E-CNY as a replacement for M0 only. Mu Changchu, for example, describes the value of E-CNY in creating and utilizing smart contracts.[53] The PBOC has fully recognized this concern and has thus used the term "at this stage" cautiously.[54] In the future, once the PBOC gains more experience with E-CNY, the scope and goals of its use could change. As Yao Qian suggests, positioning E-CNY as an M0 replacement at this stage not only measures risk but is also forward-looking.[55] At this stage, to ensure that E-CNY will not be over-issued, commercial banks are required to maintain a one-hundred percent reserve ratio.[56] As a result, E-CNY should not have any derivative deposits or money multipliers. Going forward, E-CNY might be changing the relationship between the PBOC and other entities in the financial infrastructure, such as commercial banks and online payment platforms.

2. Two-Tier System for Issuance and Redemptions

The distribution of E-CNY will follow the traditional currency distribution model—a two-tier system with two distinct layers of functionality. On the first layer, the PBOC will issue and redeem E-CNY to commercial banks and other authorized entities, such as existing mobile payment platforms (Alipay and WeChat Pay) and telecommunication companies. On the second layer, commercial banks and other authorized entities will distribute E-CNY to the general public.

As with existing fiat currency, the PBOC maintains the sole authority to issue E-CNY, which gives E-CNY the ultimate status of being legal tender. For the general public, commercial banks and other authorized entities are still the major way to receive E-CNY. E-CNY users can

53. Mu Changchun, *Smart Contract and E-CNY*, CF40 (Sept. 19, 2022), http://www.cf40.com/en/news_detail/12852.html?_isa=1 [https://perma.cc/U3XK-KHY9].

54. *See* Martin Chorzempa, China's Central Bank-Backed Digital Currency Is the Anti-Bitcoin, PIIE (Jan. 31, 2018, 5:00 AM), https://www.piie.com/blogs/china-economic-watch/chinas-central-bank-backed-digital-currency-anti-bitcoin [https://perma.cc/2PWS-UZAH] ("One section of the [PBOC] statement explores ways to automatically implement 'smart' contracts with computer code. While the potential to add new social functions is viewed positively, including automating tax paying and blocking terrorism financing, smart contracts will not be a part of the digital currency, at least at this stage.").

55. Lian Xin (連心), Yanghang Fu Xing Zhang, Fan Yifei Chen Shuzi Renminbi Zhuyao Dingwei yu M0. Zhuanjia Jiedu [Yanghang] Jijiang Faxing CBCC (央行副行长范一飞称数字人民币主要定位于 M0 专家解读或迈向 CBCC) [Fan Yifei, Deputy Governor of the Central Bank, Said that Digital RMB Is Mainly Positioned in M0. Experts Interpret [the Central Bank] is About to Issue a CBCC], Xinlang Caijing (新浪財經) [SINA FIN.] (Sept. 15, 2020, 9:49 AM), https://finance.sina.cn/blockchain/2020-09-15/detail-iivhvpwy6781057.d.html [https://perma.cc/3FUP-HZ35].

56. *Id.*

download a digital wallet to store E-CNY,[57] similar to using a physical wallet to hold cash. This model avoids disintermediating the financial system by leaving user interactions to commercial banks or other entities, and it also reduces the responsibilities and risk exposure of the central bank. While specific digital wallets are required to use E-CNY, at this point, it does not appear that the PBOC is requiring individuals or businesses to download and utilize particular digital wallets, though the PBOC likely has the authority to make such a requirement, even if there would be logistical challenges to enforcing such a requirement.

D. *"Loosely Coupled" Design with Offline Transactions and Manageable Anonymity*

To make E-CNY function more like cash, the PBOC invented a system called "loosely coupled account links" (松耦合), whereby transactions can happen between two E-CNY wallets.[58] Unlike traditional payment systems, in which transactions can only happen between two bank accounts, an E-CNY wallet does not need to be associated with a bank account to make transactions.[59] With an E-CNY wallet on each smartphone, users can transfer money by closely shaking two phones.[60] Transactions can be made offline, which functions more like cash. Therefore, using E-CNY requires a digital wallet. A digital wallet uses security chips and other technologies to enable the functions of E-CNY.[61] Thus, it may be supported by IC cards,[62] mobile phones, wearable objects, and Internet of Things devices.[63]

Because of its "loosely coupled" nature, E-CNY can achieve "manageable anonymity" (可控匿名) because many transaction details can be eliminated when transactions are made offline and between two wallets instead of going through the online banking system. For now, "manageable anonymity" refers to the fact that individuals and their transactions are not anonymous from the PBOC and authorized entities with whom it shares information but can be anonymous vis-à-vis third

57. Andrew Galbraith & Samuel Shen, *China Central Bank Launches Digital Yuan Wallet Apps for Android, iOS*, REUTERS (Jan. 4, 2022), https://www.reuters.com/markets/currencies/china-cbank-launches-digital-yuan-wallet-apps-android-ios-2022-01-04/ [https://perma.cc/6JV8-QWT8].

58. WORKING GRP., *supra* note 11, at 3.

59. *Id.*

60. *Id.* at 14.

61. *Id.* at 9.

62. Integrated circuit (IC) cards use an IC chip to store information on the card instead of using magnetic tape like a traditional credit card.

63. WORKING GRP., *supra* note 11, at 9.

party intermediaries, such as commercial banks and internet platforms.[64] Indeed, E-CNY claims "to meet the public demand for anonymous small value payment services based on the risk features and information processing logic of current electronic payment system[s]."[65] However, the anonymity is still manageable because a wallet can be deactivated, and a transaction can be reversed if suspicious or illegal activities are identified. The manageability comes from E-CNY's centralized governance system where the PBOC has access to all transaction data, unlike blockchain, in which a decentralized governance system dominates the network.

II. CHINA'S ADDITIONAL MOTIVATIONS FOR ISSUING E-CNY

Central banks worldwide share similar motivations when experimenting with CBDCs. These motivations are potentially improving financial inclusion, reducing transaction costs in the payment system, enhanced capacity to combat money laundering and other financial crimes, facilitating cross-border payments, and improving payment diversity.[66] Similarly, this Article does not need to reiterate all of them in detail.[67] Instead, this Article only focuses on three of China's possible

64. Duan Xiangyu (段相宇), Guancha | Yanghang Shuzi Huobi Jiang Ruhe Yingxiang Ni Wo? (觀察 | 央行數字貨幣將如何影響你我?) [Observation | How Will Central Bank Digital Currencies Affect You and Me?], Zhongyang Jiwei (中央紀委) [CENT. COMM'N FOR DISCIPLINE INSPECTION] (June 7, 2020, 7:00 AM), https://www.ccdi.gov.cn/yaowen/202006/t20200607_219642.html [https://perma.cc/8FHK-N7FX].

65. WORKING GRP., *supra* note 11, at 7.

66. BANK FOR INT'L SETTLEMENTS ET AL., CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES 5–6 (2020) [hereinafter FOUNDATIONAL PRINCIPLES], https://www.bis.org/publ/othp33.pdf [https://perma.cc/79KA-73Y4]. For money laundering, *see* Robert Z. Mahari et al., *AML by Design: Designing a Central Bank Digital Currency to Stifle Money Laundering*, MIT MEDIA LAB (Aug. 29, 2021), https://www.media.mit.edu/articles/aml-by-design-designing-a-central-bank-digital-currency-to-stifle-money-laundering/ [https://perma.cc/8CD6-AHHK]. For financial inclusion, *see Examining Regulatory Frameworks for Digital Currencies and Blockchain: Hearing Before the S. Comm. on Banking, Hous., & Urb. Affs.*, 116th Cong. *passim* (2019) (statement of Mehrsa Baradaran, Professor of Law, Univ. of Cal. Irvine Sch. of Law), https://www.banking.senate.gov/imo/media/doc/Baradaran%20Testimony%207-30-19.pdf [https://perma.cc/6HHJ-S8S9]; *IMF Seminar: CBDCs for Financial Inclusion: Risks and Rewards*, IMF, https://meetings.imf.org/en/2022/Annual/Schedule/2022/10/14/imf-seminar-cbdcs-for-financial-inclusion-risks-and-rewards [https://perma.cc/J4JT-7HUF] (last visited May 27, 2023). Some experts are skeptical that digital money will make much of a difference by itself, *see, e.g.*, Nadir Mohammed et al., *Is Central Bank Digital Currency the Right Tool to Expand Financial Inclusion?*, WORLD BANK BLOGS (Dec. 1, 2022), https://blogs.worldbank.org/allaboutfinance/central-bank-digital-currency-right-tool-expand-financial-inclusion [https://perma.cc/XA87-M9FL]. For cross border payments, *see* BANK FOR INT'L SETTLEMENTS ET AL., CENTRAL BANK DIGITAL CURRENCIES FOR CROSS-BORDER PAYMENTS *passim* (2021) [hereinafter CROSS-BORDER PAYMENTS], https://www.bis.org/publ/othp38.pdf [https://perma.cc/25EU-CC4M].

67. WORKING GRP., *supra* note 11, at 4.

unique motivations that are distinct from other countries. First, China appears to be using E-CNY and novel regulations to address the duopoly of the mobile payment market. Second, China's experimentation with E-CNY has been sped up by Diem (formerly known as Libra) due to the perceived threat that Diem could potentially undermine the monetary sovereignty of the RMB. Third, it is also arguable that China has an agenda to use E-CNY to internationalize the RMB and circumvent sanctions.

A. *Responding to the Cashless Economy and the Duopoly of Alibaba and Tencent in the Payment Market*

The PBOC wants to promote digitalization in China and is reacting to decreasing demand for cash. Since 2000, the amount of currency issuance has risen from thirteen trillion to 182 trillion yuan, but the proportion of paper cash in circulation decreases year by year.[68] The decrease also indicates that households' and businesses' access to paper cash is in decline. There is a danger that they will no longer have access to risk-free central bank money and are overly dependent on private platforms such as Alipay and WeChat pay that do not have the same mandate as the PBOC to protect against financial risk. Central banks usually consider it an obligation to provide public access. This access could be crucial for confidence in a currency. E-CNY could act like a "digital banknote" and could fulfill this obligation. China has moved rapidly toward a cashless economy in recent years due to the widespread development of mobile payment platforms. In 2019, with 851 million smartphone owners, eighty-six percent of China's population used mobile payments to make purchases.[69] The total value of all mobile transactions in a single year was fifty-two trillion U.S. dollars.[70] Therefore, the majority of China's population is becoming increasingly accustomed to cashless transactions.

However, the mobile payment market is dominated by two private companies, with Alibaba controlling 55.1% and Tencent controlling 38.9%, giving the two an effective duopoly over trillions of dollars in mobile payments.[71] Two private companies dominating ninety-four percent of the market share creates financial risks. For instance, a disruption to their digital payment infrastructure could potentially cause serious short-term economic instability. The bankruptcy of a private

68. Zhongguo de Huobi Gongying Liang (中国货币供应量) [China's Money Supply], EASTMONEY.COM, https://data.eastmoney.com/cjsj/hbgyl.html [https://perma.cc/AW5P-D4JD] (last visited May 27, 2023).

69. *How Will a Central Bank Digital Currency Advance China's Interests?*, CHINA POWER, https://chinapower.csis.org/china-digital-currency/ [https://perma.cc/85ZL-MWSF] (last visited May 27, 2023).

70. *Id.*

71. *Id.*

company could also be devastating. In addition, the government is not keen to cede control over payment systems to the private sector. Therefore, it is possible that the PBOC intends to enhance its own control over digital currency to not only serve as a backstop but also reduce the autonomy of these companies in the market. Consequently, this strengthens both the PBOC's supremacy and financial stability which avoids disintermediating commercial banks. To be clear, the Chinese government does not want to entirely disintermediate existing companies or even change the fact that they are a duopoly. Rather, the infrastructure of E-CNY allows the PBOC, and whatever political forces to which the PBOC is beholden, to exert pressure and control the behavior of the duopoly more directly.

B. *Responding to Cryptocurrencies and Diem*

Internationally, the emergence of cryptocurrencies and Diem[72] has pushed the PBOC to explore its own digital currency. Cryptocurrencies, especially Bitcoin, again triggered intense debate over who should control money in the future.[73] The peer-to-peer payment system of Bitcoin also urged the world to rethink the merits and drawbacks of existing payment systems.[74] Some countries, particularly China and Russia, have criticized the oversized role that the United States plays in the global financial system.[75] As the financial and monetary authority in the second-biggest economy, the PBOC has felt forced to rethink the role of the PBOC and the need to issue CBDC to compete with cryptocurrencies and optimize the payment system.[76] Therefore, one primary reason for the development and issuance of E-CNY is the maintenance of currency sovereignty.[77]

---

72. DIEM, https://www.diem.com/en-us/ [https://perma.cc/5WBY-PRMP] (last visited May 27, 2023).

73. Siripurapu, *supra* note 20; Gita Blatt, *Reimagining Money in the Age of Crypto and Central Bank Digital Currency*, IMF BLOG (Sept. 1, 2022), https://www.imf.org/en/Blogs/Articles/2022/09/01/reimagining-money-in-the-age-of-crypto-and-central-bank-digital-currency [https://perma.cc/S7SB-R24M]; Zongyuan Zoe Liu, *Besides China, Putin Has Another Potential De-Dollarization Partner in Asia*, COUNCIL ON FOREIGN RELS. (Mar. 11, 2022, 12:28 PM), https://www.cfr.org/blog/besides-china-putin-has-another-potential-de-dollarization-partner-asia [https://perma.cc/22BY-ULMU].

74. Siripurapu, *supra* note 20.

75. Carla Norrlof, *China and Russia Announced a Joint Pledge to Push Back Against Dollar Hegemony*, WASH. POST (Apr. 9, 2021, 7:00 AM), https://www.washingtonpost.com/politics/2021/04/09/china-russia-announced-joint-pledge-push-back-against-dollar-hegemony/ [https://perma.cc/9DBW-BMCL].

76. WORKING GRP., *supra* note 11, at 2–3.

77. *Id.* at 5, 6; Steffen Murau & Jens van't Klooster, *Rethinking Monetary Sovereignty: The Global Credit Money System and the State*, PERSPS. ON POL., Aug. 2022, at 1–18, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/33EE76D8B70FB9

The Diem Association's efforts to launch its Diem payment system in 2019 directly sped up China's experiment with E-CNY because of the perceived threat to currency sovereignty.[78] Compared to crypto-currencies, which are often associated with high volatility, highly distributed or nonexistent internal governance, and technological issues making them unlikely to replace fiat money as a form of payment, Diem appeared to be a much stronger competitor to central bank money. With a potential 2.7 billion monthly active users worldwide,[79] if Diem had been widely adopted, the concern was that central banks would face the threat of losing control of tracking their citizens' financial activities and financial data within their jurisdictions to Diem. As of 2023, Diem has not been adopted and the project stalled.[80] Other stablecoin companies, such as Circle, however, could also appear threatening to the PBOC for similar reasons.[81]

Significant adoption of money not denominated in the sovereign currency could see a national currency substituted by another with the domestic central bank gradually losing control over monetary matters and the domestic economy.[82] This could be a risk that the PBOC is concerned about; the widespread adoption of cryptocurrencies or stablecoins could diminish the use of RMB, which could further undermine the monetary sovereignty of the RMB and the capacity of the PBOC to manage China's economy.[83] Therefore, to prevent this from happening, China has been

54A03BF1124B79AA5C/S153759272200127Xa.pdf/rethinking-monetary-sovereignty-the-global-credit-money-system-and-the-state.pdf [https://perma.cc/V6KW-WARW].

78. Jiaying Jiang & Karman Lucero, *Background and Implications of China's Central Bank Digital Currency: E-CNY*, SLS BLOG (Apr. 6, 2021), https://law.stanford.edu/2021/04/06/background-and-implications-of-chinas-central-bank-digital-currency-e-cny/ [https://perma.cc/HY9N-VMMT].

79. Press Release, Facebook, Facebook Reports Third Quarter 2020 Results (Oct. 29, 2020), https://s21.q4cdn.com/399680738/files/doc_news/Facebook-Reports-Third-Quarter-2020-Results-2020.pdf [https://perma.cc/XFE2-V2X8].

80. *Facebook-Funded Cryptocurrency Diem Winds Down*, BBC NEWS (Feb. 1, 2022), https://www.bbc.com/news/technology-60156682 [https://perma.cc/XNR9-W2HV].

81. Timmy Shen, *Stablecoins Could Pose Risks to Global Financial System, Chinese Central Bank Official Says*, FORKAST (July 8, 2021), https://forkast.news/stablecoins-could-risk-global-financial-system-pboc-says/ [https://perma.cc/4NVM-K8Z9].

82. BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES (2020), https://www.bis.org/publ/othp33.pdf [https://perma.cc/PB63-XUUG].

83. Alun John et al., *China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling*, REUTERS (Sept. 24, 2021, 1:49 PM), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/ [https://perma.cc/B28K-89C7].

speeding up its experimentation with E-CNY.[84] It has also banned the mining and use of cryptocurrencies within its own financial system.[85]

C. *Internationalization of the RMB?*

The implications of E-CNY not only concern fears about currency sovereignty but also about China's capacity to compete internationally as a financial policy innovator. Some reports claim that China intends to internationalize its RMB with the use of E-CNY.[86] The prospect of increased internationalization of the RMB is a perennial topic, most recently with Xi Jinping's visit to Saudi Arabia and discussions around increasing the roll of the RMB in global energy markets.[87] China has had a longstanding interest in internationalizing the RMB,[88] an ambition that dates to at least 2007. However, inter-nationalization of the RMB may not be a key outcome of the development of E-CNY. This is because E-CNY, by itself, represents an additional form of money, while the barriers to the RMB's internationalization depend more on institutional development and the policy choices made by the PBOC and the Chinese government more broadly.[89]

The internationalization of a currency involves many aspects of functions of money: a store of value, a medium of exchange, a unit of account, and sometimes, a standard or deferred payment.[90] Currency digitalization is an innovation in the area of payment but does not cover all other aspects. A country's currency becoming an international

---

84. Don Weinland, *China Is Rapidly Rolling Out Its New Digital Currency*, ECONOMIST (Nov. 18, 2022), https://www.economist.com/the-world-ahead/2022/11/18/china-is-rapidly-rolling-out-its-new-digital-currency [https://perma.cc/WU3Y-FXCJ].

85. Francis Shin, *What's Behind China's Cryptocurrency Ban?*, WORLD ECON. F. (Jan. 31, 2022), https://www.weforum.org/agenda/2022/01/what-s-behind-china-s-cryptocurrency-ban/ [https://perma.cc/M4KT-MEYW].

86. Chen Jia, *E-CNY Certain to Promote Renminbi's Internalization*, CHINA DAILY (July 29, 2021), https://global.chinadaily.com.cn/a/202107/29/WS610201faa310efa1bd66528b.html [https://perma.cc/4DKZ-NVDZ].

87. Teddy Ng, *China Pushes to Boost Role of Yuan in Global Energy Markets as Xi Jinping Wraps Up Saudi Arabia Visit*, S. CHINA MORNING POST (Dec. 10, 2022), https://www.scmp.com/news/china/diplomacy/article/3202831/china-pushes-boost-role-yuan-global-energy-markets-xi-jinping-wraps-saudi-arabia-visit [https://perma.cc/JGC2-K6F8].

88. BLOOMBERG, DEVELOPMENTS IN OFFSHORE RMB: TOWARDS INCREASED TRANSPARENCY AND FURTHER INTERNATIONALIZATION OF THE RENMINBI *passim* (2013), https://www.cmegroup.com/education/files/china-steps-up-efforts-to-internationalize-renminbi.pdf [https://perma.cc/2ZTT-LHBD].

89. Michael Pettis, *Changing the Top Global Currency Means Changing the Patterns of Global Trade*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 12, 2022), https://carnegieendowment.org/chinafinancialmarkets/86878 [https://perma.cc/P6QD-YA2Q].

90. Irena Asmundson & Ceyda Oner, *What Is Money?*, INT'L MONETARY FUND (Sept. 2012), https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm [https://perma.cc/WW22-3ETW].

currency depends fundamentally on that country's economic, political, technological, and military capacities and influence. The mere change of form or the digitalization of the RMB will not make the RMB an international currency. To truly internationalize the RMB, China would need to do much more, such as promoting market-oriented reforms, developing the RMB offshore market, loosening capital controls, further developing the rule of law, and welcoming foreign investments. As Henry Paulson Jr. suggested, China would need to develop efficient and well-regulated financial markets that earn the respect of international investors so that China can eliminate capital controls and turn the RMB into a market-determined currency.[91] Current trends toward the internationalization of the RMB, to the extent that they exist, are not focused on the use of a digital versus more traditional currency. Rather, economists appear to be more focused on the popularity of the RMB bond market and growing potential risks in the United States.[92]

E-CNY's geopolitical implications, however, extend beyond the internationalization of the RMB. The E-CNY could help advance China's foreign policy goals in other ways. For example, one considered impact of E-CNY, or more accurately, the greater development of a digital infrastructure for the use of the RMB more internationally, is that it would help China engage with countries targeted by U.S. or other sanctions by allowing Chinese companies to transact with sanctioned entities using currency and intermediaries (whether banks or some other institution) that are not integrated in or dependent on the U.S. led global financial system.[93] One relatively unconsidered dynamic, however, is that this could remove the possibility for China's government to plausibly deny knowing when entities utilizing E-CNY conduct transactions prohibited by the U.S. government or any other political institution.

There is a great deal of concern in the media about China's grand ambitions with the E-CNY. While the government may harbor many such ambitions, E-CNY at this stage is only modestly different from existing money. One of the PBOC's key motivations appears to be cultivating the talent and institutional knowhow to develop digital currencies and be able to flexibly respond to the impact of digital currencies as they are developed and deployed across the world, whatever that impact happens to be. The PBOC likely wants to be prepared for the unknown contingencies that come from digital currencies. By developing E-CNY,

91. Henry M. Paulson Jr., *The Future of the Dollar*, FOREIGN AFFS. (May 19, 2020), https://www.foreignaffairs.com/united-states/future-dollar [https://perma.cc/UL6F-6C5D].

92. Martin Chorzempa, *China's Pursuit of Leadership in Digital Currency*, PETERSON INST. FOR INT'L ECON. (Apr. 15, 2021), https://www.piie.com/commentary/testimonies/chinas-pursuit-leadership-digital-currency [https://perma.cc/9SBR-422F].

93. Kumar & Rosenbach, *supra* note 7.

they are also developing the capacity to be more prepared for an unknown, more digital future.

III. WHAT ARE THE POTENTIAL IMPACTS OF E-CNY?

There remains a great deal of mystery and questions around the development and deployment of E-CNY. Below is a discussion regarding the potential impacts considering currently public information.

A. *Impacts on Cost and Efficiency*

It is unclear if the E-CNY will help the PBOC reduce the net costs of currency creation and distribution. Although the PBOC could reduce the cost of running the cash-based system, additional expenditures, such as server space and the costs of running the new institutions responsible for E-CNY, will lead to other costs. Establishing the entire E-CNY system and relevant financial infrastructures likely will not be cheap or easy. It is possible that, by shifting to a digital currency that is free for individuals and businesses to use, the PBOC is engaging in a cost-shifting mechanism away from merchants. The PBOC itself will be more directly responsible for the infrastructure of the currency and transactions made with it, but holding and transacting with E-CNY will be cheaper for individuals and businesses. Realizing these goals, however, requires more than just developing a digital currency; it requires building institutions that connect the PBOC with financial intermediaries and individuals and organizations in a trusted, secure, and fluid network with a digital currency that is easy to use. Such a project is about more than just technology.

One key argument is that, as a digital currency, E-CNY's most obvious benefit is faster, cheaper, and more efficient payments, both domestically and across borders.[94] This argument is similar to arguments about the benefits of digital currencies (including cryptocurrencies) more generally and is based on the digital nature of E-CNY which, in theory, can provide for frictionless transactions. Yao Qian touts the virtues of digital currencies as programmable and "intelligentized," affording possibilities such as smart contracts, account-less access, and other tools that could benefit consumers.[95] To be clear, this is mostly theoretical at this point. A potential problem is that many of the "frictions" involved in

94. CROSS-BORDER PAYMENTS, *supra* note 66; *Central Bank Digital Currency (CBDC) Frequently Asked Questions*, FED. RSRV., https://www.federalreserve.gov/cbdc-faqs.htm [https://perma.cc/94GH-SGK3] (last visited June 1, 2023).

95. Xu Zhong (徐忠) & Yao Qian (姚前), Xu Zhong Yao Qian: Shuzi Piaoju Jiaoyi Pingtai Chubu Fang'an (許忠堯謙：數字票據交易平台初步方案) [Xu Zhong Yao Qian: Preliminary Plan for Digital Bill Trading Platform], Xiao Tu (小兔) [BABIT], https://www.8btc.com/books/834/cnfinance201617/_book/content/10.html [https://perma.cc/PY9H-YSC8] (discussing the initial plan of the exchange platform for digital notes).

transactions are not physical or technical, but rather social and legal. Transaction costs will still play a large and complex, if different, role in digital currency transactions.

Current pilots of E-CNY have generally been far more lackluster and quotidian; there have not been "intelligentized" or programmable pilot uses of E-CNY containing more affordances for users compared to regular fiat currency. The main benefit in these pilot cases appears to be that the government is handing it out for free.[96] E-CNY has been "programmed" such that pilot cases have limited the context and extent to which consumers can use E-CNY, such as with specific retailers or for a particular purpose (like consumption).[97] In this sense, E-CNY is comparable to digital gift cards. Therefore, E-CNY's distinction from using apps in China's highly mobile payments ecosystem is that, with E-CNY, the PBOC can limit what you do with your money in more targeted ways. From this perspective, it is unclear why consumers in or outside of China would want to readily adopt or use E-CNY. To date, the government has basically had to pay people to use it.[98] Doing so on a sufficient scale to encourage mass use and adoption would be prohibitively expensive and unsustainable. Former PBOC official Xie Ping has confirmed limited adoption of E-CNY so far.[99]

B. *Impacts on the Payment System and the Mobile Payment Duopoly*

The impact on the existing payment system depends significantly on how the PBOC deploys E-CNY. The PBOC seems to emphasize the roles of existing intermediaries, especially commercial banks. In the two-tier design of E-CNY, the PBOC decides to rely on commercial banks and other authorized entities as intermediaries to distribute E-CNY. Thus, the role of commercial banks and these entities would remain significant and maintain several similarities with their roles in the current economy. This of course raises the question of what exactly is different about E-CNY. Like other topics discussed above, the goals inherent in the development

96. Enoch Yiu, *Bank of China Offers Customers E-Laisse to Promote Retail Use of Digital Yuan in Hong Kong*, S. CHINA MORNING POST (Dec. 12, 2022, 8:35 AM), https://www.scmp.com/business/banking-finance/article/3203037/bank-china-offers-customers-e-laisee-promote-retail-use-digital-yuan-hong-kong [https://perma.cc/TQH7-VVRV].

97. *China Uses Digital Yuan to Stimulate Virus Hit Consumption*, REUTERS (May 30, 2022, 7:26 AM), https://www.reuters.com/markets/currencies/china-uses-digital-yuan-stimulate-virus-hit-consumption-2022-05-30/ [https://perma.cc/E984-C4XS].

98. Jennifer Conrad, *China's Digital Yuan Works Just Like Cash—With Added Surveillance*, WIRED (Nov. 8, 2022, 8:00 AM), https://www.wired.com/story/chinas-digital-yuan-ecny-works-just-like-cash-surveillance/ [https://perma.cc/8RFE-M7M5].

99. Xie Ping, *supra* note 48; *Former PBOC Official Says China's Digital Yuan Is Little Used - Caixan*, REUTERS (Dec. 29, 2022, 3:54 AM), https://www.reuters.com/technology/former-pboc-official-says-chinas-digital-yuan-is-little-used-caixin-2022-12-29/ [https://perma.cc/73FE-85CD].

and deployment of E-CNY could be quite ambitious. With the current state of E-CNY, however, a little bit of digging and investigation reveals a more banal reality.

As mentioned above, one of the reasons that the PBOC has experimented with E-CNY is to respond to Alibaba and Tencent's duopoly in the payment market and be more prepared for different contingencies. Since the PBOC could choose to clear transactions and expand insights into the nature and contexts of transactions, Alipay and Tencent could lose a great deal of de facto independence and maneuver room with more widespread adoption of E-CNY, particularly if E-CNY deployment decreases their role as intermediaries or places more rules on what they can do in terms of data collection and analysis as intermediaries. At the very least, the PBOC would have more leverage over Alipay and Tencent with a widely used E-CNY serving as a digital tether. The onset of E-CNY could also catalyze the PBOC's own rulemaking and attempts to expand influence over the duopoly, even if the mechanisms of such expansion are not related to E-CNY directly.

For example, the PBOC and Chinese government more broadly are already chipping away at Alipay and WeChat Pays' combined power. New rules passed in 2021 require Alibaba and Tencent (as well as other tech companies) to share their data with the PBOC and other regulators. This data sharing went into effect in December 2022.[100] Despite some remaining logistical hurdles for implementation,[101] this data-sharing requirement changes the nature of the relationship between tech companies, the PBOC, and other regulators. This has all taken place in the context of a broader political and regulatory crackdown by the Chinese government against tech companies, including Alibaba and Tencent.[102] While not every piece of the tech crackdown targets fintech or digital payment platforms per se, it does represent a broader shift in the relationship between the government and tech companies. Digital payments and the future of E-CNY should be viewed in the context of this changing relationship.

Netting serves as another example. Since 2017, a new rule required mobile payment companies to clear their transactions through a stated-owned clearing corporation, NetsUnion Clearing Corporation Ltd (网联清算有限公司), a partially state- but majority privately-owned entity,

100. Jimmy Choi, *PBOC Pushes Big Techs to Hand over User Data, Report Says*, CENT. BANKING (Nov. 25, 2022), https://www.centralbanking.com/central-banks/financial-stability/7953792/pboc-pushes-big-techs-to-hand-over-user-data-report-says [https://perma.cc/N2FN-CP8M].

101. Sun Yu, *China's Central Bank Struggles to Force Tech Groups to Share User Data with State*, FIN. TIMES (Nov. 3, 2022), https://www.ft.com/content/75409a44-6cfb-43e9-be31-776eb814a919 [https://perma.cc/KB86-BWY5].

102. *China's Big Tech Crackdown: A Complete Timeline*, CHINA PROJECT, https://thechinaproject.com/big-tech-crackdown-timeline/ [https://perma.cc/349P-9EM3] (last visited Jan. 31, 2023).

with a number of tech companies including Alibaba and Tencent having significant shares.[103] While the state has already taken a greater role in mobile payment transaction clearing, Alipay and Tencent still have a great deal of flexibility when it comes to netting and otherwise managing funds controlled on their platforms. E-CNY, allowing the PBOC to clear more transactions itself, would likely have an impact on how these digital platforms handle their consumers' money flows. Currently, a highly detailed understanding of how Alipay and WeChat Pay handle transactions and the flow of money is possibly only known by the companies themselves. Even though they have to clear a majority of transactions via NetsUnion, they have a great deal of autonomy in handling their funds between transactions. The fact that NetsUnion is also a mostly private entity also places at least logistical limits on the PBOC and other government agencies' access to clearing and data. E-CNY could make the PBOC (and the government by extension) a primary actor with direct oversight of and influence over how the companies manage their customer's funds. The duopoly might have less flexibility and leeway with growing deployments of E-CNY. What exactly the PBOC would do with this leverage remains to be seen. In theory, when the government created NetsUnion, it could have established it as a state-owned enterprise within the PBOC or government regulator. It did not.

E-CNY could also take away some market share that these two companies currently possess. Merchants potentially have the economic motivation to switch to E-CNY because it is free for merchants to transact with E-CNY while Alipay and WeChat Pay charge merchants fees.[104] Consumers, on the other hand, seem to be less motivated because it is free for them to use either E-CNY or Alipay/WeChat Pay. Alipay and WeChat Pay have the advantage of momentum; consumers are already used to using their platforms ubiquitously. Besides, the digital wallet underlying E-CNY is similar to digital wallets for Alipay and WeChat Pay, suggesting that the "user experience" for digital currencies will be similar to existing models, or at least that the PBOC is attempting to make them so. It could even be more difficult for consumers to adopt to E-CNY as they are so accustomed to Alipay and WeChat Pay. However, E-CNY, backed by the PBOC as the state agency, has more power to dissuade

103. Jinshan Hong, *How China's Central Bank Is Clamping Down on the Mobile Payment Industry*, FORBES (Aug. 18, 2017, 2:35 AM), https://www.forbes.com/sites/jinshanhong/2017/08/18/how-chinas-central-bank-is-clamping-down-on-the-mobile-payment-industry/?sh=131334f350be [https://perma.cc/Z5NL-QQHC].

104. *WeChat Pay/Alipay Fees for Merchants*, OCEAN PAYMENTS (Sept. 9, 2021), https://www.oceanpayment.com/blog/19775/ [https://perma.cc/XPX6-4Y65]; Sonnet Frisbie, *Widespread E-CNY Adoption in China Is Coming, Whether Banks and Businesses Like It or Not*, MORNING CONSULT (June 13, 2022), https://morningconsult.com/2022/06/13/e-cny-adoption-in-china-is-coming/ [https://perma.cc/J8YZ-RWUX].

consumers from using the incumbents by force. For instance, mandates could require salaries or government subsidies to get paid with E-CNY.

Going forward, Alipay and WeChat Pay will likely be both competitors and crucial partners of the PBOC. They are competitors because they all hunt for more users in the payment market. They are partners because the PBOC intends to rely on Alipay and WeChat Pay as the second-tier distributors of E-CNY. Alipay and WeChat Pay could greatly help with E-CNY circulation because of their strong networks and widespread application scenarios. It is unwise to nudge them out of the market entirely. There could be other markets to explore. According to interviews with employees, Alipay does not have enough information to predict how specifically a digital currency will impact the payments environment or their business. One employee stated: "[a]s people pioneered different kinds of money, they created different kinds of markets."[105]

C. *Impacts on Monetary Policy*

Widespread adoption of E-CNY could give the PBOC greater capacity to develop and deploy mechanisms of monetary policy. This greater capacity in theory offers both advantages and disadvantages. A digital currency offers the capacity for more tailored, specific, and siloed interventions into the economy, both by controlling the flow of currency as well as by controlling interest rates more directly. It is important to reiterate that this is all still theoretical. Each of these affordances depends on a highly developed digital infrastructure to accommodate E-CNY as well as actual widespread use. The PBOC has so far chosen not to make E-CNY interest bearing by itself.[106] While a digital currency potentially offers more flexibility, it likely will not solve structural economic problems without the addition of institutional innovation and reform. Implementing a digital currency such that the PBOC and other regulators could take advantage of the network effects required to use such affordances, depends on more than the mere development of a digital wallet and digital RMB. The PBOC and the government more broadly would need to find a way to actually realize the widespread use of E-CNY and develop the personnel and knowledge to take advantage of all the new information and capabilities that E-CNY provides.

D. *Impacts on BRI Countries*

E-CNY could be most impactful in countries that: (1) have more integrated economic relationships with China and are accustomed to utilizing Chinese consumer services; (2) do not have strongly established

105. Zhang Xuan & Wang Tuo, *supra* note 17.

106. WORKING GRP., *supra* note 11, at 7.

financial systems; and (3) might be drawn to mobile payment systems. Many countries participating in the Belt and Road Initiative (BRI), for example, could have great potential for burgeoning digital payments markets. Since the BRI involves Chinese companies, the use of a more frictionless E-CNY might encourage more consumers in BRI countries to utilize the yuan in digital form, thus spurring increased international use of the RMB and establishing the PBOC as a de facto international clearinghouse. As of yet, none of this has happened. E-CNY's pilots have remained overwhelmingly domestic, and consumers in Africa's largest economies, for example, continue to use forms of payment other than Chinese tech platforms tied to the yuan.[107] However, BRI countries might also be reluctant to be increasingly beholden to the Chinese government. These countries might be choosing to transact in dollars not only because the U.S. dollar is the international reserve currency but also to partially hedge China's potential influence over their nations' growing infrastructure and financial systems.

E. *Impacts on International Settlements*

It is unclear how E-CNY will affect international settlements, though some have argued that one goal and outcome of E-CNY will be to undermine the role of the dollar as an international reserve currency or otherwise challenge the United States' power as the global financial nexus.[108] China's Cross-Border Interbank Payment System (CIPS) and other SWIFT alternatives already exist without the need for digital currencies.[109] It appears that many barriers to setting up international settlement systems are not technical, but have more to do with legal, institutional, and policy hurdles. New institutions that China sets up in conjunction with E-CNY could change international finance. For example, if the Chinese government further improved market access and

---

107. *Distribution of Online Payment Methods in Selected African Countries as of 2021*, STATISTA, https://www.statista.com/statistics/1190895/distribution-of-online-payment-methods-in-african-countries/ [https://perma.cc/9FKC-PDBG] (last visited Apr. 13, 2023).

108. Eustance Huang, *China's Digital Yuan Could Challenge the Dollar in International Trade This Decade, Fintech Expert Predicts*, CNBC (Mar. 15, 2022, 2:22 AM), https://www.cnbc.com/2022/03/15/can-chinas-digital-yuan-reduce-the-dollars-use-in-international-trade.html [https://perma.cc/6SPC-U4JD]; Zongyuan Zoe Liu, *China Is Quietly Trying to Dethrone the Dollar*, FOREIGN POL'Y (Sept. 21, 2022, 3:59 PM), https://foreignpolicy.com/2022/09/21/china-yuan-us-dollar-sco-currency/ [https://perma.cc/ YG66-J74R].

109. Barry Eichengreen, *Sanctions, SWIFT, and China's Cross-Border Interbank Payments System*, CSIS (May 20, 2022), https://www.csis.org/analysis/sanctions-swift-and-chinas-cross-border-interbank-payments-system [https://perma.cc/8XHS-5USC]; Huileng Tan, *China and Russia Are Working on Homegrown Alternatives to the SWIFT Payment System. Here's What They Would Mean for the US Dollar*, BUS. INSIDER (Apr. 28, 2022, 11:17 PM), https://www.businessinsider.com/china-russia-alternative-swift-payment-cips-spfs-yuan-ruble-dollar-2022-4 [https://perma.cc/L8YE-HW29].

lessened convertibility restrictions in conjunction with implementing a digital currency then international governments, businesses, and other actors might be more inclined to use a Chinese-backed, SWIFT alternative.

But it is unlikely a digital currency, by itself, would greatly change international settlement systems. It is unclear how E-CNY itself could improve market access, lessen convertibility restrictions, or address rule of law concerns. For example, many complaints about current international clearing systems involve the slow speed of transactions as well as the expense of transferring money across borders. The time and expense involved, however, appear to be more related to the gatekeeping capacities of banks and regulatory requirements of different countries, rather than specific technological issues. A digital currency might change the specific dynamics of who can gatekeep and how, but it will not eliminate further institutional, legal and policy barriers.

IV. WHAT ARE THE CHALLENGES FACING THE DEVELOPMENT AND DEPLOYMENT OF E-CNY?

One of the key challenges associated with E-CNY development and deployment is the uncertainty of data access and data usage. This uncertainty raises a series of questions. Who has access to what information? How will the state guarantee due process rights regarding access to and use of data? How will the state and intermediaries protect users' privacy? Additional challenges include a lack of technological transparency and cybersecurity threats.

A. *The Uncertainty of Information Access and Use*

The purely informational nature of E-CNY raises challenges about information access and protection: to what information do which government agencies have access? How does tracking, investigating, and suspending accounts work? The PBOC will have complete access to information concerning transactions using E-CNY. What about other government agencies? It seems clear that other agencies will need access to this information, including law enforcement and tax authorities. What rules govern access to this information? Will local governments have any access to the PBOC's information?

While existing rules detail and purport to control government agencies' access to and sharing of information—including the Notice of the State Council on Issuing the Interim Measures for the Administration of Sharing of Government Information Resources (the "Measures")[110]

110. Guowuyuan Guanyu Yinfa Zhengwu Xinxi Ziyuan Gongxiang Guanli Zanxing Banfa de Tongzhi (國務院關於印發政務信息資源共享管理暫行辦法的通知) [Notice of the State

and Guidelines for the Preparation of Catalogues of Government Information Resources (the "Guidelines")[111]—their specific applicability to E-CNY remains unclear. The Measures specify four principles regarding how government information should be shared and require that government information should be divided into three categories: unconditional sharing, conditional sharing, and non-sharing.[112] The Guidelines require all government departments to compile, maintain, and update their catalogues of government information resources.[113] However, the Measures do not clearly define or enumerate what information belongs to which category and how to specifically differentiate sharable and non-sharable information.[114] Therefore, it remains unclear if E-CNY information collected by the PBOC is sharable and, if it is, whether it should be shared unconditionally. Although the Guidelines do enumerate four categories (and a few secondary catalogues) of government information resources, it is still unclear if E-CNY information fits into one of these.

Some more broadly applicable legislation aimed at data protection, such as the Data Security Law (the "DSL")[115] and the Personal Information Protection Law (the "PIPL"),[116] have clauses nominally placing limits on how the state can collect, utilize, and analyze data. However, these clauses are quite vague, and it is unclear how they are to be enforced generally, let alone in the context of E-CNY. How will individuals know that government agencies and private companies are following the law, either the DSL or PIPL? In terms of some unanswered

---

Council on Printing and Distributing the Interim Measures for the Management of Government Information Resources Sharing], Zhongua Renmin Gongheguo Zhongyang Renmin Zhengfu (中華人民共和國中央人民政府) [CENT. PEOPLE'S GOV'T OF THE PEOPLE'S REPUBLIC OF CHINA] (Sept. 5, 2016) [hereinafter Guowuyuan Guanyu], http://www.gov.cn/zhengce/content/2016-09/19/content_5109486.htm [https://perma.cc/RRV9-BKNM].

111. Guojia Fazhan Gaige Wei Zhongyang Wang Xin Ban Guanyu Yinfa Zhengwu Xinxi Ziyuan Mulu Bianzhi Zhinan de Tongzhi (國家發展改革委 中央網信辦關於印發政務信息資源目錄編制指南的通知) [Notice of the National Development and Reform Commission and the Central Cyberspace Administration on the Issuance of the Guidelines for the Preparation of Catalogues of Government Information Resources], Zhongua Renmin Gongheguo Zhongyang Renmin Zhengfu (中華人民共和國中央人民政府) [CENT. PEOPLE'S GOV'T OF THE PEOPLE'S REPUBLIC OF CHINA] [hereinafter Guojia Fazhan], https://www.gov.cn/xinwen/2017-07/13/5210203/files/2415d43d2bcb4dfe9c3f1e1b5c0626c1.pdf [https://perma.cc/H78K-UNG5].

112. Guowuyuan Guanyu, *supra* note 110.

113. *Id.*

114. *Id.*

115. Data Security Law (promulgated by the Standing Comm. of the Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), art. 38, 2021 P.R.C. LAWS 84. http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml [https://perma.cc/A5VG-KFA2].

116. Zhonghua Renmin Gongheguo Geren Xinxi Baohu (中华人民共和国个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. of the Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), 2021 P.R.C. LAWS.

questions, the PBOC should consider various transparency mechanisms, such as releasing periodic transparency reports detailing such information, to alleviate the concerns of individuals and businesses.

On top of that, it is unclear how exactly citizen rights will be enforced under this existing paradigm. The Guidelines mandate that the National Development and Reform Commission shall be responsible for creating and organizing an information-sharing platform.[117] They also order the creation of an "Inter-Ministerial Joint Meeting for Big Data Development" made up of departments from the State Council and local governments, that is responsible for "the overall planning and coordination of sharing of government information resources . . . and inspection of the implementation of the sharing of government information resources."[118] This is a complex task all on its own. Combined with the general opacity that is typical of Chinese intergovernmental regulation and disciplining, the general public appears to have no way to monitor or confirm that government agencies are protecting their information. Therefore, it would be helpful if this "Joint Meeting" published transparency reports detailing the extent to which government agencies follow the guidelines.

There are additional questions related to law enforcement and national security agencies' access to information. For example, the Australian Strategic Policy Institute has published a report in which they highlight some of the concerning ways that the Ministry of State Security is involved in the E-CNY project.[119] What kind of access will the Ministry of State Security have to the PBOC's trove of E-CNY related information? In addition to the PBOC itself, intermediaries involved in the deployment of E-CNY must necessarily have access to at least some information involved in E-CNY transactions. What rights and responsibilities do they have regarding this information? For example, will the way that Alipay and WeChat Pay treat user information and the analytics surrounding it change with E-CNY? What about other intermediaries? It is clear that the amount of data collected from E-CNY could be useful and valuable under the right circumstances. To what kinds of uses will all of this accumulated data be put? What kinds of rules and regulations are necessary to incentivize the productive use of this data while simultaneously protecting individual privacy and the integrity of the system as a whole?

These questions are important for reasons of information security and the protection of individual rights. Increased government access to

117. Guojia Fazhan, *supra* note 111, at 4.

118. *Id.* at 12.

119. Samantha Hoffman et al., *The Flipside of China's Central Bank Digital Currency,* AUSTRALIAN STRATEGIC POL'Y INST. (Oct. 14, 2020), https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency [https://perma.cc/P3GD-NX89].

transaction information raises serious questions about privacy and free expression. In theory, this information could be used to spy on and coerce individual account holders for reasons other than criminal activity. It would be beneficial for the rights of users as well as the viability of E-CNY if the National People's Congress (NPC) articulated clear rules regarding how the PBOC can share collected data with third parties, including other government agencies and private companies. For example, existing rules strictly govern the amount and kinds of information that the PBOC shares with credit rating agencies, as well as what credit rating agencies can do with this information. It would also be necessary for these rules to include clear and transparent enforcement mechanisms that can be monitored by the public.

However, at this stage, it is unclear how much, if any, information collected by the PBOC in conjunction with E-CNY will fall under these provisions. These existing regulations, however, could at least serve as a potential model for future regulations on information sharing and usage for E-CNY. The NPC, or at least PBOC, should also issue clear rules articulating the duties of intermediaries, whether they be traditional commercial banks, online mobile empires, or other entities regardless of their status as a government or private entity.

B. *Due Process Challenges*

Widespread deployment of E-CNY would potentially offer the PBOC, and the Chinese government by extension, unprecedented, real-time influence over the economic rights and capabilities of individuals. Currently, central banks and law enforcement often need to rely on the cooperation and compliance of intermediaries to investigate and enforce laws related to financial crime.[120] This includes legal actions against individuals committing financial crimes such as money laundering as well as entities subject to government sanctions. Such institutional frictions increase the incentives for governments to act within legal bounds. In theory, the fact that the PBOC or another governmental entity could monitor more transactions conducted with E-CNY would give relevant authorities the power to unilaterally halt transactions and effectively freeze individuals or institutions out of the financial system. Absent additional mechanisms, individuals and businesses would just have to assume that the PBOC is doing so legally.

For example, online payment intermediaries govern the closing of accounts based on their terms of services (which are often opaque and not very specific). Will the government have the power to shut off a user from accessing their digital wallet and digital currency? Losing access to one's Alipay or WeChat account is likely quite devastating to certain actors in

120. Jiang & Lucero, *supra* note 78.

certain circumstances. But the PBOC's denials of access to E-CNY accounts could result in greater consequences. If one loses their Alipay account, they could start another one, including with another platform. If the PBOC decides to cut off their access to using E-CNY, it is unclear what alternatives such a person or entity might have, particularly if wider use of E-CNY reduces the use of paper currency. As a result, it seems necessary to clearly articulate under what circumstances the PBOC or other relevant authority can halt a transaction and further shut off an E-CNY account, what procedures to follow, and what rights individuals regarding their own digital wallets and the E-CNY maintained therein. Even though a litany of laws already governs information sharing for government agencies and private entities, it would be helpful if the NPC and PBOC more clearly articulated the rights of citizens and the responsibilities of every entity involved in E-CNY.

C. *Privacy Protection Challenges*

The amount of information collection that a digital currency enables raises serious questions about privacy, both in terms of private companies as well as from governments. Current rules suggest that both the PBOC and commercial banks, at a minimum, will collect copious amounts of information about businesses, individuals, and their transactions. Digital payment platforms already collect large amounts of information. Given the broad extent of information collection, how will the PBOC protect users' privacy? The PBOC's proposed "manageable anonymity" is ambiguous and leaves many unanswered questions.

The Civil Code of the PRC (the "Civil Code"), which came into effect on January 1, 2021, could address some of the privacy issues here and mandate the protection of personal information.[121] Article 1034 of the Civil Code states that personal information of natural persons is protected by law and defines personal information as "various information recorded electronically or in other forms that can identify a specific natural person separately or in combination with other information, including a natural person's name, date of birth . . . and whereabouts information, among others."[122] Under this definition, relevant information of E-CNY, such as account information and transaction information, most probably can "identify a specific person" either separately or in combination with other information, and thus in theory should be in the category of personal information protected by law.

---

121. Zhonghua Renmin Gongheguo Minfa Dian (中華人民共和國民法典) [THE CIVIL CODE OF THE PEOPLE'S REPUBLIC OF CHINA], Zhonghua Renmin Gongheguo Quanguo Renmin Daibiao Dahui (中華人民共和國全國人民代表大會) [NAT'L PEOPLE'S CONG. OF THE PEOPLE'S REPUBLIC OF CHINA], http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml.

122. *Id.*

Article 1035 specifies the principles and conditions of processing personal information.[123] The PBOC and other entities processing relevant E-CNY information might have to follow these rules. Article 1039 specifically addresses the roles of state "organs" and chartered institutions assuming administrative functions.[124] Their staff should protect the privacy and personal information obtained in the course of fulfilling their duties.[125] Here, as a major personal information processor, the PBOC has a legal responsibility to keep confidential the privacy and personal information of E-CNY users and activities.

Any violations of the law should be subject to punishment. However, the Civil Code has not specified which department oversees enforcing these laws.[126] It is also not clear that private citizens have any capacity to investigate or otherwise enforce their rights against government agencies in this capacity. Article 1038 briefly mentions that any personal information leakage, tampering, or loss should be reported to the "competent authorities."[127] The NPC, State Council, or PBOC should each specify what government agencies are responsible for monitoring compliance as well as how individuals can otherwise confirm that their rights are otherwise being protected.

The PIPL could also address some of the privacy concerns. For instance, where personal information processors provide a third party with the personal information they process, the law requires that they notify the individuals of the third party's relevant information and obtain independent consent from the individual.[128] Where personal information processors provide anonymized information to a third party, the third party must not use technology or other means to re-identify the individuals. When dealing with sensitive information, such as financial information (e.g., E-CNY transactions in this case), personal information processors must demonstrate a specific purpose and necessity for the collection of sensitive data and shall obtain the individuals' independent consent. Article 34 specifically requires that government agencies in China only collect information needed for the course of their duties, and Section 3 generally places responsibilities and limits on government agencies when it comes to the collection, use, and sharing of citizen data.[129] In practice, it is unclear how this all works, including in relation to information collected for E-CNY. Overall, the law could have an

123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*
128. Zhonghua Renmin Gongheguo Geren Xinxi Baohu (中华人民共和国个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. of the Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), 2021 P.R.C. LAWS.
129. *Id.*

important role to play, but questions about enforcement agencies and mechanisms remain.

It is currently unclear if this law will manifest its intended purpose. Some articles are ambiguous, which could have negative impacts on protecting users' privacy. For instance, without obtaining consent from the individuals, personal information processors (in this case, it could be the PBOC and other entities distributing and circulating E-CNY) can process personal information to "carry out acts such as news reporting and public opinion oversight in the public interest."[130] This language is open to interpretation; "public opinion oversight" and "public interest" could have many different meanings. Rules like Article 13, Section 5, could give the PBOC and other relevant entities rights to process or disclose personal information in excess of needs. At this stage, there does not appear to be any oversight body or mechanism that would manage this issue with any kind of public transparency.

However, greater transparency comes with tradeoffs. More disclosures about technical details could provide more information to potential hackers and other saboteurs. A digital currency relies on digital technologies. Traditionally, nefarious actors have stolen money by counterfeiting the currency, impersonating other individuals to use their money, or by stealing currency directly (such as by robbing a bank). A digital currency changes but does not remove these risks. E-CNY will likely become a tempting target for hackers. Nefarious actors might try to attack the E-CNY infrastructure—both for reasons of counterfeiting currency as well as attacking China's financial system—and to find ways to impersonate others' digital wallets to access their digital money. There have already been publicly confirmed examples of counterfeit wallets for E-CNY.

D. *Responsibilities of Intermediaries*

Thus far, there appears to be a lack of transparency, both technical and legal, in terms of the specific expectations that the PBOC has of commercial banks and other intermediaries, particularly digital payment platforms such as Alipay and WeChat Pay. The PBOC will implement E-CNY by continuing to rely on commercial banks and other entities to distribute E-CNY. The details of how these relationships work matter, because absent clear legal or institutional changes, it is unclear how E-CNY will change the role or capacities of commercial banks.

It will also change the roles of other intermediaries, such as mobile payment platforms, telecom companies, and whatever other companies the PBOC permits to host E-CNY wallets. Will these entities adopt certain powers traditionally limited to government agencies? Commercial

130. *Id.* art. 13, § 5.

banks may be already accustomed to complying with strict and complex laws related to consumer protection and financial stability, as well as Anti-Money Laundering (AML) and Know Your Customer (KYC) laws.[131] There might be a steeper learning curve for other kinds of institutions. How will E-CNY change the relationship between the PBOC and commercial banks? How will it change the relationship between commercial banks and individual consumers and private businesses? At this stage, it is likely that the PBOC will somehow involve traditional banks, the mobile payments duopoly, and other companies in the process of E-CNY implementation and deployment, but the exact role to be played by Alipay and WeChat Pay, and the future of their relationships with the PBOC and consumers, is unclear. In an interview with the *Financial Times*, Alipay employees stated that they "do not have sufficient visibility as to the impact of the E-CNY on consumers' payment behavior and the payment industry" to understand its role at this time.[132] They stated that "it is not clear how the E-CNY will fit into or change the current digital payment industry landscape."[133] So far, it appears that the Chinese government is taking a very cautious approach to deploying E-CNY. This is likely a prudent move, but the lack of transparency is concerning.

V. ADDITIONAL LEGAL QUESTIONS SURROUNDING E-CNY

There are additional legal questions surrounding the development and deployment of E-CNY. Currently, the Chinese government has a draft update of the Law of the PRC on the People's Bank of China that would ensure that the PBOC has all due legal authority to issue a digital currency, which is slated to take effect in the spring of 2023.[134] If history

130. AML laws are "measures and procedures carried out by financial institutions and other regulated entities to prevent financial crimes." Polina Rebeka, *KYC and AML 2023—the Difference and Best Practices*, SUMSUBER (Dec. 26, 2022), https://sumsub.com/blog/kyc-and-aml/ [https://perma.cc/WX5P-MH56]. KYC laws involve "the process of obtaining information about the customer and verifying their identity." *Id.* The difference between AML and KYC laws is that "AML involves a broad range of measures, usually referred to as an AML compliance program. KYC is just one component of this program, and is therefore encompassed by AML." *Id.* AML and KYC compliance is required for entities regulated under AML/CFT (Countering the Financing of Terrorism) laws, such as financial institutions, credit institutions, e-money institutions, and other entities. *Id.*

132. Alison Tudor-Ackroyd, *What Will China's Central Bank Digital Currency Mean for Alipay and WeChat Pay?*, S. CHINA MORNING POST (Sept. 5, 2020, 10:00 AM), https://www.scmp.com/business/banking-finance/article/3100285/what-will-chinas-central-bank-digital-currency-mean-alipay [https://perma.cc/2DB5-CWV7].

133. *Id.*

134. Zhongguo Renming Yinhang Guanyu "Zhonghua Renmin Gongheguo Renmin Yinhang fa (Xiuding Gao Zhiqiu Yijian Gao)" (中國人民銀行關於《中華人民共和國人民銀行法（修訂徵求意見稿）》公開徵求意見的通知) [Notice of the People's Bank of China on

is any indication, creating a currency also involves creating a set of institutions as well as a market. As such, it might be important to further enshrine the articulation, legality, and functions of all the actors involved in E-CNY more clearly.

Anti-money laundering is an additional concern. In theory, a digital currency allows for the government to have greater insight into and control over transactions. This suggests that the government will have more tools to combat money laundering. On the other hand, like many other issues discussed above, money laundering is often not a problem of control over transaction clearing but rather of contextual intelligence and being able to confirm that the right actors are engaging in an appropriate transaction with funds that belong to them. Digital technology offers novel tools to confirm identities and prevent counterfeiting, but they are not foolproof. It is unclear at this stage how the PBOC will develop the infrastructure to confirm the prerequisite authenticity of each aspect of each transaction. Greater access to data will allow for broader analysis, but it is possible that money laundering and other forms of financial crime will remain a kind of cat and mouse game; a digital currency will change the way the game is played.

Fraud also raises potential legal challenges. All currencies face the problem of counterfeits, identity theft, and currency theft. A digital currency will likely face similar challenges. Yet, there does not appear to be a way for digital currencies and transaction-clearing mechanisms to be any "surer" of identities and funds than existing systems. More details about identity verification would help clear up some of these questions. This is a practical problem. Legally, in addition to needing to be able to prosecute fraud, governments will also need to determine who bears the pecuniary loss. In other words, who will be responsible for lost funds in the case of fraud? One of the presumed advantages of E-CNY is that the PBOC can not only remunerate victims of fraud rather inexpensively, but also undo the fraudulent transaction, thus depriving the fraudster of their illicit gains and having greater insight into who committed the fraud.[135] At this point, there currently is not an explicit policy in place.

Lastly, E-CNY has the potential to change the nature of taxation in the future. As a digital currency becomes more widespread, the government will theoretically have more information about how its

---

the Public Solicitation of Comments on the "Law of the People's Bank of the People's Republic of China (Draft for Comments)"], PEOPLE'S BANK OF CHINA (Oct. 23, 2020), http://www.gov.cn/zhengce/zhengceku/2020-10/24/content_5553847.htm [https://perma.cc/H9GY-BQ92].

135. Ahmet Faruk Aysan & Farrukh Nawaz Kayani, *China's Transition to a Digital Currency Does It Threaten Dollarization?*, 2 ASIA & GLOB. ECON. 1, 1–3 (2022); Kent Thurne, *Digital Yuan: China's Digital Currency*, SEEKING ALPHA (Oct. 6, 2022), https://seekingalpha.com/article/4453452-digital-yuan [https://perma.cc/Q7FF-VU8J].

citizens make and spend money. This will likely change the nature of tax evasion and tax investigations. It might also be able to collect taxes more directly with the use of smart contracts, rather than relying on individual actors to be honest and forthcoming about their tax obligations. But the change would require tax authorities to obtain access to the PBOC's database regarding E-CNY activities. It is too early to tell how this would occur and what procedures would need to be followed.

CONCLUSION

E-CNY is China's pioneering effort to deploy a digital currency. While other countries have also started to deploy digital currencies, the size of China's economy and the potential future scope of E-CNY indicate that the initial deployment of E-CNY could mark the beginning of a turning point for digital currencies globally. It would be wise for other sovereign central banks interested in digital currencies across the world to pay close attention to the development of E-CNY. One way or another, it will likely be impactful, both for China domestically but for the international community as well.

On that note, this Article has taken a close look at China's potential motivations and goals for issuing E-CNY. At this stage, the PBOC has a domestic agenda with a focus on solving domestic financial and social concerns. Accordingly, the potential impacts of E-CNY, at least initially, are more likely domestic. The PBOC could have greater insight into citizens' economic and financial activities, particularly in aggregate, with a clear E-CNY record. The broader deployment of E-CNY could also directly affect the duopoly of Alipay and WeChat Pay. The role of commercial banks and other intermediaries will likely remain significant, though some changes are expected. The major challenges surrounding the development and deployment of E-CNY are related to the access to and use of data, due process rights, and privacy protections. Additionally, some legal questions involving money laundering, fraud, taxation, and antitrust, remain unclear and need further attention. As described above, there remain many unanswered questions regarding the technical infrastructure of E-CNY, including but not limited to, how different it really is from existing digital money. Is the only key difference the increasingly prominent role of the PBOC, and the Chinese government more generally, in the financial system? The general lack of transparency raises more questions than it answers and suggests that the Chinese government has many reasons for hiding key details about how E-CNY works, both for reasons of security as well as obfuscating potentially unpopular motives.

Going forward, the PBOC and other entities will likely articulate new rules and understandings regarding how E-CNY and the various institutions involved in its deployment should operate. It will be important for policymakers, research scholars, and other interested parties to pay close attention to these developments from now on.

HOW TO CLOSE PANDORA'S DOX: A CASE FOR THE FEDERAL REGULATION OF DOXING

Hannah Shankman[*]

Abstract

Doxing, or the sharing of one's personally identifiable information on the Internet without consent, saw a boom during the COVID-19 pandemic. It became a way for Internet users to punish people for racist, rude, or anti-masking behavior and to quench a collective thirst for justice. While some continue to view doxing as an exercise in accountability, it is a malleable tool that can suit anyone's aim. White supremacists, neo-Nazis, and the alt-right regularly resort to doxing those with whom they disagree. Beyond the harassment, financial harm, and death threats doxing victims face, it is a tactic that is counter to foundational First Amendment values. An omnipresent threat of doxing has the potential to close the marketplace of ideas and suppress the free flow of thought.

Presently, there is no clear protection for doxing victims. Although more and more states are considering legislation and social media websites are attempting to self-regulate, the present mechanisms remain inadequate. Jurisdictional issues, First Amendment concerns, and Section 230 of the Communications Decency Act present huge barriers to effective regulation. Doxing victims pay the price and are left without clear recourse. For these reasons, this Article argues that the federal government must pass anti-doxing legislation to adequately protect against the tactic. This Article proposes a piece of model legislation that addresses doxing's unique features and First Amendment concerns.

INTRODUCTION

You may remember the video. It was posted May 25, 2020—the first summer of the COVID-19 pandemic and on the same day as the murder of George Floyd.[1] The video began with a white woman who picked up a dog by its collar in what looked to be a park.[2] She walked toward the camera and asked the person recording her to stop.[3] The voice behind the camera responded, "Please don't come close to me."[4] At this point, about twenty seconds into the video, things took a turn. The woman proceeded to let the man know that she was going to call the police.[5] She stated, "I am going to tell them that there is an African American man threatening

---

* J.D. 2022, The George Washington University Law School; B.A. 2017, Binghamton University, State University of New York. I would like to thank Professor Dawn C. Nunziato for her guidance and support, my seminar classmates for their encouragement and feedback, and my mother, Julie Shankman, for everything.

1. Megan Phelps-Roper, *The Real Story of "The Central Park Karen*," COMMON SENSE (Aug. 3, 2021), https://bariweiss.substack.com/p/the-real-story-of-the-central-park?s=r [https://perma.cc/9P78-D3UK]. Megan Phelps Roper was raised in the Westboro Baptist Church, which was founded by her grandfather. The church is known for publicly protesting "vices" such as homosexuality, and the church gained notoriety in the 2000s for protesting at the funerals of American soldiers who died in the War in Afghanistan and the War in Iraq. *See* Snyder v. Phelps, 562 U.S. 443, 448 (2011) ("The [Westboro Baptist Church] frequently communicates its views by picketing, often at military funerals. In the more than 20 years that the members of Westboro Baptist have publicized their message, they have picketed nearly 600 funerals."). Ms. Phelps-Roper left the Westboro Baptist Church in 2012 after she began to disagree with the church's teachings. She cites engaging in open dialogue with others on Twitter as the impetus for her changed views. *See* MEGAN PHELPS-ROPER, UNFOLLOW: A MEMOIR OF LOVING AND LEAVING THE WESTBORO BAPTIST CHURCH *passim* (2019).

2. Tamar Lapin, *Video of White Woman Calling Cops on Black Man in Central Park Draws Outrage*, N.Y. POST (May 25, 2020, 8:36 PM), https://nypost.com/2020/05/25/video-of-white-woman-calling-cops-on-black-man-in-central-park-draws-outrage/ [https://perma.cc/428F-4CX6].

3. *Id.*

4. *Id.*

5. *Id.*

my life."[6] She then called the police and said over the phone that an African American man is recording her and threatening her and her dog.[7]

This minute long video was posted to Twitter and went viral.[8] The caption that accompanied the tweet referred to the woman as a "Karen"[9] and informed viewers that this interaction occurred because the man recording asked the woman to comply with Central Park's rules and place her dog on a leash in the Ramble.[10] Twitter users that reposted, commented, and replied to the video were outraged by the white woman weaponizing the man's race against him to the police and deemed her behavior racist.[11]

To quote one user:

> The way she tried to first evoke fear in him by telling him what she was going to say. She knew that those words were a threat to his life. And then she turned around and did it, with increasing faux urgency. While her dumbass was being filmed. White supremacy is a sickness.[12]

Shortly after the video was posted, the Internet[13] identified the woman

---

6. *Id.*

7. *Id.*

8. The Associated Press, *Video Shows White Woman Calling Police on Black Man in Central Park*, N.Y. TIMES (May 27, 2020), https://www.nytimes.com/video/us/100000007159234/amy-cooper-dog-central-park-police-video.html [https://perma.cc/4VRM-T4HQ]. At the time of this Article, the video had been viewed 45 million times on Twitter alone. *See* Troy Closson, *Amy Cooper Falsely Accused Black Bird-Watcher in 2nd 911 Conversation*, N.Y. TIMES (May 26, 2021), https://www.nytimes.com/2020/10/14/nyregion/amy-cooper-false-report-charge.html [https://perma.cc/5S9V-JDKM].

9. "Karen" is a term used to refer to white women that are seen as entitled or rude. Elle Hunt, *What Does It Mean to Be a 'Karen'? Karens Explain*, GUARDIAN (May 13, 2020), https://www.theguardian.com/lifeandstyle/2020/may/13/karen-meme-what-does-it-mean [https://perma.cc/85NK-BS6B].

10. Lapin, *supra* note 2. The Ramble is one area within Central Park, located in New York City, New York.

11. *See, e.g.*, Dr. Shola Mos-Shogbamimu (@SholaMos1), TWITTER (May 26, 2020, 3:03 AM), https://twitter.com/SholaMos1/status/1265176663194841090 [https://perma.cc/FV9R-F4WP] ("Can't express how angry and horrified I am by this RACIST. I'm so glad your brother is OK. This evil against black people must end. Thank you for making this public. Anyone offended by the use of 'Karen' can go rot! #AmyCooper is Karen personified and a #WhiteSupremacist."). Users were also alarmed by the way the woman was handling the dog. *See Tweet*, TWITTER, https://twitter.com/melodyMcooper/status/1264965252866641920?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1264965252866641920%7Ctwgr%5Eshare_3&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2020%2F05%2F26%2Fnyregion%2Famy-cooper-dog-central-park.html [https://perma.cc/M5VF-8SNH] (last visited May 12, 2023).

12. SUMMER'S RENAISSANCE (@EssBreezyBaby), TWITTER (May 25, 2020, 4:39 PM), https://twitter.com/EssBreezyBaby/status/1265019761462775813.

13. At the time of this Article, it is unclear who was the first person to release Amy Cooper's name on the Internet. This is common with instances of doxing, and this Article will discuss this issue in Section I.B.

in the video as Amy Cooper.[14] Within hours of the video's release, her personal phone number and address were posted as well.[15] She started to receive death threats, hundreds of phone calls, and graphic messages.[16] Later that night, a crowd gathered outside her apartment to show their displeasure, and within two days, Franklin Templeton fired Amy from her position at the investment firm.[17] The result of this interaction in the park? Amy Cooper was doxed.

Doxing[18] is a type of cyber-harassment.[19] It involves the online public release of personal information that can be used to identify or locate an individual, usually without the individual's consent.[20] Additionally, there is an unspoken message behind the release of this information: harass the named individual.[21]

You may be wondering: "Why should I care? Amy is merely being held accountable for her racist actions. This is in the public's interest." After experiencing a summer that dealt with a long-overdue racial reckoning, and years of people's repeated refusal to comply with masking measures during a pandemic, an apathy toward a person being doxed and subsequently fired for racist behavior is reasonable. And you would not be alone in this sentiment: since the summer of 2020, viral videos of individuals saying racist things or yelling at employees over being asked to wear a mask inside have become all too common.[22] Consequently, entire TikTok pages dedicated to identifying the people who transgressed in these videos have sprung up and generated millions of views.[23] It seems society has developed a collective thirst for accountability and justice.

---

14. Daniel Johnson, *'Central Park Karen' Defends Her Actions in First Interview Since Fleeing U.S.*, NAT'L POST (Aug. 5, 2021), https://nationalpost.com/news/central-park-karen-defends-her-actions-in-first-interview-since-fleeing-u-s [https://perma.cc/A96T-GZDJ].

15. *Id.*

16. *Id.*

17. *Id.*; Lisette Voytko, *Amy Cooper Fired After Viral Central Park Video*, FORBES (May 27, 2020, 1:09 PM), https://www.forbes.com/sites/lisettevoytko/2020/05/26/amy-cooper-fired-after-viral-central-park-video/?sh=1377333f5c53 [https://perma.cc/N556-CWWA] ("'We have made the decision to terminate the employee involved.' Franklin Templeton wrote on its official Twitter account, adding, 'We do not tolerate racism of any kind.'").

18. Doxing is also sometimes spelled "doxxing."

19. Hannah C. Mery, *The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment*, 52 ST. MARY'S L.J. 905, 911 (2021).

20. Alexander J. Lindvall, *Political Hacktivism: Doxing & the First Amendment*, 53 CREIGHTON L. REV. 1, 2 (2019).

21. *Id.*

22. *See* Richard Tribou, *Florida Man Without Mask Seen Shouting at Costco Fired from Job*, ORLANDO SENTINEL (July 8, 2020, 7:16 AM), https://www.orlandosentinel.com/news/florida/os-ne-florida-man-without-mask-costco-video-fired-from-job-20200708-s2o767gqzbetljip7w5h7tdiqi-story.html [https://perma.cc/P8KX-5QC4].

23. *See* TizzyEnt (@tizzyent), TIKTOK, https://www.tiktok.com/@tizzyent [https://perma.cc/J5VW-LQWR]; Danesh (@thatdaneshguy), TIKTOK, https://www.tiktok.com/@thatdaneshguy?lang=en [https://perma.cc/U529-Q9M8].

Posting people's names, places of employment, addresses, and phone numbers provides a mechanism to quench this thirst.

While doxing is a way to punish people for their perceived crimes,[24] the sentence that results can be lifelong and severe.[25] Doxing has repeatedly led to death threats, harassment, and job loss for those that are doxed.[26] As reporter Zeeshan Aleem points out, job loss is especially harsh in the American social scheme because there is a weak social safety net, and it often results in the additional loss of one's health care.[27] Further, a person who is doxed often becomes "radioactive" on the job market and unhirable down the line.[28] With the doxers playing the judge, jury, and executioner based on minute-long videos, we as a society need to reckon with whether this punishment tactic should be permitted to continue.

This question becomes even more poignant when you consider doxing's malleability. It is a tool that can be used by any group to suit any aims. Indeed, the Amy Coopers of the world are not the only people that are doxed. White supremacists, neo-Nazis, and the alt-right have regularly resorted to doxing people whose views they disagree with.

Damon Young, a black writer, editor, and critic for *The New York Times*, *The Washington Post*, and *GQ*, is one example. He was doxed by white supremacists after he published an article, "Whiteness Is a Pandemic," about the March 2021 Atlanta shooting of six Asian women.[29] Tanya Gersh, a Jewish real estate agent from Whitefish, Montana, is another.[30] She had her phone number published on the *Daily Stormer*, a

---

24. Dylan E. Penza, *The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States Can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 304 (2018) ("Many 'doxxers' see this behavior as a form of vigilante justice wherein they reveal the information of people in order to punish them for perceived crimes.").

25. Johnson, *supra* note 14 (Amy Cooper has since left the United States and lives in undisclosed foreign country. She states that she "wishes to move to a non-english speaking country where the story did not run.").

26. *Cancel Culture, Part 2: A Case Study*, N.Y. TIMES (Aug. 11, 2020) [hereinafter *Cancel Culture*], https://www.nytimes.com/2020/08/11/podcasts/the-daily/cancel-culture.html [https://perma.cc/X926-YDV2].

27. *Id.*

28. *Id.*

29. Damon Young, *The Second Best Thing About Getting Doxed by White Supremacists*, WASH. POST (Jan. 31, 2022), https://www.washingtonpost.com/magazine/2022/01/31/damon-young-second-best-thing-about-getting-doxed-by-white-supremacists/ [https://perma.cc/3ATD-V5T4][hereinafter *The Second Best Thing*]; Damon Young, *Whiteness Is a Pandemic*, ROOT (Mar. 17, 2021, 1:00 PM), https://www.theroot.com/whiteness-is-a-pandemic-1846494770 [https://perma.cc/96JZ-B57L] [hereinafter *Whiteness*].

30. Elizabeth Williamson, *How a Small Town Silenced a Neo-Nazi Hate Campaign*, N.Y. TIMES (Nov. 8, 2021), https://www.nytimes.com/2021/09/05/us/politics/nazi-whitefish-charlottesville.html [https://perma.cc/7T7E-37XR].

popular neo-Nazi website, after she was involved with a real estate dispute with the mother of Richard B. Spencer, a white nationalist alt-right leader.[31] Female video game developers Zoe Quinn and Brianna Wu, and feminist media critic Anita Sarkeesian, are other examples.[32] They were doxed and suffered years-long misogynistic online harassment, including death threats and threats of rape, because they advocated for more inclusivity in video games in the cultural phenomenon now known as "GamerGate."[33] The list of those doxed by white supremacists goes on and on.

Given these realities, this Article argues that doxing poses a substantive harm and should be regulated by the federal government. Not only can doxing lead to intimidation, harassment, financial harms, and leave those who are doxed fearing for their life, it is a tactic that doxers can use to entirely stifle speech. Eleven states have recognized this danger and passed doxing prohibitions or strengthened existing laws to include this tactic, and three more states are currently considering doxing legislation.[34] However, state regulation is inadequate. These Internet interactions rarely happen entirely within state lines, and perpetrators are likely beyond the reach of a state court's jurisdiction. This Article argues that the federal government needs to pass anti-doxing legislation to adequately protect against the tactic.

This Article proceeds in five parts. Part I provides a general definition of doxing and discusses specific aspects of the tactic that make it unique. This part includes a discussion of First Amendment issues as they pertain to doxing's regulation. Part II outlines the ways doxing could be regulated, including self-regulation by social media websites, state by state regulation, and federal legislation. Part III then explains why federal legislation provides the best chance to combat doxing. Next, Part IV provides a model piece of federal legislation, and explains why the proposed legislation would likely survive a First Amendment challenge. Finally, Part V concludes.

---

31. *Id.*; *Richard Bertrand Spencer*, S. POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/individual/richard-bertrand-spencer-0 [https://perma.cc/SJ5B-69QG] (last visited Mar. 18, 2022).

32. Caitlin Dewey, *The Only Guide to Gamergate You Will Ever Need to Read*, WASH. POST (Oct. 14, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/14/the-only-guide-to-gamergate-you-will-ever-need-to-read/ [https://perma.cc/4FGX-UWLH].

33. *Id.*

34. Emma Betuel, *Should Doxing Be Illegal?*, MARKUP (Aug. 17, 2021, 8:00 AM), https://themarkup.org/ask-the-markup/2021/08/17/should-doxxing-be-illegal [https://perma.cc/6GQ7-UH2H].

I. DEFINING DOXING AND ITS UNIQUE FEATURES

Though doxing entered mainstream channels over ten years ago[35] and has seen a boom in the last five years,[36] most attribute the origins of the tactic to hackers in the 1990s.[37] Hackers would post fellow users' personal information as a means of retaliation during an argument.[38] The term "dox" comes from the abbreviated form of documents: "docs."[39] It is a nod to the fact that Internet users could use documents to reveal a formerly anonymous person's identity.[40] Users would then "drop" the documents to reveal one's identity.[41] Over time, this methodology took on the term "doxing."[42]

A. *Doxing: Toward a General Definition*

Today, legislators and academics define the term as sharing someone's "personal information" or "personally identifiable information" on the Internet.[43] These definitions also recognize a certain intent on behalf of the doxer. To constitute doxing, the doxer must intend a level of harassment toward the target by releasing their information.[44] The doxer can either intend to cause this harassment themselves or simply serve as a facilitator and leave the harassment to those that view the posted information.[45]

Definitions of doxing tend to use the broad term "personally identifiable information" because each instance does not necessarily involve the same release of information.[46] While, at a minimum, doxing involves the online publication of a target's full name, the additional information that

35. Megan Garber, *Doxing: An Etymology*, ATLANTIC (Mar. 6, 2014), https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/ [https://perma.cc/T2F5-VZPM].

36. Nellie Bowles, *How Doxing Became a Mainstream Tool in the Culture Wars*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html [https://perma.cc/L9RE-E9RS].

37. Garber, *supra* note 35.

38. *Id.*

39. *Id.*

40. *Id.*

41. Michelle Park, *The Doxing Guide: What It Is, Statistics, Legality, and Prevention*, GARBO (Aug. 16, 2021), https://www.garbo.io/blog/doxing [https://perma.cc/K8KY-FJNH].

42. Garber, *supra* note 35.

43. *See* Lisa Bei Li, *Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting*, 70 FED. COMMC'NS L.J. 317, 326 (2018); Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

44. Lindvall, *supra* note 20, at 8; Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

45. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

46. Svana Calabro, *From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting*, 51 SUFFOLK U. L. REV. 55, 67 (2018).

is released beyond one's name varies. It can include phone numbers, work and home addresses, emails, social security numbers, employer contact information, or some combination of this information.[47] Put simply, there is not one uniform way doxers dox; therefore, the definition is intentionally broad to capture each variation.

Legislators and academics also consider doxing a type of "cyber-harassment."[48] It is typically grouped with cyber-stalking, cyber-bullying, and swatting because there is significant overlap between these acts' definitions.[49] For example, cyber-stalking is where a perpetrator uses social media, Internet databases, and other online resources to repeatedly intimidate, terrorize, threaten, or cause fear in another person.[50] Often, the cyber-stalker is personally acquainted with their victim, and in many cases, the perpetrator and victim had a romantic relationship.[51]

Similarly, cyber-bullying is defined as "the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature,"[52] and "the electronic posting of mean-spirited messages about a person (such as a student) often done anonymously."[53] Swatting is another variation of cyber-harassment.[54] It is where a person falsely reports an emergency at a victim's home—such as a hostage situation or active shooter—to bait the police into sending a Special Weapons and Tactics (SWAT) team to the victim's home.[55] The idea is the SWAT team will enter the target's home with guns drawn, and at a minimum, terrify the unsuspecting victim.[56]

Doxing is similar to these other forms of cyber-harassment because they all have goals of instilling fear, causing intimation, and harassing the target. However, as the tactic currently stands, doxing contains a few

47. Patricia R. Recupero, *New Technologies, New Problems, New Laws*, 44 J. AM. ACAD. PSYCHIATRY & L. 322, 325 (2016); Lindvall, *supra* note 20; Dylan E. Penza, *The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States Can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 303–04 (2018).

48. Penza, *supra* note 47; Calabro, *supra* note 46; *Clark Bill Criminalizes Malicious Publication of Private Information*, KATHERINE CLARK 5TH DIST. OF MASS. (Dec. 8, 2016), https://katherineclark.house.gov/press-releases?ID=845879BE-5C95-4115-A5ED-A4BD79CA611B [https://perma.cc/Y3E3-PFEN].

49. Penza, *supra* note 47; Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, 40 AM. J. TRIAL ADVOC. 41, 43 (2016).

50. Sameer Hinduja, *Cyberstalking*, CYBERBULLYING RSCH. CTR., https://cyberbullying.org/cyberstalking [https://perma.cc/4BRP-2ATU] (last visited May 13, 2023).

51. Vasiu & Vasiu, *supra* note 49.

52. *Cyberbullying*, OXFORD DICTIONARY (3d ed. 2010).

53. *Cyberbullying*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/cyberbullying [https://perma.cc/267B-TJKA] (last visited May 13, 2023).

54. Penza, *supra* note 47, at 304.

55. *Id.* at 304 n.50; Calabro, *supra* note 46, at 60.

56. *See* Calabro, *supra* note 46, at 56 (describing the 2016 swatting of Congresswoman Katherine Clark).

unique qualities that distinguishes it from other forms of cyber-harassment. These distinctive features are important to keep in mind when thinking about how to appropriately address doxing.

B. *Doxing's Unique Features*

The main unique features of doxing are the: (1) semi-public nature of the information released by doxers; (2) doxing's accountability feature; (3) the involvement of multiple actors; and (4) free speech concerns. Notably, these are also the main themes that underscore many of the arguments against doxing regulation.[57] This section will address each in turn.

1. The Information Is Already Public

First, the information that is released in a doxing episode has a varying degree of "publicness."[58] Home addresses can be found with a quick search online through "whitepages.com" or "peoplefinder.com,"[59] and doxers are often using public information that does not require a hack to access.[60] Rather, doxers are simply gathering information from sites like LinkedIn, Facebook, or Google.[61] For this reason, some argue that legislators should not regulate doxing, as perpetrators only use a victim's public information.[62] As the Supreme Court noted in *Cox Broadcasting Corp. v. Cohn*, "interests in privacy fade when the information involved already appears on the public record."[63]

These are valid concerns; yet, focusing on the nature of information ignores a few important points. For one, there is a difference between personally identifiable information existing on the Internet as various independent data points, and a post curated to host all of one's personally identifiable information in one place.[64] The latter presents a level of accessibility, to the millions of people on the Internet, to whom this information was not previously available. And this is all done without the con-

57. I would like to thank my peers for raising many of these concerns while I was writing this Article.

58. Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2456 (2017).

59. *See* Nicole Levine, *How to Find a Current Address for Someone*, WIKIHOW (Mar. 15, 2022), https://www.wikihow.com/Find-a-Current-Address-for-Someone [https://perma.cc/W6ZP-U48M] (describing what online websites to use to find a person's address).

60. MacAllister, *supra* note 58.

61. Zaraki Kenpachi, *How to Dox Someone on TikTok*, SELFOY (Jan. 5, 2022), https://selfoy.com/how-to-dox-someone-on-tiktok-know-more-about-it/ [https://perma.cc/CS9B-V4GG].

62. MacAllister, *supra* note 58, at 2458.

63. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–95 (1975).

64. MacAllister, *supra* note 58, at 2458.

sent of the person to whom the information belongs. A doxing post fundamentally concentrates and alters the nature of the information. It turns it into a weapon that can be used by anyone who views it.

Furthermore, not all the information doxers release is publicly accessible.[65] For example, personal cell phone numbers are not generally considered part of the public record, and social security numbers are clearly private.[66] To say that doxing strictly involves public information is an overstatement.

Lastly, prohibitions against doxing are not solely rooted in the "interest in privacy" or in the "zone of privacy that surrounds every individual" that is discussed in *Cox Broadcasting*.[67] Rather, proposed doxing regulations are also focused on the malicious and threatening intent of the doxer in posting the target's information.[68] While doxing arguably invades the privacy of the victim, doxers are also using this information—both public and private—to *intentionally* cause serious financial and reputational harms, emotional distress, death threats, and sustained harassment and intimidation.[69] This should help distinguish doxing from other privacy cases where the Supreme Court has said protections were limited because of the public nature of information.

2. A Good Faith Dox?

Next, some argue doxing is not qualitatively the same as other forms of cyber-harassment. Unlike cyber-stalking or cyber-bullying, where malignant aims are foundational to the perpetrator's goals, a doxer may not consider themselves as holding a malicious intent.[70] Doxers could view themselves as seeking justice and holding those that transgress accountable.[71] Popular TikTok users hold this view and portray themselves as engaging in a type of "good faith" awareness campaign.[72]

---

65. Park, *supra* note 41.

66. Frayda Bluestein, *Are Cell Phone Bills Public Records*, COATES' CANNONS NC LOC. GOV'T L. (Oct. 5, 2011), https://canons.sog.unc.edu/2011/10/are-cell-phone-bills-public-records/ [https://perma.cc/M3CB-H6RK].

67. *Cox Broad. Corp.*, 420 U.S. at 487.

68. Lindvall, *supra* note 20, at 5.

69. Penza, *supra* note 47, at 305–08; *Cancel Culture*, *supra* note 26.

70. Penza, *supra* note 47, at 304.

71. *Id.*

72. Ryan Broderick, *TikTok Drama Channels Are Turning into Online Intelligence Agents*, VERGE (Dec. 6, 2021, 8:30 AM), https://www.theverge.com/22809838/tiktok-drama-channels-osint-antivaxx-doxxing-creators [https://perma.cc/MYC5-9VBD] ("[Michael] Mc told *The Verge* he's trying to bring some accountability back to how people behave on the internet."); Penza, *supra* note 47, at 304 n.45 ("Perhaps the most well known recent case of doxxing as vigilante justice took place after the white supremacist rally in Charlottesville last August, where in internet users, most notably Twitter user @YesYoureRacist tried to release the identities of those who attended the rally.").

This nuance is particularly relevant when a person is doxed after a video of them acting in a racist manner goes viral, and Internet users subsequently contact the person's place of employment. Returning to the case of Amy Cooper highlights this point. Many would argue that Franklin Templeton *should* have the ability to terminate a racist employee, and the doxers are simply bringing this information to the employer's attention. One may argue that doxing should be permitted because it provides this ability to bring awareness to transgressions.

These concerns are easily addressed by a well-drafted statute. A doxing statute could limit the prohibition to the *malicious* publication of personally identifiable information.[73] A statute could then define malicious publication as the posting of such information with the intent to "threaten, intimidate, harass, stalk."[74] Adding this mal-intent requirement would help distinguish between doxing that is premised on causing harm and socially beneficial forms of online identification.[75] The intent precondition creates a needed balance: barring doxing rooted in harassment while permitting good faith awareness campaigns.

Of course, there may be cases where it is questionable whether the doxers are genuinely engaged in a "good faith" awareness campaign. In such instances, the court would have to judge the behavior on a case-by-case basis and look at the surrounding context to determine if the necessary mal-intent was present. Proving the necessary intent is common feature of the American legal system, and such an inquiry for doxing would be no different.

3. Multiple Actors and Different Roles

Doxing rarely involves the action of a singular perpetrator.[76] A doxing campaign usually comprises action on behalf of multiple actors collectively partaking in different roles: some releasing the personally identifiable information, some contacting the victim, and others engaging in both genres of action.[77] This creates the question of who involved in the tactic should be held liable and what behaviors should trigger liability.

Again, this difficulty could be solved by the drafting of the doxing statute. The statute could attach liability for the person that initially posts personally identifiable information as well as for people who facilitate,

---

73. MacAllister, *supra* note 58, at 2457–59.

74. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).

75. *Doxing Should Be Illegal. Reporting Extremists Should Not*, AM. DEFAMATION LEAGUE (Jan. 15, 2021), https://www.adl.org/blog/doxing-should-be-illegal-reporting-extremists-should-not [https://perma.cc/E9CM-ANAX].

76. MacAllister, *supra* note 58.

77. MacAllister, *supra* note 58, at 2474 (stating that actors can work together in a "cybermob," with "one poster starting the abuse and others piling on").

assist, or promote the posting of such information.[78] This additional liability for the facilitation of doxing would help capture the "conspiratorial" doxers—the individuals who are not necessarily the initial poster. There may still be questions surrounding the identity of the defendant, but these are tactical questions that plaintiffs and prosecutors must regularly decide based on available evidence. Nevertheless, the suggested statutory language would provide victims the opportunity for recourse in the common scenario when there is not one sole doxer.[79]

4. First Amendment Free Speech Concerns

Lastly, doxing implicates concerns rooted in the freedom of expression. The first free speech concern is that the public can use doxing, or the threat of doxing, to stifle speech. Individuals could dox those with whose viewpoints they disagree instead of responding with alternative narratives or counter speech. Gamergate and Damon Young's doxing are examples of this.[80] The women of Gamergate were doxed after criticizing the video game culture and advocating for greater inclusion for women in the video game field.[81] Writer Damon Young was doxed after critically analyzing how whiteness, and white supremacy, led to the March 16, 2021, murders of six Asian American women in Atlanta.[82]

If people must be concerned about the release of their personally identifiable information and the inevitable harassment that follows when they share opinions, they may become reluctant to share their points of view. This is concerning because an "open marketplace" of ideas is central to the First Amendment and to democracy.[83] An omnipresent threat of doxing has the potential to close the marketplace and suppress the free flow of thought. This is counter to foundational First Amendment values and provides another reason why doxing should be regulated.

The second concern centers on the doxing post itself: doxers argue their posts are protected free speech.[84] While doxing is speech,[85] and the

78. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016); L.B. 227, 107th Leg., 1st Sess. (Neb. 2021).

79. Betuel, *supra* note 34.

80. Dewey, *supra* note 32; *The Second Best Thing*, *supra* note 29.

81. Dewey, *supra* note 32.

82. *The Second Best Thing*, *supra* note 29.

83. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969).

84. *See* Gersh v. Anglin, 353 F. Supp. 3d 958, 963 (D. Mont. 2018) ("Anglin contends that his motion to dismiss should be granted because the speech giving rise to Gersh's claim enjoys First Amendment protection. He argues that: (1) the speech does not fall within an unprotected category; and (2) the speech involved both a matter of public concern.").

85. *See* Brush & Nib Studio, LC v. City of Phoenix, 448 P.3d 890, 905 (Ariz. 2019) ("Pure speech includes written and spoken words, as well as other media such as paintings, music, and film 'that predominantly serve to express thoughts, emotions, or ideas.'").

First Amendment prevents Congress and the states from enacting any law that abridges the freedom of speech,[86] the analysis of whether First Amendment protections apply in these cases is not necessarily that cut and dry. For one, protections do not apply when the government restricts "unprotected" speech,[87] such as obscenity,[88] true threats,[89] fighting words,[90] or incitement.[91] In instances of these categories of speech, the government is free to restrict its use. The Court has also emphasized that the level of First Amendment protection depends on the public significance of the speech.[92] For speech on matters of private concern, "First Amendment protections are often less rigorous."[93] Comparatively, matters of public concern are at the heart of the First Amendment and strongly protected.[94]

While the First Amendment also prevents the government from regulating speech based on its content or the viewpoints expressed,[95] courts have upheld statutes that regulate speech based on content.[96] To be clear, statutes containing content-based restrictions are considered especially pernicious, presumptively invalid,[97] and must survive the often-fatal inquiry of "strict scrutiny,"[98] but it has been done.[99] To do so, the government must show the statute serves a compelling interest, and that the government has regulated the speech by the least restrictive means.[100]

In evaluating the constitutionality of a doxing regulation, a court would first need to determine whether doxing constitutes unprotected or protected speech.[101] Some academics have argued that doxing could fall into the true threat exception and constitute unprotected speech.[102] After

86. U.S. CONST. amend. I.
87. Nev. Comm'n on Ethics v. Carrigan, 564 U.S. 117, 121 (2011).
88. Miller v. California, 413 U.S. 15, 22 (1973).
89. Watts v. United States, 394 U.S. 705, 708 (1969).
90. Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942).
91. Brandenburg v. Ohio, 395 U.S. 444, 449 (1969).
92. Snyder v. Phelps, 562 U.S. 443, 451–52 (2011).
93. *Id.* at 452.
94. *Id.* at 451–52.
95. City of Los Angeles v. Alameda Books, Inc., 353 U.S. 425, 434 (2002).
96. *See* Burson v. Freeman, 504 U.S. 191, 193, 211 (1992) (holding that a Tennessee statute "prohibit[ing] the solicitation of votes and the display or distribution of campaign materials within 100 feet of the entrance to a polling place" survived strict scrutiny and was constitutional under the First Amendment).
97. *Alameda Books, Inc.*, 353 U.S. at 434.
98. *Id.* at 434.
99. *See, e.g.*, *supra* note 96.
100. *Id.* at 455.
101. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790, 799 (2011).
102. *See* MacAllister, *supra* note 58, at 2465 ("The exception most relevant to this Note's effort to find a remedy for doxing is the 'true threat' exception."); Lindvall, *supra* note 20, at 5 ("These [doxing] statutes' mens rea requirements should allow them to fall into the First Amendment's true-threats exception.").

all—like a threat—doxing and the harassment that follows can cause a victim to fear impending violence, bodily harm, or death. It is unclear whether this argument would be convincing for a court. The Supreme Court has limited true threats to instances where "the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals."[103] Though true threats may be implied,[104] a "threat" is premised on actions yet to come. A threat articulates acts the speaker has "intent to commit."[105] With doxing, part of the harm has already occurred when the doxer posts the personally identifiable information. For this reason, and the limited scope of the true threats doctrine, it is far from certain a court would consider doxing a true threat.

Nonetheless, even if a court determined doxing was protected speech, the inquiry would not end. Speech protected by the First Amendment can still be constitutionally regulated if the regulation passes intermediate or strict scrutiny.[106] Strict scrutiny applies when the speech is content based, and intermediate scrutiny applies when the speech is content neutral.[107] A court is likely to consider an anti-doxing statute to be content based. As the Supreme Court has noted, "[g]overnment regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed."[108] An anti-doxing statute is content based because it will regulate based on the type of information the perpetrator releases: personally identifiable information.

Consequently, an anti-doxing statute would likely need to pass strict scrutiny for a court to uphold the regulation. While often fatal, an anti-doxing statute may be able to survive strict scrutiny if the statute closely connects doxing to matters of private concern. Speech on purely private matters "does not carry as much weight in the strict scrutiny analysis as speech concerning matters of public concern."[109] Courts have been willing to find compelling government interests and uphold content-based statutes in instances of non-consensual pornography (NCP).[110] A doxing

103. Virginia v. Black, 538 U.S. 343, 359 (2003).

104. Nat'l Coal. on Black Civic Participation v. Wohl, 498 F. Supp. 3d 457, 479 (S.D.N.Y. 2020).

105. *Black*, 538 U.S. at 359.

106. Holder v. Humanitarian L. Project, 561 U.S. 1, 27–28 (2010).

107. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989); Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

108. *Reed*, 576 U.S. at 163.

109. State v. VanBuren, 214 A.3d 791, 808 (Vt. 2019).

110. *See id.* at 794 (upholding the constitutionality of a Vermont statute banning disclosure of NCP); State v. Casillas, 952 N.W.2d 629, 634 (Minn. 2020) (finding that a Minnesota statute criminalizing the non-consensual dissemination of private sexual images did not violate the First Amendment because it survived strict scrutiny); State v. Katz, 179 N.E.3d 431, 439 (Ind. 2022)

statute modeled on these NCP statutes, too, could be upheld. Therefore, arguing doxing constitutes "free speech" does not end the inquiry surrounding regulation—an anti-doxing statute could be carefully crafted to pass strict scrutiny. This Article will provide one such statute but will first discuss why doxing-specific legislation is the best way to regulate the tactic.

II. WAYS TO COMBAT DOXING

There are a few possible ways to address doxing. First, social media sites could regulate the practice on their own. Second, states could either let traditional tort law handle the practice, or they could decide to pass legislation and attach criminal or civil liability to doxing. Finally, Congress could enact federal legislation to proscribe doxing. As described below, federal criminal legislation is the optimal option because this would avoid the jurisdictional issues involved with state statutes, protect citizens in every state against the tactic, and provide the best chance for an exception to Section 230 immunity.

A. *Regulation by Social Media Companies*

Self-regulation by social media sites is a logical place to begin the inquiry of how to address doxing. Doxing tends to occur on these websites, and many social media websites already have policies in place concerning the practice.[111] For example, Twitter prohibits posting a person's home address or physical location information; identity documents; contact information, "including non-public personal phone numbers or email addresses"; financial account information; and biometric data without permission from whom the information belongs.[112] Tweets containing such information may be removed, and the perpetrator's Twitter account may be suspended.[113]

Similarly, Meta, the media conglomerate that is the parent company to Instagram and Facebook, prohibits doxing.[114] Specifically, Meta pro-

(holding that a Indiana statute criminalizing the non-consensual distribution of an intimate image was constitutional).

111. *See, e.g.*, *Private Information and Media Policy*, TWITTER HELP CTR., https://help.twitter.com/en/rules-and-policies/personal-information [https://perma.cc/W8L2-72H3] (last visited May 13, 2023) ("Sharing someone's private information online without their permission, sometimes called doxxing, is a breach of their privacy and of the Twitter Rules.").

112. *Id.*

113. *Id.*

114. *Privacy Violations*, META TRANSPARENCY CTR., https://transparency.fb.com/policies/community-standards/privacy-violations-image-privacy-rights/ [https://perma.cc/P5K3-6CZJ] (last visited Apr. 29, 2023) (stating that Facebook removes "content that shares, offers or solicits

hibits sharing or soliciting government-issued numbers related to personal identity, such as social security or passport numbers, private contact information like phone numbers, physical addresses, email addresses, and financial information.[115]

Finally, TikTok does not permit doxing on its platform.[116] TikTok's community guidelines define doxing as the act of "collecting and publishing personal data or personally identifiable information (PII) for malicious purposes."[117] The site goes on to define PII as including "residential address, private email address, private phone number, bank statement, social security number, or passport number."[118]

Though the most popular social media sites have policies against doxing, users on the platform are at the mercy of the social media site. This means users are subject to the site's determination of what constitutes doxing and what does not, as well as the site's removal decision. To have any social media post taken down, a user must often first "report" a post.[119] The social media site then evaluates the post and decides whether the content violates its "community guidelines" or "rules" before it takes

---

personally identifiable information or other private information that could lead to physical or financial harm, including financial, residential, and medical information, as well as private information obtained from illegal sources"); *Exposed Private Information*, INSTAGRAM HELP CTR., https://www.facebook.com/help/instagram/122717417885747 [https://perma.cc/5VY2-DGCB] (last visited Apr. 29, 2023) ("Posting private and confidential information is a violation of our Terms of Use. Private and confidential information includes, but isn't limited to, credit card information, social security or alternate national identity numbers, private address or location information, non-public phone numbers and non-public email addresses.").

115. *Privacy Violations*, *supra* note 114. Meta recently strengthened its doxing policy after its oversight board—the governing body in charge of Facebook's and Instagram's content decisions—recommended it do so. The updated policy against doxing no longer permits users to share private residential information, even when the information was publicly available online. *See* Meera Navlakha, *Meta Won't Let People Share Private Home Information Anymore*, MASHABLE (Apr. 11, 2022), https://mashable.com/article/meta-private-residential-home-information-doxxing#:~:text=The%20policy%20change%20will%20further%20protect%20victims%20of%20doxxing.&text=Meta%20will%20no%20longer%20allow,information%20is%20publicly%20available%20online [https://perma.cc/N3EL-L46Q].

116. *Community Guidelines*, TIKTOK, https://www.tiktok.com/community-guidelines?lang=en [https://perma.cc/9NGG-HX9E] (last updated Mar. 2023).

117. *Id.*

118. *Id.*

119. Due to the vast volume of content posted on social media websites, most sites have their own automated content evaluation in addition to flagging by users. *See* Rep. of the Special Rapporteur on the Promotion & Prot. of the Right to Freedom of Op. & Expression, U.N. Doc. A/HRC/38/35, at 12 (2018) [hereinafter Rep. of the Special Rapporteur]. This means sites are regularly evaluating content without any prompting. *See id.* However, the algorithms used to automatically moderate content have raised concerns of "overblocking," and given the volume of content generated on a social media site, these algorithms are unable to capture every violation of the site's guidelines. *See id.*; *see Privacy Violations*, *supra* note 114.

it down.[120] If a user disagrees with the site's determination, the user has limited options. This is especially true for those that disagree with the site's decision to keep content on the site. A user that had their content taken down may appeal the site's enforcement decision,[121] but a user that reported a post, to no avail, has no clear recourse.[122] A user could continue to report content they want taken down, or hope that the site's automated content evaluation algorithm independently removes the post, but again, the user must rely on the social media site to take appropriate action. Put simply, there is no way to *force* a social media website to remove content or to comply with its own internal community guidelines. Rather, users are at the mercy of the site's own regulation and enforcement decisions.

Section 230 of the Communications Decency Act (CDA) further crystalizes this reality because it precludes external regulation of a site's content. Enacted in 1996, Section 230(c)(1) of the CDA provides "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[123] Section 230(c)(1) distinguishes between the users on computer services who create content and the computer service provider that gives people access to that content.[124] Courts have deemed Google, Yahoo!, Facebook, and Craigslist all to be "interactive computer service" providers.[125]

Courts have interpreted Section 230(c)(1) to bar "lawsuits seeking to hold a service provider liable for its exercises of a publisher's traditional

120. *See Private Information and Media Policy*, *supra* note 111 (explaining that, when reviewing reports under its policy, Twitter "consider[s] a number of things," such as what type of information is being shared, who is sharing the information, whether the information is available elsewhere online, and why is the information being shared).

121. *See Our Range of Enforcement Options*, TWITTER HELP CTR., https://help.twitter.com/en/rules-and-policies/enforcement-options [https://perma.cc/52HM-6W7D] (last visited Apr. 30, 2022) (stating that when a tweet is removed, the user who generated the tweet can appeal the decision if they believe there was an error); *Account Safety*, TIKTOK, https://support.tiktok.com/en/safety-hc/account-and-user-safety/account-safety [https://perma.cc/UZY3-2PZC] (last visited May 18, 2023) (noting a TikTok user whose account is banned or video is removed can submit an appeal if the user believes it was incorrectly removed or banned); *Appealed Content*, META (Jan. 19, 2022), https://transparency.fb.com/policies/improving/appealed-content-metric/ [https://perma.cc/7GTT-35W5] ("To appeal a decision on Facebook, people select the option to 'Request Review' after we notify them that their content has been removed or covered with a warning. When a review is requested, Meta reviews the post again and determines whether or not it follows our Community Standards.").

122. *See* Rep. of the Special Rapporteur, *supra* note 119 (emphasizing that appeals are permitted when content is removed).

123. 47 U.S.C. § 230(c)(1) (2018).

124. VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 3 (2021).

125. *Id.*

editorial functions—such as deciding whether to publish, withdraw, postpone or alter content."[126] This means that social media sites enjoy a broad immunity against civil suits for the content posted on their website because they simply publish the content and do not generate the content.[127] Section 230 has been effectively used to shield websites against claims that the user generated content on the site constituted "defamation, privacy invasions, intentional infliction of emotional distress, and civil rights violations."[128] As some scholars have noted, the immunity associated with Section 230 provides little incentive for sites to self-regulate the content on their sites.[129]

In terms of doxing, those who feel they have been doxed on social media must first hope that the social media site considers the post to be violative of community guidelines. If the site does not view the post as violating community guidelines, the post will remain accessible for other users to see. Then, even in instances where a user clearly violated a website's guidelines, Section 230 would preclude a user from suing a social media site if it does not effectively enforce their doxing policy.[130] Section 230 also completely removes social media from facing civil liability.[131] Consequently, those that are doxed on a social media site are unable to sue the site for facilitating the doxing.[132]

Barnes v. Yahoo!, Inc. is a perfect example of how these social media realities hurt victims. In *Barnes*, the victim's ex-boyfriend created a fake Yahoo! public profile of her and posted nude pictures of her taken without her consent.[133] The ex-boyfriend also posted her personal phone number, work phone number, work address, and personal address on the profile.[134] The ex-boyfriend went on to use the fake profile to try and solicit sex from others on the site's chatroom.[135] After receiving numerous phone calls, emails, and personal visits from unknown men, the victim utilized Yahoo!'s own procedures to try and have the site take the fake profile down.[136] These attempts failed, and the victim then sued Yahoo! for negligently failing to take down the unauthorized profile.[137] The court held that Section 230 shielded Yahoo! from liability on this basis.[138]

126. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).
127. BRANNON & HOLMES, *supra* note 124.
128. MacAllister, *supra* note 58, at 2468.
129. *Id.*
130. *Id.* at 2467.
131. *Id.*
132. *Id.* at 2468.
133. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).
134. *Id.*
135. *Id.*
136. *Id.* at 1098–99.
137. *Id.* at 1099.
138. *Id.* at 1105.

While many advocate for the CDA's overhaul, political support for such change remains to be seen.[139] While an amended CDA would help doxing victims, an amended Section 230 would not provide victims a direct way to pursue the doxer. Instead, an amendment would remove the site's immunity and permit a victim to sue the site if they were doxed. Victims would still have to rely on the policies and guidelines enacted by the social media sites. Comparatively, legislation would provide a direct and much-needed path for victims to challenge the tactic.

B. *State-by-State Regulation*

State-by-state regulation is another route to address doxing. This could be accomplished by victims using common law tort claims or specific anti-doxing legislation. Most states have not yet legislated against the practice.[140] In such instances, doxing victims would have to try and pursue a tort law claim against the doxer.[141] The victim could file a defamation, harassment, or intentional infliction of emotional distress (IIED) suit.[142]

1. Common Law Remedies

Tanya Gersh successfully brought one such civil suit against Andrew Anglin, the publisher of an alt-right website, *The Daily Stormer*.[143] In 2016, Ms. Gersh, a realtor in Whitefish, Montana, agreed to work with Whitefish resident Sherry Spencer to sell Spencer's mixed-use commercial building.[144] Ms. Sherry Spencer is the mother of a white supremacist, Richard Spencer.[145] Richard Spencer gained notoriety after the 2016 presidential election when a video captured him saying "Hail Trump! Hail our people! Hail victory."[146] After years of discontent with Richard Spencer's behavior, members of the Whitefish community were outraged after

139. *See* BRANNON & HOLMES, *supra* note 124, at 30 ("[I]n 2018, the push to reform Section 230 gained further momentum in Congress. Twenty-six bills in the 116th Congress would have amended Section 230.").

140. Betuel, *supra* note 34.

141. MacAllister, *supra* note 58, at 2479.

142. *Id.*

143. Gersh v. Anglin, 353 F. Supp. 3d 958, 962–63 (D. Mont. 2018); Aaron Bolton, *Neo-Nazi Publisher Ordered to Pay $14 Million in Troll Storm Lawsuit*, MONT. PUB. RADIO (Aug. 8, 2019, 5:38 PM), https://www.mtpr.org/montana-news/2019-08-08/neo-nazi-publisher-ordered-to-pay-14-million-in-troll-storm-lawsuit [https://perma.cc/7J7U-GEJK].

144. *Tanya Gersh v. Andrew Anglin*, S. POVERTY L. CTR., https://www.splcenter.org/seeking-justice/case-docket/tanya-gersh-v-andrew-anglin [https://perma.cc/D3FZ-NS7R] (last visited Apr. 29, 2022) [hereinafter *Tanya Gersh*].

145. *Id.*

146. *Id.*

the release of this video.[147] In turn, members considered protesting outside of the Spencer-owned building.[148]

Ms. Spencer called Ms. Gersh, one of the few Jewish members of Whitefish, for advice after learning about the discontent within the community.[149] Ms. Spencer agreed to sell the building with help from Ms. Gersh, but Ms. Spencer ultimately decided against the sale and began posting online that she was pressured by Ms. Gersh into selling her property.[150] Mr. Anglin, a friend of Richard Spencer, discovered the story and began publishing news articles on his website.[151] Mr. Anglin attacked Ms. Gersh and published Ms. Gersh's phone numbers, email addresses, and social media profiles, as well as Gersh's husband and twelve-year-old son's personally identifiable information.[152]

In bringing her suit, Ms. Gersh relied on an invasion of privacy theory, an IIED theory, and Montana's Anti-Intimidation Act that protects against harassment, threats, and intimidation when one is attempting to exercise a legally protected right.[153] She was awarded over $14 million in compensatory and punitive damages.[154] Yet, the ability of other doxing victims to replicate Ms. Gersh's success is not guaranteed.

Ms. Gersh was able to succeed under a tort theory for a few unique reasons. For one, Ms. Gersh was able to point to a singular doxer, Mr. Anglin, who caused her harm and was clearly the proper defendant. He not only was the person that originally posted her personally identifiable information, but Mr. Anglin also called upon his readers to: "Just make your opinions known. Tell them you are sickened by their Jew agenda," and "hey—if you're in the area, maybe you should stop by and tell her in person what you think of her actions."[155] For many other victims, their cases of doxing may not involve instances of such explicit requests for action from a singular person. Rather, the doxer could just post the person's information and allow for an implied request for action from other "conspirators." Such a scenario would raise the complicated threshold question of who could be held liable in a tort suit, which was not present in Ms. Gersh's case.

Even if the victim could find a viable defendant, the victim would then need to prove the case on the merits of the tort claims, which may be difficult for a victim to do. If the doxer simply posted true information,

147. *Id.*
148. *Id.*
149. *Id.*
150. *Tanya Gersh*, *supra* note 144.
151. *Id.*
152. Gersh v. Anglin, 353 F. Supp. 3d 958, 962 (D. Mont. 2018).
153. *Id.* at 963; MONT. CODE ANN. § 27-1-503(2) (2021).
154. *Tanya Gersh*, *supra* note 144.
155. *Id.*

such as a victim's home address, a defamation suit would fail.[156] For an IIED suit to succeed, the victim would have to show that the defendant's conduct was outrageous or extreme.[157] The requirement of outrageous conduct is a high bar.[158] Ms. Gersh was able to easily pass this bar because "Anglin assisted, encouraged, and ratified a vicious campaign of anti-Semitic harassment against her and her family."[159] Comparatively, it is not obvious that a judge or a jury would view the mere posting of personally identifiable information as sufficiently outrageous. This hurdle could ultimately prove fatal to a victim's IIED suit.

It is likely that a doxing victim would need a severe case—one comparable to Ms. Gersh's—to prevail under tort law. It is doubtful that simply having personally identifiable information posted online would be sufficient for a victim to prevail under a tort law theory; yet, this is a common mode of doxing. Consequently, even though victims have these tort remedies available, there is still a need for specific doxing legislation because tort-based litigation will not often provide a viable solution for doxing victims.

2. Doxing Specific State Legislation

States have utilized various approaches when attempting to regulate doxing.[160] States have either strengthened pre-existing cyber-stalking laws to include doxing[161] or pursued specific anti-doxing legislation.[162] The categories of existing state-level anti-doxing legislation include statutes aimed at protecting groups of people such as law enforcement, judges,[163] or heath care workers;[164] general civil doxing statutes;[165] and

156. MacAllister, *supra* note 58, at 2479.

157. *See* Snyder v. Phelps, 562 U.S. 443, 451 (2011) (stating that to succeed in an IIED under Maryland law, a plaintiff must prove "the defendant intentionally or recklessly engaged in extreme and outrageous conduct that caused the plaintiff to suffer severe emotional distress.").

158. MacAllister, *supra* note 58, at 2479.

159. Gersh v. Anglin, 353 F. Supp. 3d 958, 970 (D. Mont. 2018).

160. Betuel, *supra* note 34.

161. *Id.*

162. *Id.*

163. *See* Jon Fingas, *New Jersey Law Bars Doxxing Campaigns Against Judges, Prosecutors and Police*, ENGADGET (Nov. 22, 2020), https://www.engadget.com/new-jersey-daniels-law-anti-doxxing-203258884.html [https://perma.cc/EZ58-TJTT] ("Governor Phil Murphy has signed Daniel's Law, a measure barring the publication (primarily on the internet) of home addresses and unlisted phone numbers for judges, prosecutors and law enforcement officers. It's named after Daniel Anderl, the son of Judge Esther Salas. A man murdered Daniel and injured his father after finding Judge Salas' address online.").

164. Betuel, *supra* note 34.

165. *E.g.*, A.B. 296, 2021 Leg., 81st Sess. (Nev. 2021) (enacted) (allowing a victim of doxing in Nevada to bring a civil action to recover damages).

criminal statutes.[166]

While legislation of any kind is a step in the right direction, there are a few overarching challenges with state legislation—both civil and criminal. For any state-based civil statutes, jurisdiction provides an initial challenge.[167] To bring a claim under state law in court,[168] the court would need to have personal jurisdiction over the doxer. In many instances, "getting" this jurisdiction could prove difficult for the victim because the doxer can use the Internet to dox from any location and any state.[169] It is inevitable that many doxing victims will seek cases against individuals who do not reside in their home state. To obtain jurisdiction over a nonresident in a civil case, the doxing victim would need to show that the defendant's action—doxing over the Internet—amounts to constitutionally minimum contacts with the victim's home state.[170]

The answer to this jurisdictional question would ultimately turn on what information the doxer posted and how strongly it relates to the victim's home state.[171] One court found minimum contacts existed when the doxer tweeted the victim's physical address in the forum state of Michigan, because the court viewed this as a plausible attempt "to pique Michiganders' interest with her tweet."[172] The court also noted that Michiganders were the ones most readily able to visit the residence.[173] However, the court acknowledged that "not . . . all doxing amounts to constitutionally minimum contacts," especially when the post has little relation to the forum state.[174]

This distinction is concerning because it favors attacks where doxers post information that can elicit a local response. Yet, many doxers may not post a home address and instead opt for email addresses or cell phone

166. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2916.A. (2021) ("It is unlawful for a person to knowingly terrify, intimidate, threaten or harass a specific person or persons by doing any of the following: . . . 4. Without the person's consent and for the purpose of imminently causing the person unwanted physical contact, injury or harassment by a third party, use an electronic communication device to electronically distribute, publish, . . . or make available for downloading the person's personal identifying information, including a digital image of the person, and the use does in fact incite or produce that unwanted physical contact, injury or harassment.").

167. For a full discussion of finding personal jurisdiction in a social media case, *see* Ellen Smith Yost, *Tweet, Post, Share . . . Get Haled into Court? Calder Minimum Contacts Analysis in Social Media Defamation Cases*, 73 SMU L. REV. 693 *passim* (2020).

168. This is true for both state courts and federal courts sitting under diversity jurisdiction. *See id.* at 695.

169. *Id.*

170. Vangheluwe v. Got News, LLC, 365 F. Supp. 3d 850, 852 (E.D. Mich. 2019).

171. *See id.* at 857 (stating that a defamatory post on social media is insufficient for minimum contacts and that "the poster's conduct must have involved the plaintiff's state in some additional way").

172. *Id.* at 860.

173. *Id.*

174. *Id.* at 860–61.

numbers.[175] Such information is less connected to one's home state but can lead to just as harmful consequences and harassment for the victim. Ultimately, the personal jurisdiction requirement for a civil statute will leave doxing victims wondering whether they will have access to recourse or may even preclude victims from successfully suing. Such uncertainty against a tactic that can cause such harm should be unacceptable.

A state statute criminalizing doxing would also present some jurisdictional challenges for a non-resident defendant, but arguably fewer. Instead of the "minimum contacts" analysis required for a civil suit, jurisdiction over a non-resident defendant in a criminal case focuses on the "intent of the defendant and the effects within the forum state."[176] To obtain criminal jurisdiction over an out-of-state doxer, the state[177] would typically need to show: "(1) an act occurring outside the state, which is (2) intended to produce detrimental effects within the state, and (3) is the cause of detrimental effects within the state."[178] The usual difficulty for the prosecution is showing the defendant *intended* to cause harm within the forum state.[179] In instances of doxing, a defendant could try to argue they did not necessarily intend harm in the forum state. However, a foundational aspect of doxing is the intent to cause some level of harm to the target. The target, in turn, resides in a specific state. If one intends to harm a specific individual who resides in a specific state, there is an inextricable intent to cause harm in that state.[180] Because of this connection, a court is likely to consider the intent element sufficiently satisfied, and the act of doxing would likely subject the doxer to a state criminal court's jurisdiction.

Nonetheless, there is one major flaw with state-by-state legislation. Doxing happens all over the country; however, a victim only has access to legal recourse if their forum state has an anti-doxing statute. While there is growing concern around the practice, citizens in thirty-nine states

175. *See* Park, *supra* note 41 (stating that in a 2017 NYU study of 5,500 doxing cases, 90% of cases included victim's address, 61% included a phone number, and 53% included an email address).

176. TERRENCE BERG, STATE CRIMINAL JURISDICTION IN CYBERSPACE: IS THERE A SHERIFF ON THE ELECTRONIC FRONTIER? 2 (2007), http://euro.ecom.cmu.edu/program/law/08-732/Crime/StateCriminalJurisdictionBerg.pdf [https://perma.cc/UN4V-4DM2].

177. In 1911, the Supreme Court first recognized that states could exercise criminal jurisdiction over acts committed outside its territorial bounds where the perpetrator intended to produce, and actually produced, detrimental effects within the state. *See* Strassheim v. Daily, 221 U.S. 280, 285 (1911). Since that decision, numerous states have adopted statutes codifying this type of extraterritorial criminal jurisdiction over defendants. *See* BERG, *supra* note 176 (listing 22 states that had adopted jurisdictional statutes by 2007).

178. BERG, *supra* note 176.

179. *Id.*

180. *See* State v. Amoroso, 975 P.2d 505, 509 (Utah Ct. App. 1999) (finding jurisdiction in part because an out-of-state retailer supplied beer to minors in the forum state).

are currently without specific protections.[181] In such instances, victims must bring makeshift tort claims, which as previously discussed, are not guaranteed to succeed.[182] Legislation on the federal level would swiftly ensure that Americans are protected against this practice, irrespective of where they reside.

C. *Federal Regulation*

Federal legislation is the optimal solution to regulate doxing. A piece of federal legislation that regulates doxing would provide federal courts jurisdiction over such cases. It would obviate any jurisdictional concerns that may be present with state statutes. Next, if the statute were criminal, it would constitute an exception to CDA Section 230 immunity.[183] Section 230 states that "[n]othing in this section shall be construed to impair the enforcement of . . . any other Federal criminal statute."[184] The Justice Department has relied on this exception in the past. In 2018, the Justice Department successfully prosecuted Backpage.com and its corporate entities for conspiracy to engage in money laundering.[185] Similarly, a federal statute criminalizing doxing could provide prosecutors a way to go after social media sites without waiting for amendments to Section 230. This possibility requires a federal criminal statute, because courts have held that this exception does not apply to state criminal statutes or civil suits based on federal criminal laws.[186]

Despite these benefits, no federal statute specifically addresses doxing. Nevertheless, some have argued that the government could utilize the Interstate Communications Statute (ICS) and the Interstate Stalking Statute (ISS) as a workaround to prosecute doxers.[187] The ICS criminalizes "any communication containing any threat to kidnap any person or any threat to injure the person of another."[188] Comparatively, the ISS prevents a person from engaging in a course of conduct on the internet with the intent to "kill, injure, harass, intimidate, or place under surveillance" another person, and that conduct must place that person in "reasonable fear of death or serious bodily injury" or cause "substantial emotional distress."[189]

By their terms, these statutes are written broadly enough to include some instances of doxing, but each statute was not crafted with doxing's

181. Betuel, *supra* note 34.
182. *See* discussion *infra* Section III.B.1.
183. BRANNON & HOLMES, *supra* note 124, at 24.
184. 47 U.S.C. § 230(c)(1) (2011).
185. BRANNON & HOLMES, *supra* note 124, at 25 n.250.
186. *Id.* at 25.
187. MacAllister, *supra* note 58, at 2470, 2474.
188. 18 U.S.C. § 875(c) (2021).
189. *Id.* § 2261A(2).

unique features in mind. For that reason, there would be challenges with enforcement. The ICS requires the user to issue a "threat to kidnap" or "threat to injure."[190] Though the statute does not define what constitutes a threat, at least one Justice has used the term's plain meaning and stated it is "an expression of an intention to inflict evil, injury, or damage on another."[191] In the doxing realm, such a requirement could prove fatal to a suit under the ICS, because doxers may only post personally identifiable information and not make an explicit threat of violence.[192] While some would consider sharing personally identifiable information a threat in and of itself, it is not clear that, given this precedent and specific statutory language, courts would consider the release of personal information "an expression of intention to inflict" injury under the ICS without explicit mentions of violence.[193]

The ISS has flaws when applied to doxing as well. Notably, the ISS requires the perpetrator to engage in a "course of conduct."[194] A course of conduct is defined as "a pattern of conduct composed of two or more acts, evidencing a continuity of purpose."[195] Again, since doxing typically involves multiple actors taking on different roles,[196] a doxer could evade prosecution because they posted personally identifiable information only once. Being able to avoid liability because of a technicality like this seems unjust, especially when a single post of personally identifiable information could cause just as much harm as a course of conduct. These flaws indicate the current federal scheme is insufficient to protect individuals against doxing. A specific federal doxing statute would provide much needed coverage.

III. A SOLUTION: A MODIFIED INTERSTATE DOXXING PREVENTION ACT

At present, there are a few pieces of proposed federal legislation that concern doxing, but Congresswoman Katherine Clark's proposal provides a valuable foundation for a federal statute.[197] After facing a doxing and swatting campaign herself, Congresswoman Clark proposed anti-

190. *Id.* § 875(c).

191. Elonis v. United States, 575 U.S. 723, 744 (2015) (Alito, J., concurring in part, dissenting in part).

192. MacAllister, *supra* note 58, at 2470.

193. *Elonis*, 575 U.S. at 744.

194. 18 U.S.C. § 2261A(2) (2020).

195. *Id.* § 2266(2).

196. MacAllister, *supra* note 58, at 2474.

197. *Compare* A Bill to Protect Federal Judges, Federal Prosecutors, and Federal Law Enforcement Officers from Violence and Doxing, S. 2247, 117th Cong. (2021) (protecting federal judges, prosecutors, and law enforcement from doxing), *with* Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016) (containing no such specific limitation).

doxing legislation in 2016.[198] Titled as the "Interstate Doxxing Prevention Act" (IDPA), the statute would create criminal liability, and the option for civil liability, when individuals have their personally identifiable information published when the publisher intends harm.[199] Despite its strengths, as the IDPA presently stands, it is flawed. Utilizing the IDPA as a starting point, Section A, Part III, of this Article proposes modifications to create an anti-doxing statute that is likely to survive a First Amendment challenge.

A. *Proposals for the Interstate Doxxing Prevention Act*

At present, the Act states:

> (a) Prohibition—Whoever, with the intent to threaten, intimidate, harass, stalk, or facilitate another to threaten, intimidate, harass, or stalk, uses the mail or any facility or means of interstate or foreign commerce to knowingly publish the personally identifiable information of another person, and as a result of that publication places that person in reasonable fear of the death of or serious bodily injury to—
>
> (1) that person;
>
> (2) an immediate family member of that person; or
>
> (3) an intimate partner of that person,
>
> shall be subject to the criminal penalty and the civil liability provided by this section.[200]

The bill defines "publish" as "to circulate, deliver, distribute, disseminate, transmit, or otherwise make available to another person."[201] The IDPA defines "personally identifiable information" as:

> (a) any information that can be used to distinguish or trace an individual's identity, such as name, prior legal name, alias, mother's maiden name, social security number, date or place of birth, address, phone number, or biometric data;
>
> (b) any information that is linked or linkable to an individual, such as medical, financial, education, consumer, or employment information, data, or records; or
>
> (c) any other sensitive private information that is linked or linkable to a specific identifiable individual, such as gender identity, sexual orientation, or any sexually explicit visual

198. Calabro, *supra* note 46, at 56, 66.
199. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016).
200. *Id.* § 2.
201. *Id.*

> depiction of a person described in clause (1), (2), or (3) of subsection (a).[202]

Finally, this bill provides for one carve-out. It states, "[t]his section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or political subdivision of a State, or of an intelligence agency of the United States."[203]

While the IDPA has some benefits, it is a content-based regulation. It must be crafted in a way that is narrowly tailored and restricts the least amount of speech, so as not to be struck down as unconstitutional.[204] To ensure that the IDPA is sufficiently tailored, this Article proposes amendments to the prohibition section, the addition of two more carve-outs, and an explicit statement the IDPA does not apply to constitutionally protected activity.

The IDPA should be amended as follows,[205] with the proposals in italics:

> (b) Prohibition—Whoever,
>
> > (i) with the intent to threaten, intimidate, harass, stalk, or facilitate another to threaten, intimidate, harass, or stalk, uses the mail or any facility or means of interstate or foreign commerce to knowingly publish personally identifiable information of another person *without consent*;
> >
> > (ii) and as a result of that publication *would cause a reasonable person to suffer significant economic injury or severe mental anguish, to fear serious bodily injury, death, or stalking, or to fear that serious bodily injury or death will be inflicted on—*
> >
> > > (1) an immediate family member of that person; or
> > >
> > > (2) an intimate partner of that person,
>
> shall be subject to the criminal penalty and the civil liability provided by this section.

---

202. *Id.*

203. *Id.*

204. City of Los Angeles v. Alameda Books, Inc., 535 U.S. 425, 434 (2002).

205. These amendments were inspired by a recent bill introduced in Nebraska's legislature by Senator Adam Morfeld, which the Anti-Defamation League help draft, and the NCP statutes from Vermont and Minnesota. *See* L.B. 227, 107th Leg., 1st Sess. (Neb. 2021); VT. STAT. ANN. tit. 13, § 2606 (2019); MINN. STAT. § 617.261 (2021).

Next, the following carve-outs should be added:

> *Exclusions: This section shall not apply to:*
> *(1) Disclosures of personally identifiable information that constitute a matter of public concern or are part of a newsworthy event;*
>
> *(2) Disclosures of only a person's name, prior legal name, alias, mother's maiden name. Additional personally identifiable information beyond one person's name, prior legal name, alias, mother's maiden name must be included in the publication for this section to apply.*
>
> Lastly, the following clause should be added: *The Legislature does not intend the Interstate Doxxing Prevention Act to allow prosecution for constitutionally protected activity.*

B. *The Amended Interstate Doxxing Prevent Act Would Likely Survive a First Amendment Challenge*

With these additions, the IDPA would likely survive strict scrutiny and a constitutional challenge. Under strict scrutiny, the government would first need to establish a compelling government interest in regulating doxing.[206] In articulating a compelling interest, the government should emphasize that doxing involves speech on private matters under the IDPA. In turn, this will make it easier for the statute to pass strict scrutiny because speech on purely private matters tends to carry less weight in the strict scrutiny analysis.[207]

In general, while personally identifiable information has varying degrees of publicness when a doxer decides to release this information during a doxing campaign, it is not going to be a matter of public concern. Indeed, doxers are often doxing to *reveal* a formerly anonymous person's identity.[208] They are posting a private individual's information so other Internet users will learn who the person is and related facts about them such as age, employment location, and financial information. The information is then curated and weaponized so the masses can easily access the victim in real life. The information is not "fairly considered as relating to any matter of political, social, or other concern to the community."[209] Rather, it is truly a public disclosure of a private individual's information.

206. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 799 (2011).
207. State v. VanBuren, 214 A.3d 791, 808 (Vt. 2019).
208. Garber, *supra* note 35.
209. Snyder v. Phelps, 562 U.S. 443, 453 (2011).

In evaluating Tanya Gersh's suit, the court acknowledged this reality and was receptive to the notion that her doxer's speech could be fairly construed as a matter of strictly private concern.[210] The amended IDPA also ensures that it does not proscribe speech that is connected to matters of public concern. If the publicly identifiable information was of public concern, the statute explicitly provides for a public interest exception. This should be sufficient for a court to consider the amended IDPA as only proscribing speech on purely private matters.

A compelling interest in regulating doxing is present because doxing substantially invades the victim's privacy, leads to substantive harms, and is rooted in the intentional creation of harassment and threats. States have regularly protected citizens against unreasonable invasions of privacy. This protection has included creating a right of action for "publicity given to private life."[211] Similarly, doxing creates unfettered intrusions into victims' private lives through the public exposure of personally identifiable information. Incessant phone calls, messages, emails, letters, social media comments, or home visits then follow the victim and possibly the victim's family members.[212] In many ways, doxing is the modern way to take away the ability of victims to retreat into the sanctity of one's home. It eviscerates any notion of anonymity and privacy the victim once had, and it is done entirely without the victim's consent. Doxing victims are truly dragged into the spotlight against their will. In such scenarios, courts have historically permitted the protection of the individual's privacy rights, and thus the government should be permitted to do so here.[213]

Doxing also leads to considerable injuries. Posting personally identifiable information subjects the target to death threats, stalking, swatting, constant harassment, and severe emotional distress.[214] There is no foreseeable endpoint to the harassment either—once the personally identifiable information is released, it becomes very difficult to "put the genie back in the bottle." Furthermore, victims can experience job loss, and the practice can prevent them from obtaining employment down the line.[215] Similar harms have been used to justify other statutes against First

210. Gersh v. Anglin, 353 F. Supp. 3d 958, 966 (D. Mont. 2018).

211. *VanBuren*, 214 A.3d at 802.

212. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009); *see Gersh*, 353 F. Supp. 3d at 963 (noting that "[w]hen Gersh filed her Complaint in the spring of 2017, she and her family had received more than 700 disparaging and/or threatening messages").

213. *See* RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (AM. L. INST. 1977) (describing how invasion of privacy claims are all rooted in an "interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others").

214. MacAllister, *supra* note 58, at 2453; Betuel, *supra* note 34.

215. *Cancel Culture*, *supra* note 26.

Amendment challenges, and these injuries should also be sufficient for doxing.[216]

Lastly, doxers intend to inflict harm and cause fear with their actions. Causing injury is foundational to the tactic. Doxers know that in posting the personally identifiable information, the target will either endure actual threats from people who see the post, or nevertheless face the distressing realization that the Internet now has access to their phone number and where they live. The government should be able to protect its citizens from this type of intentional creation of fear. After all, true threats are exempt from First Amendment protections to "protect[] individuals from the fear of violence, from the disruption that fear engenders, and from the possibility that the threatened violence will occur."[217] This reasoning also applies to doxing. In sum, the invasions of privacy, substantial harm, and the malicious and threatening nature of doxing constitutes a compelling government interest that justifies regulation.

After articulating a compelling interest, the government would need to show that the IDPA is "narrowly tailored" and uses the least restrictive means to regulate the speech.[218] In looking for narrowly tailored statutes in other contexts, courts have considered: (1) whether the statute provides clear definitions; (2) the applicable mens rea; and (3) whether there are statutory carve-outs.[219] The amended IDPA has each of these features and is narrowly tailored to the harms of doxing.

To start, the IDPA precisely defines what constitutes "personally identifiable information" and "publishing." A clear definition of these terms is important because it decreases the risk of sweeping in constitutionally protected speech. Next, the IDPA has a malicious intent requirement and requires a knowing mens rea. It only attaches liability when the doxer has the specific intent to harm, harass, intimidate, or threaten. Further, it criminalizes doxing when the doxer *knowingly* publishes personally identifiable information without the target's consent. Requiring a knowing mens rea and the specific intent to harm creates a high standard. It means the statute will not cover negligent, or even reckless publications, and ensures that the statute only covers a narrow category of speech. Courts have been receptive to upholding statutes criminalizing protected speech where there is a knowing mens rea and specific intent to harm requirement.[220] Though courts could accept a lower mens rea—like recklessness—this

216. State v. Katz, 179 N.E.3d 431, 459 (Ind. 2022).

217. R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1991).

218. City of Los Angeles v. Alameda Books, Inc., 535 U.S. 425, 455 (2002).

219. State v. VanBuren, 214 A.3d 791, 811 (Vt. 2019); State v. Casillas, 952 N.W.2d 629, 643–44 (Minn. 2020); *Katz*, 179 N.E.3d at 459.

220. *See VanBuren*, 214 A.3d at 811–12; *Casillas*, 952 N.W.2d at 643; *Katz*, 179 N.E.3d at 459–60.

higher standard follows recent jurisprudence and gives the amended IDPA the best chance to pass constitutional muster.

The IDPA with its additional carve-outs tailors the applicability of the Act and guarantees that it only targets speech in accord with First Amendment jurisprudence. The original carve-out exempted investigative or intelligence activities of law enforcement.[221] This is beneficial because law enforcement often enlists the public to identify individuals suspected of crimes. For example, the FBI recently requested the public's assistance in identifying individuals captured on videos who attended the January 6th U.S. Capitol riot.[222] The IDPA would explicitly protect the public's assistance with this type of law enforcement identification request.

As amended, the IDPA also contains a "newsworthiness" exception, that would permit the publishing of personally identifiable information when it of "public concern." This carve-out is essential. Matters of public concern are at the heart of the First Amendment.[223] A statute that limits public commentary on public issues would run the very real risk of not surviving a First Amendment challenge. Courts have proven receptive to upholding statutes criminalizing protected speech where there is a public concern exception.[224]

One may argue that this carve-out is too broad; whether something is of "public concern" may vary in the matter of days in our viral, Internet-based, society. For example, when Amy Cooper was initially doxed, her story may not have been of public concern. But, days later, it was a national news story. Courts would have to evaluate whether the information was a matter of public concern at the time of its publication. This may result in excluding some doxing victims from coverage. Nevertheless, this carve-out is likely a necessary provision for courts to uphold the IDPA and afford victims a much-needed remedy for doxing.

This newsworthy carve-out would also protect journalists who may release names and addresses when covering stories.[225] The Court has noted in *Cox Broadcasting Corp. v. Cohn* that reporters cannot be made liable for publishing names in the public record.[226] This carve-out assures that the IDPA is in line with this holding. Moreover, protection for journalists is important now more than ever. Reporters have recently come

221. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

222. *See U.S. Capitol Violence*, FBI MOST WANTED, https://www.fbi.gov/wanted/capitol-violence [https://perma.cc/GJ79-6D9G] (compiling videos and over 400 pictures of attendees at the January 6th riot that the FBI are requesting assistance in identifying) (last visited May 18, 2023).

223. Snyder v. Phelps, 562 U.S. 443, 451–52 (2011).

224. *VanBuren*, 214 A.3d at 791; *Casillas*, 952 N.W.2d at 643.

225. *Casillas*, 952 N.W.2d at 643.

226. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 491 (1975).

under attack in the doxing debate.[227] Yet, journalists are essential to free speech and press. This carve-out would guarantee that journalists are not precluded from adequately doing their job.

Lastly, the amended IDPA makes clear it does not infringe upon other constitutional activity. This statement acknowledges that the IDPA may have to give way to overriding First Amendment values. One such scenario is instances of public figures and doxing.[228] Where a doxing case is premised on the release of personally identifiable information of a public figure, it is unlikely that a suit or criminal prosecution would proceed. This is because First Amendment jurisprudence has repeatedly noted that public figures are individuals "intimately involved in the resolution of important public questions or, by reason of their fame, shape events in areas of concern to society at large."[229] Therefore, they are not afforded the same protections as private individuals.[230] In such instances, it is more likely that doxing of a public figure would constitute "public concern." In conjunction with the public concern carve-out, this additional statement makes clear that the IDPA does not infringe upon First Amendment jurisprudence surrounding public figures. This also makes certain that the IDPA is narrowly tailored.

These clear definitions, mens rea, and statutory carve-outs all ensure that the IDPA is narrowly tailored. Given the compelling government interest, the IDPA is likely to survive strict scrutiny.

C. *The Amended Interstate Doxing Prevention Act Has Additional Strengths That Address Doxing's Unique Features*

The amended IDPA has distinctive aspects which make it a valuable tool to combat doxing. First, the IDPA only proscribes speech when the doxer knowingly publishes the information with the *intent* "to threaten, intimidate, harass, stalk."[231] In conjunction with the public concern carve-out, this malicious intent requirement would prevent the prosecution of truly good faith awareness campaigns.

Additionally, the IDPA contains "facilitation" language. Under this proposed statute, liability will attach if one "facilitate[s] another to threaten, intimidate, harass, or stalk."[232] This language is critical because it will ensure prosecutors can go after some of the "conspirator" doxers—the participants that may assist in the campaign but are not the initial

227. Ariel Zilber, *Taylor Lorenz Slammed for 'Doxxing' 'Libs of TikTok' Creator*, N.Y. POST (Apr. 19, 2022, 11:05 AM), https://nypost.com/2022/04/19/taylor-lorenz-blasted-for-doxxing-libs-of-tiktok-creator/ [https://perma.cc/DW8G-7T8F].

228. Hustler Mag., Inc. v. Falwell, 485 U.S. 46, 51 (1988).

229. *Id.*

230. *Id.* at 51–53.

231. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

232. *Id.*

poster. Having a way to address the multiple actors in a doxing crusade is crucial, and the IDPA has language to that effect.

This language would also likely create a route for prosecutors to pursue the social media companies that permit doxing on their sites. Since the IDPA is a federal criminal statute, CDA Section 230 liability would not apply. Prosecutors could then use this basis to argue that the site facilitated another to threaten, intimate, harass, or stalk. In turn, the IDPA could prove valuable in pressuring social media companies to effectively regulate doxing on their own.

The IDPA's definition of personally identifiable information is advantageous because it covers the information doxers most often release. Academic studies that focus on doxing and compile quantitative data on the subject are rare.[233] But, in one of the only available studies, researchers found that of the 5,500 online files associated with doxing, 90% included the victim's address, 61% included a phone number, 53% included an email address, 33% included a date of birth, and 50% included information about the target's family members.[234] Though less common, the doxing files contained credit card numbers (4.3%) and social security numbers (2.6%) at times.[235] The IDPA definition of personally identifiable information reflects the research and covers phone numbers, addresses, date, or place of birth. The definition also goes beyond this and covers more information that doxers could release, such as biometric data. This will allow the statute to adequately respond to advancements in technology, such as facial recognition technology, which could influence the type of information doxers release in the future. Importantly, the IDPA's definition of personally identifiable information covers "employment information." This is significant because doxers are more frequently publishing the victim's place of employment. Indeed, TikTok videos regularly include such information.[236] The IDPA adequately accounts for this development.

The IDPA no longer requires that the publication of personally identifiable information must place a person in "reasonable fear of the death

233. *See* Briony Anderson & Mark A. Wood, *Doxing: A Scoping Review and Typology*, *in* THE EMERALD INTERNATIONAL HANDBOOK OF TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE 205, 208 (Jane Bailey et al. eds., 2021).

234. Peter Snyder et al., *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, *in* PROCEEDINGS OF THE 2017 INTERNET MEASUREMENT CONFERENCE 432, 434, 437–38 (2017).

235. *Id.* at 438.

236. *See, e.g.*, Danesh (@thatdaneshguy), TIKTOK (Jan. 30, 2022), https://www.tiktok.com/@thatdaneshguy/video/7058919000859856174?is_from_webapp=1&sender_device=pc&web_id6947444569463358982 [https://perma.cc/2VZA-TXN3] ("Hello Roger Miller, director of golf and recreation in the city of Coronado, San Diego. Oof, this one's going to be messy.").

of or serious bodily injury."[237] This requirement mandated a high level of harm and thus ran the risk of excluding many victims who instead suffer from severe emotional distress, reputational or financial harms, or job loss. As amended, the IDPA permits liability when a person suffers significant economic injury, severe mental anguish, fear of death, bodily harm, or stalking. This amendment affords greater protection to more people.

Finally, the IDPA no longer permits liability for Internet users who only post an individual's name. This added carve-out is valuable because attaching criminal liability for only posting one's name creates a very low bar. It could capture too much speech. A full name on the Internet may serve as a key to unlock other personally identifiable information, but the legislature must make difficult decisions about the point at which liability attaches. The mere posting of one's name is too low of a bar, and the amended IDPA acknowledges this.

CONCLUSION

In considering the application of unchanging constitutional principles to new and rapidly evolving technology, courts should proceed with caution. We should make every effort to understand new technology. We should consider the possibility that important societal implications of developing technology may become apparent only with time. We should not jump to the conclusion that new technology is fundamentally the same as some older thing with which we are familiar. We should also not hastily dismiss the judgment of legislators, who may be in a better position than we are to assess the implications of new technology.[238]

Doxing is a harmful tactic. It is used to harass and inflict severe emotional distress, and it has the potential to stifle the free flow of thought. The time has now come to regulate doxing and the best way to do so is through a federal statute. The suggested amendments to the IDPA provide legislators with an example of legislation that was narrowly drafted to pass a First Amendment challenge. Doxing-specific legislation is needed so victims like Damon Young and Brianna Wu are not left without protection.

The time is now for Congress to act. Doxing has entered the mainstream's consciousness and the current legal framework is not equipped to protect doxing victims. Moreover, doxing will likely surge in popularity in the coming years, because social media sites like TikTok, which

237. Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. § 2 (2016).

238. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 806 (2011) (Alito, J., dissenting).

has quickly become the most popular web domain,[239] have countless pages that promote doxing-like behaviors. Given the malleability of the tactic, which can be used against individuals on either side of the political spectrum, there should be a viable chance at securing bipartisan support for federal doxing legislation.

239. Johan Moreno, *TikTok Surpasses Google, Facebook as World's Most Popular Web Domain*, FORBES (Dec. 29, 2021, 4:47 PM), https://www.forbes.com/sites/johanmoreno/2021/12/29/tiktok-surpasses-google-facebook-as-worlds-most-popular-web-destination/?sh=4b0ea2b643ef [https://perma.cc/PD3Y-BTZK].

THE PLACE FOR ILLUSIONS: DEEPFAKE TECHNOLOGY AND THE CHALLENGES OF REGULATING UNREALITY

Lindsey Joost[*]

Abstract

Existing laws are insufficient to address the harms caused by deepfakes. This Note explores the characteristics of deepfakes that make preventing both the misuse of the technology and its proliferation on social media and the Internet difficult. This Note will then continue by explaining the special potential harms that deepfakes pose. The third part of this Note will address how the existing legal framework fails, including how Section 230 of the Communications Decency Act serves as a barrier to redress. Finally, this Note suggests potential remedies for deepfake transgressions to reduce the potential harm that deepfakes can inflict.

And one eye-witness weighs
More than ten hear-fays. Seeing is believing,
All the world o'er.
– Plautus[1]

---

* J.D., University of Florida Levin College of Law, Class of 2023.

1. The commonplace saying is a rough translation from "pluris est oculatus testis unus quam auriti decem," meaning "one witness with good eyes is worth more than ten witnesses with good ears." *See* REGINE MAY, APELIUS AND DRAMA: THE ASS ON STAGE 55 (2006).

"Jack's in charge of the choir. They can be—what do you want them to be?"
"Hunters."
– Lord of the Flies[2]

INTRODUCTION

After recent controversy, rapper Eminem has declared himself a feminist.[3] Following the release of a poorly-received diss-track aimed at Facebook founder Mark Zuckerberg, the rapper released a new record—a "diss against the patriarchy"—in which the rapper takes a stand against men and sticks up for women: "I'm standing up to men who are hairy and stink. You know they think they're on top, but I grab them by the stank."[4] It's that same distinctive voice, crude humor, crafted lyricism, and cutting insults for which he is famous. The rapper spits out rapid-fire verses, incorporating witty, clever jokes, while using pronunciation and diction as tools to skillfully bend vowels and emphasize phonemes, rhyming words people never thought could be rhymed.[5]

However, this is not the real Slim Shady; it is a synthesized voice imitation whose lyrics and vocal performance are the product of a text-generating algorithm and impressive artificial intelligence (AI) audio speech synthesis.[6] The song amounts to nothing more than a fun gimmick, but the implications of the technology that created the track are profound. Today, anyone with Internet access can download an app that allows them to take existing audio and alter it to make any particular person realistically look like they said something they would never say.[7]

And the same is true for images. Even video can be faked. Take the video, appearing nearly a month after the Russian invasion into Ukraine, of Ukrainian President Volodymyr Zelenskyy. In the minute-long video, he appears behind a presidential podium, the Ukrainian crest of arms emblazoned on the backdrop behind him and informs the public that he

2. WILLIAM GOLDING, LORD OF THE FLIES 19 (1954).

3. Calamity AI, *Eminem Deepfake Song Feat. Kanye West | MUSIC VIDEO*, YOUTUBE (Mar. 16, 2021), https://www.youtube.com/watch?v=LRX_towD6rs [https://perma.cc/PL7C-FYX6].

4. *Id.*

5. Genius, *Eminem Proves There Are Plenty of Words That Rhyme with 'Orange'*, YOUTUBE (Dec. 30, 2016), https://www.youtube.com/watch?v=lPcR5RVXHMg [https://perma.cc/ARU8-6HF7].

6. Jacob Vaus, *The Unreal Slim Shady: How We Trained an AI to Simulate Eminem's Style*, BUILTIN (Mar. 22, 2022), https://builtin.com/artificial-intelligence/ai-simulate-eminem [https://perma.cc/J7VX-2NPS].

7. Tom Kulik, *Faking It: Why Deepfakes Pose Specific Challenges Under Copyright & Privacy Laws*, ABOVE THE LAW (July 15, 2019, 12:47 PM), https://abovethelaw.com/2019/07/faking-it-why-deepfakes-pose-specific-challenges-under-copyright-privacy-laws/ [https://perma.cc/SY75-G99B].

has made the "difficult decision" to surrender to Russian forces.[8] Staring solemnly into the camera, he speaks directly to his people: "there is no more tomorrow . . . Lay down your arms and return to your families. You should not die in this war."[9] The message broadcast on live television in Ukraine and appeared on the news station's website, as well as social media.[10] The video, unsurprisingly, went viral.[11]

But the forgery failed to bring about the hoped-for effect: people were quick to spot some tell-tale clues of deepfakery, and social media platforms quickly removed the fake content.[12] Fortunately, the public had been warned; predicting that the Russians might deploy deepfake technology in the war, the Ukrainian Center for Strategic Communication had released a series of tweets, cautioning its citizens about deepfaked disinformation: "[i]magine seeing Vladimir Zelensky on TV making a surrender statement. You see it, you hear it—so it's true. But this is not the truth! This is deepfake technology."[13]

Seeing is believing—but what happens when you trust your own eyes? Deepfake technology—which uses AI to create digitally altered audio, images, and videos that appear legitimate—has rapidly improved and is capable of producing audiovisual imagery that is increasingly difficult to discern from genuine recordings.[14] While there are undoubtedly positive applications of the technology, with the increasing sophistication and accessibility of deepfake technology, novel forms of abuse, exploitation,

---

8. Catalina Marchant de Abreu, *Debunking a Deepfake Video of Zelensky Telling Ukrainians to Surrender*, FRANCE24 (Mar. 18, 2022), https://www.france24.com/en/tv-shows/truth-or-fake/20220317-deepfake-video-of-zelensky-telling-ukrainians-to-surrender-debunked [https://perma.cc/N6Z3-9CKM].

9. *Id.*

10. Bobby Allyn, *Deepfake Video of Zelenskyy Could Be 'Tip of the Iceberg' in Info War, Experts Warn*, NPR (Mar. 16, 2022, 8:26 PM), https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia [https://perma.cc/XLX7-CLK9].

11. *Id.*

12. The deepfake was generally thought to be poor quality. The deepfake double "looked unnatural, with a face that didn't match its body, and its voice sounded different from that of its target." *See* Tom Simonite, *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be*, WIRED (Mar. 17, 2022, 1:30 PM), https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/ [https://perma.cc/ZAT2-HG6T].

13. Samantha Cole, *Hacked News Channel and Deepfake of Zelenskyy Surrendering Is Causing Chaos Online*, VICE (Mar. 16, 2022, 1:08 PM), https://www.vice.com/en/article/93bmda/hacked-news-channel-and-deepfake-of-zelenskyy-surrendering-is-causing-chaos-online [https://perma.cc/NRT9-GQ2E].

14. *See* Lutz Finger, *Deepfakes – The Danger of Artificial Intelligence That We Will Learn to Better Manage*, FORBES (Sept. 8, 2022, 8:00 AM), https://www.forbes.com/sites/lutzfinger/2022/09/08/deepfakesthe-danger-of-artificial-intelligence-that-we-will-learn-to-manage-better/?sh=5eb9cffc163a [https://perma.cc/Q4AN-C2GU] ("AI-supported deepfake technology offers improved capabilities – but it also increases the scale for manipulation and bad actor intervention.").

and manipulation have emerged.[15] Among these are face-swapped pornography and fake news.[16] Deepfake technology, therefore, raises grave concerns for one's reputation, personal privacy rights, and national security as a whole.

Currently, only three states have laws that directly deal with deepfakes.[17] Legal scholars have suggested that deepfake transgressions be dealt with under various areas of existing U.S. law such as defamation, copyright infringement, revenge pornography, and harassment.[18] Though the current legal framework on its face appears sufficient to address deepfake transgressions, in practice, applying existing laws to the problems deepfakes pose fails to adequately address the unique issues presented by the technology. Even the proposed "DEEP FAKES Accountability Act"—which would require that all deepfakes contain a watermark and a disclaimer to be legal—vastly mischaracterizes deepfakes as a mere labeling issue and provides no real redress to victims, who would remain responsible for pursuing damages and initiating proceedings against deepfake creators despite being inadequately positioned to do so.

Existing laws—both federal and state, and both civil and criminal—are insufficient to prevent, address, or remedy the harms caused by deepfakes. Further, First Amendment free speech protections provide significant challenges to the government's ability to regulate deepfakes. In Part I of this Note, I will explore the characteristics of deepfakes that make preventing both the misuse of the technology and its proliferation on social media and the Internet so difficult. Part II will then continue by explaining the unique potential harms that deepfakes pose. Part III will address how the current legal framework fails to adequately prevent these harms or provide remedy to victims, including how Section 230 of the Communications Decency Act serves as a major barrier to redress. In Part IV, I will suggest potential remedies for deepfake transgressions by broadening the language of the Violence Against Women Act Reauthorization Act to include deepfake pornography transgressions, creating state statutes which classify deepfake pornography as a specific type of sexual cybercrime, and educating the public on both the existence of deepfakes and the threats that they pose in order to reduce the potential harm that political deepfakes can inflict.

---

15. *See* discussion *infra* Part I.C (discussing the harms of deepfake technology).

16. *See infra* notes 56, 77 and accompanying text.

17. *See* Abigail Loomis, *Deepfakes and American Law*, Davis Pol. Rev. (Apr. 20, 2022), https://www.davispoliticalreview.com/article/deepfakes-and-american-law#:~:text=The%20only%20states%20with%20legislation,specific%20subset%20of%20informational%20deepfakes [https://perma.cc/429U-B6FP] ("The only states with legislation concerning deepfakes are Virginia, Texas, and California.").

18. *See* discussion *infra* Parts II.A–II.D.

I. BACKGROUND

A. *What Are Deepfakes?*

A deepfake is "a video that superimposes hyper-realistic faces onto the bodies of others with the intent of creating a new video with fake representations."[19] Deepfakes are a kind of AI-generated synthetic media that swaps one person in an image, video, or audio recording with another person's likeness.[20] Deepfakes take their name from the technology used to generate this fake content: deep learning.

Deep learning is a subset of machine learning technology that uses multiple layers of neural networks—a specific structure of organized algorithms—to process data, discover, and then create patterns.[21] Deep learning stacks these algorithms in a hierarchy of increasing complexity, with each level building from the knowledge gained from the preceding level of complexity.[22] This iterative process means that the longer the algorithm runs, the more it knows.

Like all deep learning computer networks, deepfake technology generates content based on data input: the algorithm is fed large data sets of real recordings or images to effectively learn what a particular face looks like at different angles, in different lightings, and with different expressions.[23] The algorithm then builds an adaptable model of the facial and vocal characteristics of a person which can then be digitally inserted over the face of a different person in a different recording seamlessly—as if it were a mask.[24]

Early, less sophisticated deepfakes triggered an uncanny valley effect—the phenomenon in which a human being experiences a negative emotional response to things that appear somewhat human-like but are clearly not.[25] Since the emergence of generative adversarial networks

---

19. Russell Spivak, *"Deepfakes": The Newest Way to Commit One of the Oldest Crimes*, 3 GEO. L. TECH. REV. 339, 339 (2019).

20. Dave Johnson & Alexander Johnson, *What Is a Deepfake? Everything You Need to Know About the AI-Powered Fake Media*, Insider (Apr. 5, 2023, 5:35 PM), https://www.businessinsider.com /guides/tech/what-is-deepfake [https://perma.cc/5BTJ-47P6].

21. Margaret Rouse, *Deep Learning*, TECHOPEDIA (Feb. 23, 2022), https://www.techopedia.com/definition/30325/deep-learning [https://perma.cc/JT8P-ETYX].

22. *Id.*

23. *Deepfake: Everything You Need to Know About What It Is & How It Works*, RECFACES (June 22, 2021), https://recfaces.com/articles/what-is-deepfake#1 [https://perma.cc/7T22-2W PA].

24. Regina Rini, *Deepfakes and the Epistemic Backstop*, 20 PHILOSOPHERS' IMPRINT 1, 5 (2020).

25. Astrid M. Rosenthal-von der Pütten et al., *Neural Mechanisms for Accepting and Rejecting Artificial Social Partners in the Uncanny Valley*, 39 J. NEUROSCIENCE 6555, 6555 (2019); *see, e.g.*, BuzzFeedVideo, *You Won't Believe What Obama Says in this Video!*, YOUTUBE (Apr. 17, 2018), https://www.youtube.com/watch?v=cQ54GDm1eL0 [https://perma.cc/3UHB-NW6V].

(GANs) in recent years, however, the final outputs of deepfake technology have quickly become more sophisticated and convincing.

GANs use two distinctive neural networks to train its model: a generator and a discriminator.[26] The networks are functionally adversarial and programmed to compete against each other, "mimic[king] the back-and-forth between a picture forger and an art detective who repeatedly try to outwit one another."[27] The first network—the generator—generates fake images based on patterns it "learns" from an existing image data set.[28] The second network—the discriminator—learns to identify whether an input image is authentic or computer-generated.[29] The generator's job is to trick the discriminator into believing the images are real.[30] As content cycles back and forth between the two networks—one algorithm producing the deepfake, the other attempting to detect deepfaked images—both networks continually improve: the discriminator gets better at identifying AI-generated images, and the generator produces more and more realistic images as it attempts to trick the discriminator.[31] The result of this reciprocal feedback loop: the generator can produce fake images with high fidelity, resulting in realistic impersonations that are increasingly indistinguishable from genuine images and recordings.[32]

While the technology behind deepfakes is highly sophisticated, its producers don't need to be. As the quality of deepfakes has radically improved in recent years, the technology used to create them has simultaneously become easier to access and more affordable.[33] FakeApp,[34] ZAO,[35] and Reface[36] are just some of the face-swapping

26. Natasha Selvaraj, *Real Face vs. AI-Generated Fake: The Science Behind GANs*, BUILTIN (Nov. 30, 2021), https://builtin.com/machine-learning/real-face [https://perma.cc/2LRK-CYFY].

27. Matthew B. Kugler & Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 NW. U. L. REV. 611, 620 (2021) (internal quotations omitted).

28. Selvaraj, *supra* note 26.

29. *Id.*

30. *Id.*

31. AENGUS COLLINS, INT'L RISK GOVERNANCE CTR., FORGED AUTHENTICITY: GOVERNING DEEPFAKE RISKS 6–7 (2019).

32. TIANXIANG SHEN ET AL., "DEEP FAKES" USING GENERATIVE ADVERSARIAL NETWORKS (GAN) 2 (2018).

33. Ben Christopher, *Can California Crack Down on Deepfakes Without Violating the First Amendment?*, CAL MATTERS (July 8, 2019), https://calmatters.org/politics/2019/07/deepfake-berman-california-politics-ab730-fake-news-first-amendment/ [https://perma.cc/9CFB-H6EA].

34. *See* Lauriane Guilloux, *FakeApp*, MALAVIDA (Mar. 7, 2019), https://www.malavida.com/en/soft/fakeapp/#gref [https://perma.cc/ZCH6-EBRN].

35. *Download ZAO*, ZAO APP, https://zaodownload.com/ [https://perma.cc/6G5A-DKJR] (last visited Apr. 18, 2023).

36. *Be Anyone and Reface Anything*, REFACE, https://hey.reface.ai/ [https://perma.cc/QK8F-HYUT] (last visited Apr. 18, 2023).

programs that are available to download on any phone, tablet, or laptop for free. The result is that anyone with access to a YouTube tutorial and enough computing power can produce their own convincing forgery.[37]

The increasing availability and affordability of deepfake technology has contributed to its rapid proliferation: over a ten-month period from December 2018 to September 2019, there was an almost one hundred percent increase in the number of deepfake videos online.[38] One piece of software commonly used to create deepfakes was downloaded more than 100,000 times in the first month after being made public.[39] These programs are specifically designed to allow the average consumer without any programming experience to create their own deepfakes with little effort: simply download the app and feed photos into the program.[40]

Still, the quality of the output depends on the volume of information put into the training data set: the software requires hundreds of images and videos to train the program to learn the features of the target object to produce truly convincing fakes.[41] This is partially why, up until this point, high-profile figures have been the main target for deepfaking, as their public profiles provide plenty of source material for an AI to learn from. However, as Joseph Foley points out, "with the number of selfies the average person takes in a lifetime and rapid technological advances, perhaps soon anyone could be used as a source."[42] Already, technology has been developed to gather publicly available accounts and websites: "[o]pen-source tools like Instagram Scraper and the Chrome extension DownAlbum make it easy to pull photos from publicly available Facebook or Instagram accounts and download them all onto your hard drive."[43] Altogether, by slashing the resources required to produce realistic fabricated content and "democratizing" the process through the dissemination of user-friendly software tools,[44] these tools allow for

37. Christopher, *supra* note 33.

38. HENRY AJDER ET AL., THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT 1 (2019).

39. Dave Lee, *Deepfakes Porn Has Serious Consequences*, BBC NEWS (Feb. 3, 2018), https://www.bbc.com/news/technology-42912529 [https://perma.cc/E54H-E8U5].

40. ADAM DODGE ET AL., USING FAKE VIDEO TECHNOLOGY TO PERPETRATE INTIMATE PARTNER ABUSE 5 (2018).

41. THANH THI NGUYEN ET AL., DEEP LEARNING FOR DEEPFAKES CREATION AND DETECTION: A SURVEY 1 (2019).

42. Joseph Foley, *14 Deepfake Examples That Terrified and Amused the Internet*, CREATIVE BLOQ (Mar. 3, 2022), https://www.creativebloq.com/features/deepfake-examples [https://perma.cc/KC7R-E8KT].

43. DODGE ET AL., *supra* note 40, at 7.

44. COLLINS, *supra* note 31.

"cheap and easy fabrication of content that hijacks one's identity—voice, face, body."[45]

B. *How Are They Used?*

Deepfakes can be used for a variety of purposes, not all of which are harmful. The most obvious beneficial uses of the technology come in the arts and have already been used for that purpose: In *Star Wars: The Last Jedi*, filmmakers used automated dialogue replacement (ADR) technology to fake additional dialogue using snippets from real recordings after Carrie Fisher's death.[46] A TikTok page dedicated to Tom Cruise deepfakes, which feature the actor showing off magic coin tricks, eating cereal with Paris Hilton, and eating a lollipop, quickly racked up tens of millions of views on the platform.[47] Snapchat filters that superimpose someone's face on a person's own in real time, digital avatars, and apps that allow a person to virtually try on online clothes while shopping are other positive uses of the technology.[48]

The technology can also be used to create satirical content that comments on politics and pokes fun at governmental figures.[49] In 2018, video footage of President Obama cursing and calling President Trump a derogatory name appeared online.[50] The video caused a stir, not because of the nature of the remarks, but because the video was entirely fake.[51] Actor and director Jordan Peele had fabricated the video entirely using deepfake technology.[52] He intended for the video to serve as a warning against deepfakes.[53] The public service announcement began by noting,

45. Robert Chesney & Danielle Citron, *Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?*, LAWFARE BLOG (Feb. 21, 2018, 10:00 AM), https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy [https://perma.cc/A6TE-DP7N].

46. Erik Gerstner, *Face/Off: "Deepfake" Face Swaps and Privacy Laws*, 87 DEF. COUNS. J. 1, 3 (2020); Evan Narcisse, *It Took Some Movie Magic to Complete Carrie Fisher's Leia Dialogue in The Last Jedi*, GIZMODO (Dec. 8, 2017), https://gizmodo.com/it-took-some-movie-magic-to-complete-carrie-fishers-lei-1821121635 [https://perma.cc/L3JZ-B34P].

47. Rachel Metz, *How a Deepfake Tom Cruise on TikTok Turned into a Very Real AI Company*, CNN (Aug. 6, 2021, 8:00 AM), https://www.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company/index.html [https://perma.cc/K373-DB4M].

48. NGUYEN ET AL., *supra* note 41, at 2.

49. Nina I. Brown, *Deepfakes and the Weaponization of Disinformation*, 23 VA. J.L. & TECH. 1, 5 (2020).

50. BuzzFeedVideo, *supra* note 25.

51. Brown, *supra* note 49.

52. Aja Romano, *Jordan Peele's Simulated Obama PSA Is a Double-Edged Warning Against Fake News*, VOX (Apr. 18, 2018), https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed [https://perma.cc/5AB9-TDNM].

53. *Id.*

"We're entering an era in which our enemies can make it look like anyone is saying anything at any point in time."[54]

C. *What Harms Do They Pose?*

The proliferation of increasingly realistic fabricated content presents numerous potential risks to individuals, organizations, and societies.

1. Threat to Individual Privacy

The first deepfake videos to circulate widely surfaced in 2017 when a Reddit user posted doctored porn clips featuring the faces of celebrities such as Emilia Clarke, Taylor Swift, Scarlett Johansson, and Gal Gadot, among others, swapped onto the faces of porn performers.[55] Pornography continues to account for the vast majority of deepfakes: a 2019 study found that, of the 14,678 deepfake videos on the Internet, 96% were pornographic.[56] While the majority of pornographic deepfakes feature actresses and musicians working in the entertainment industry, everyday citizens have been victimized by deepfake pornography as well.[57]

Nonconsensual deepfake pornography is essentially the next iteration of revenge pornography, representing a new and degrading means of humiliation, harassment, and abuse. While revenge pornography involves leaking a real nude image or video initially shared privately, deepfake pornography allows the perpetrator to fabricate a pornographic video starring any woman who has shared images of herself on the Internet.[58] Most disturbingly, because these videos are built off public photos, anyone can be a victim. After being superimposed into dozens of graphic sex scenes (including one video that was falsely described as real "leaked" footage and has been watched on a major porn site more than 1.5 million times), Scarlett Johansson stated, "Nothing can stop someone from cutting and pasting my image or anyone else's onto a different body."[59] While the creation of deepfakes requires some technical know-how, a marketplace sprung up for people seeking these videos.[60]

54. BuzzFeedVideo, *supra* note 25.

55. Ian Sample, *What Are Deepfakes – and How Can You Spot Them?*, GUARDIAN (Jan. 13, 2020, 5:00 PM), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [https://perma.cc/LA99-3AJD].

56. AJDER ET AL., *supra* note 38, at 6.

57. *See id.* at 2 (stating that all but one percent of the subjects featured in deepfake pornography videos were actresses and musicians working in the entertainment sector).

58. Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479, 1481 (2020).

59. Drew Harwell, *Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: 'Everybody is a Potential Target*', WASH. POST (Dec. 30, 2018), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/ [https://perma.cc/33WS-PK4L].

60. Gieseke, *supra* note 58, at 1485; Romano, *supra* note 52.

Deepfake producers offer to create videos by request on forum-based websites like 4chan, 8chan, and Voat.[61] What is the going rate for these videos? About twenty dollars per fake.[62]

Like revenge porn, deepfake pornography can be used as a powerful instrument of individual intimidation, coercion, or defamation and can cause problems in the context of intimate partner abuse. "A fake video that causes an audience to believe that a partner was featured in revenge porn can cause precisely the same kind of reputation, privacy, and property harms, and can rob people of their potential for the rest of their lives."[63] While the video may not be real, the psychological damage to the individual is. Because, while the sex scenes look realistic, they are not consensual cyber porn. "Face-swapped porn inflicts the harm of sexual objectification without consent. Like nonconsensual porn, face-swapped porn violates the partner's expectation that all aspects of sexual activity should be founded on consent."[64]

In addition to the psychological effects of being the subject of nonconsensual deepfake pornography, compromising images and videos can damage a victim's reputation, rendering them "unemployable, undateable, and potentially at physical risk."[65] A single intimate image can quickly dominate the first several pages of search engine results for the victim's name, meaning that one Google search could uncover a deepfake sex tape in which the victim did not participate, permanently affecting her ability to find a job. "Deepfake technology is being weaponized against women."[66]

2. Threat to National Security and Politics

Perhaps even more disturbing than the harm to individuals that deepfakes can cause are the national security implications of sophisticated forgeries: a well-executed and well-timed deepfake has the potential to cause significantly destabilizing political impacts.

In May 2019, a video of U.S. Speaker of the House and Democrat Congresswoman Nancy Pelosi went viral on social media.[67] In the video, Pelosi's speech appeared slurred, as she stumbled over her words. The video "was retweeted by the official Twitter account of U.S. President Trump, receiving over 6.3m views" in the three months after it was posted.[68] "On a popular Facebook page, the video received over 2.2m

61. Gieseke, *supra* note 58.
62. Harwell, *supra* note 59.
63. DODGE ET AL., *supra* note 40.
64. *Id.* at 4.
65. *Id.*
66. Sample, *supra* note 55.
67. AJDER ET AL., *supra* note 38, at 11.
68. *Id.*

views in the forty-eight hours following its initial upload, with commenters calling Pelosi 'drunk' and a 'babbling mess.'"[69]

However, the video wasn't real. "Pelosi's speech had been slowed down" to make her appear drunk.[70] While the video was ultimately harmless, the rapid spread of this manipulated video[71] demonstrates the potential for deepfakes to generate significant harm on a much broader scale—creating social unrest, political distrust, and delegitimizing the news media.

Crude deepfakes—such as the Zelenskyy deepfake mentioned earlier—have already been created and spread by foreign powers in attempt to disrupt democracy by targeting political leaders. For example, in 2009, John Beyrle, former U.S. Ambassador to Moscow, was the subject of a fake sex video which appeared to show him having an affair.[72] The video was supposedly disseminated by the Russian government and was created to harm his reputation.[73] Similarly, Michael McFaul, who served as the American ambassador to Russia from 2012 to 2014, was accused of pedophilia, having had his face inserted into photographs and his speech "spliced . . . to make me say things I never uttered."[74]

Altogether, the technology opens up the potential that any foreign government could use the technology for any means—including depicting an American politician using a racial epithet, taking a bribe, or encouraging certain political action.[75] In 2018, a deepfake video of President Trump was released where he appears to call on Belgium to exit the Paris Climate Agreement.[76] In the fictional address, he is shown saying: "As you know I had the balls to withdraw from the Paris climate agreement. And so should you."[77] A Belgian political party created the fake video, apparently to "start a public debate," but it is easy to see how the technology could easily be leveraged for more nefarious means.[78]

---

69. *Id.*

70. *Id.*

71. Scholars refer to videos like these that have been manipulated with basic editing tools or intentionally placed out of context as "shallowfakes." *See id.*

72. Deb Riechmann, *I Never Said That! High-Tech Deception of 'Deepfake' Videos*, AP NEWS (July 2, 2018), https://apnews.com/article/north-america-donald-trump-ap-top-news-elections-artificial-intelligence-21fa207a1254401197fd1e0d7ecd14cb [https://perma.cc/2GQP-3FUT].

73. *Id.*

74. *Id.*

75. *Id.*

76. Hans von der Burchard, *Belgian Socialist Party Circulates 'Deep Fake' Donald Trump Video*, POLITICO (May 21, 2018, 2:13 PM), https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/ [https://perma.cc/683Q-HK63].

77. *Id.*

78. *Id.*

Senator Marco Rubio has spoken out against the harms deepfakes pose, noting that "[i]t's a weapon that could be used—timed appropriately and placed appropriately—in the same way fake news is used, except in a video form, which could create real chaos and instability on the eve of an election or a major decision of any sort."[79]

The spread of deepfakes will threaten to erode the trust necessary for democracy to function effectively, for two reasons. First, and most obviously, the marketplace of ideas will be injected with a particularly dangerous form of falsehood, as deepfaked videos—though false—purport to be truth. As journalist Franklin Foer explains in *The Atlantic*, what makes deepfakes so frightening is "the acuity of the technology: A casual observer can't easily detect the hoax."[80] Second, and more subtly, "the public may become more willing to disbelieve true but uncomfortable facts."[81] As Senator Rubio warned, "deepfakes pose an especially grave threat to the public's trust in the information it consumes; particularly images, and video and audio recordings posted online."[82] There is a potential for weaponization of the *idea* that we cannot believe any image could be wielded by authoritarians and totalitarians worldwide.[83] News organizations may hesitate from rapidly reporting real, disturbing events for fear that the evidence of them will turn out to be fake.[84]

II. WHY CURRENT LEGAL FRAMEWORKS FAIL

While the existing legal framework provides victims who become the subject of unwanted deepfakes some avenues for redress, those existing legal claims only apply in very specific circumstances, and thus fail to serve as feasible solutions. Tort and copyright law could provide a cause of action for some victims, but both are vulnerable to a First Amendment defense that deepfakes are protected speech. Further, Section 230 of the Communications Decency Act (CDA), which provides substantial protection to online platforms, acts as a powerful barrier to recovery for victims in most circumstances.

---

79. Riechmann, *supra* note 72.

80. Franklin Foer, *The Era of Fake Video Begins*, ATL. (May 2018), https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877/ [https://perma.cc/4SWP-GC4X].

81. Chesney & Citron, *supra* note 45.

82. *Rubio, Warner Express Concern over Growing Threat Posed by Deepfakes*, MARCO RUBIO US SEN. FOR FLA. (Oct. 2, 2019), https://www.rubio.senate.gov/public/index.cfm/2019/10/rubio-warner-express-concern-over-growing-threat-posed-by-deepfakes [https://perma.cc/5CTP-RFHF].

83. Sam Gregory, *Deepfakes and Synthetic Media: What Should We Fear? What Can We Do?*, WITNESS BLOG (July 30, 2018), https://blog.witness.org/2018/07/deepfakes/ [https://perma.cc/8RRY-SP48].

84. *Id.*

A. *Tort Law*

State tort law typically supplies the remedy for civil privacy violations. Defamation law appears specifically applicable to the threat presented by deepfakes, given that deepfake technology provides the opportunity for anyone's image to be used in a variety of ways and therefore the potential to cause significant damage to a person's reputation. While state law governs defamation causes of action and thus the standard varies, the tort typically requires an unprivileged publication of a false and defamatory statement concerning another person where harm to a reputation can be presumed or "special harm" can be shown.[85] Defamatory statements are those that "tend to damage another's reputation to the extent of lowering their regard in the community or deterring others from associating with them."[86] Images or videos can constitute defamatory "statements," even if the image is doctored.[87]

However, to create liability for defamation there must be publication of matter that is both defamatory and false.[88] When deepfakes can be compared to an original recording, proving that the deepfake is in fact fake will be relatively straightforward. However, as the quality of deepfakes improves, proving that a recording is false may require expensive and complex technology.[89]

Further, a deepfake cannot constitute "defamation" if the content does not claim to be "real."[90] Disclaimers that the content is a deepfake will likely preclude any liability for defamation; deepfakes, by definition, are doctored, and therefore cannot reasonably be interpreted as stating actual facts about the person involved.[91]

Further, a deepfake creator has a powerful defense to any defamation claim by arguing that the video is a parody. In the landmark Supreme

---

85. RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

86. *Id.*

87. *See* Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 80 (W. Va. 1983) ("[I]t is well established that although libel is generally perpetrated by written communication, it also includes defamation through the publication of pictures or photographs."); Kiesau v. Bantz, 686 N.W.2d 164, 178 (Iowa 2004) (finding that a doctored photo can be defamatory), *overruled in part by* Alcala v. Marriott Int'l, Inc., 880 N.W.2d 699 (Iowa 2016).

88. RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

89. *See* Jason Haas, *Deepfake Dilemma*, 2019 INTELL. PROP. MAG. 33, 33 ("Even expensive discovery measures may prove inadequate to identify a deepfake creator, leaving a plaintiff's only possible recourse to sue republishers.").

90. Kristen Dold, *Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy*, ROLLING STONE (Apr. 17, 2018), https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-a-creepy-internet-trend-could-threaten-democracy-629275/ [https://perma.cc/M2XX-FK28].

91. *See* Hustler Magazine v. Falwell, 485 U.S. 46, 57 (1988) (finding that the magazine's parody ad could not "reasonably be understood as describing actual facts about [respondent] or actual events in which [he] participated").

Court case *Hustler v. Falwell*, televangelist Jerry Falwell sued *Hustler* magazine for defamation and intentional infliction of emotional distress after it published a satirical ad suggesting he had drunken sex with his mother in an outhouse.[92] The ad contained a disclaimer: "ad parody—not to be taken seriously."[93]

The Court ruled against Falwell, finding that the ad parody was not believable and therefore did not contain false statements of fact; as a result, the magazine was constitutionally immune from defamation liability.[94] As Erik Gerstner explains,

> Defamation is by its nature mutually exclusive of parody. By definition, defamation requires a false statement of fact; parody, to the degree that it is perceived as parody by its intended audience, conveys the message that it is not the original and, therefore, cannot constitute a false statement of fact.[95]

Deepfake videos are also likely to trigger the common law tort of intentional infliction of emotional distress (IIED).[96] Unlike with a defamation claim, the victim of IIED does not need to prove that a statement is false: the only concern with regard to IIED is whether the conduct was "patently offensive"—false or not.[97] However, *Falwell* further demonstrates that the First Amendment defense extends to other theories of tort liability that may offer individuals redress, such as IIED.[98] The Supreme Court rejected both claims, holding that the First Amendment prohibits public figures from recovering damages for the tort of IIED if the emotional distress was caused by a parody that a reasonable person would not have interpreted as factual.[99] Further, the intent requirement for a claim of IIED is a powerful barrier to remedy for victims of deepfake media: "[w]hile there will clearly be intent in the creation of the media itself, in many cases it is unlikely that a court will find actual intent to cause emotional distress."[100] Given these constitutional limits, a deepfake can likely only be prohibited if it falsely depicts an individual, "does not include a disclaimer, and is made with

92. *Id.* at 52.

93. *Id.*

94. Alicia J. Bentley, *Hustler Magazine v. Falwell: The Application of the Actual Malice Standard to Intentional Infliction of Emotional Distress Claims*, 49 OHIO STATE L.J. 825, 828 (1988).

95. Gerstner, *supra* note 46, at 1, 5.

96. *Id.* at 5–6.

97. *Id.* at 6.

98. Shannon Reid, *The Deepfake Dilemma: Reconciling Privacy and First Amendment Protections*, 23 U. PA. J. CONST. L. 209, 217 (2021).

99. *See* Hustler Magazine v. Falwell, 485 U.S. 46, 50 (1988).

100. Gerstner, *supra* note 46, at 6.

knowledge that it was false or with reckless disregard of whether it was false or not."[101]

B. *Copyright*

Copyright law also fails to provide a remedy for those victimized by deepfakes because deepfake creators can likely receive First Amendment protection under the concept of "transformative use." In April 2020, the YouTube creator Vocal Synthesis, an anonymous YouTube account that uses AI to make vocal impersonations of celebrities and politicians rapping various content, received the first copyright claim for deepfaked audio content.[102] The videos in dispute were two AI-powered voice impersonations depicting Jay-Z rapping William Shakespeare's "To Be or Not to Be" soliloquy from Hamlet, and Billy Joel's "We Didn't Start the Fire."[103] Like the Eminem video, the videos in question are "entirely computer-generated using a text-to-speech model trained on the speech patterns of Jay-Z."[104]

Apparently unamused by the Shakespearean jest, Jay-Z's legal team sought to remove the videos from the platform, claiming in their DMCA takedown notice[105] that the content "unlawfully uses an AI to impersonate our client's voice."[106] YouTube initially removed the videos, but ultimately, Jay-Z's claim was unsuccessful; within a matter of days, YouTube rejected the copyright claims, citing insufficient grounds from the claimant.[107] The videos were promptly reinstated.[108]

---

101. Daniel Lipkowitz, *Manipulated Reality, Menaced Democracy: An Assessment of the DEEP FAKES Accountability Act of 2019*, N.Y.U. J. LEGIS. & PUB. POL'Y QUORUM (Mar. 5, 2020), https://nyujlpp.org/quorum/lipkowitz-manipulated-reality-menaced-democracy-deepfakes-accountability-act/ [https://perma.cc/S5DN-SBT6].

102. Andy Baio, *With Questionable Copyright Claim, Jay-Z Orders Deepfake Audio Parodies Off YouTube*, WAXY (Apr. 28, 2020), https://waxy.org/2020/04/jay-z-orders-deepfake-audio-parodies-off-youtube/ [https://perma.cc/QU2A-GGH8].

103. *Id.*

104. Marc Hogan, *What Does JAY-Z's Fight over Audio Deepfakes Mean for the Future of AI Music?*, PITCHFORK (May 11, 2020), https://pitchfork.com/thepitch/what-does-jay-zs-fight-over-audio-deepfakes-mean-for-the-future-of-ai-music/ [https://perma.cc/AB6H-AH6Z].

105. "DMCA" stands for the "Digital Millennium Copyright Act." A DMCA takedown notice "informs a company, web host, search engine, or internet service provider that they are hosting or linking to material that infringes on a copyright. The party that receives the notice should take down the material in question as soon as possible." *DMCA Notice: Everything You Need to Know*, UPCOUNSEL (Oct. 5, 2020), https://www.upcounsel.com/dmca-notice [https://perma.cc/A9BR-SL2V].

106. Baio, *supra* note 102.

107. Nick Statt, *Jay Z Tries to Use Copyright Strikes to Remove Deepfaked Audio of Himself from YouTube*, VERGE (Apr. 28, 2020, 6:38 PM), https://www.theverge.com/2020/4/28/21240488/jay-z-deepfakes-roc-nation-youtube-removed-ai-copyright-impersonation [https://perma.cc/4TUD-3N5L].

108. *Id.*

Though Roc Nation has not yet taken any of their claims to court, the Jay-Z situation and commentary surrounding the initial takedown attempt demonstrate that copyright law is not a viable source of redress for those who unwillingly become the subject of deepfake creations in most circumstances. First, a person's "sound" or general appearance is not copyrightable; the person depicted in the deepfake must own the source material used to create the deepfake to bring a copyright infringement claim. Second, the doctrine of fair use likely provides a viable First Amendment defense to deepfake creators in most cases, since deepfakes almost by definition qualify as "transformative use."

Copyright protection only applies to "original works of authorship fixed in any tangible medium of expression."[109] While 17 U.S.C. § 102 provides copyright protection to "sound recordings" and "musical works," this protection applies to the underlying musical elements and lyrics of a work.[110] A voice or vocal style, on the other hand, cannot be copyrighted, as those sounds are not "fixed"; rather, there are an infinite number of words or phrases a person could potentially utter in their distinctive voice.[111] Using AI to impersonate someone's voice, therefore, does not violate existing copyright law.[112]

Similarly, an individual's appearance is not protectable under copyright because an appearance is "not created like a work of authorship—it simply exists."[113] Any photographs or videos used to create a deepfake *are* subject to copyright protection, but existing regulations exclusively cover the person who created the content: the "author."[114] If the subject of the deepfake did not take and post the source material of the deepfake themselves, he or she has no claim for copyright infringement.[115]

Even when an individual depicted in the deepfake owns all images and video used to create a deepfake, the doctrine of fair use—which

---

109. 17 U.S.C. § 102(a).

110. *Id.*

111. *See* Midler v. Ford Motor Co., 849 F.2d 460, 462 (9th Cir. 1988) ("A voice is not copyrightable. The sounds are not 'fixed.'"); Butler v. Target Corp., 323 F. Supp. 2d 1052, 1055 (C.D. Cal. 2004) (explaining that although lyrics to a song are copyrightable, the underlying voice is not).

112. Hogan, *supra* note 104.

113. Zachary Schapiro, *Deep Fakes Accountability Act: Overbroad and Ineffective*, 2020 B.C. INTELL. PROP. & TECH. F. 1, 13; *see* 17 U.S.C. § 102 (granting copyright protections to works of authorship); *see also* Downing v. Abercrombie & Fitch, 265 F.3d 994, 1004 (9th Cir. 2001) (noting that a person's likeness is not a "work of authorship" within meaning of the Copyright Act and thus is not subject to copyright protection).

114. The copyright owner is the one who creates the content. *See* 17 U.S.C. §§ 102, 106(3) (establishing that "pictorial, graphic . . . [and] motion pictures and other audiovisual works" may be protected by copyright by the authors of the work).

115. In cases where a photographer or videographer took the content, ownership may be stipulated in the contract with the photographer or videographer. *See* Schapiro, *supra* note 113.

allows for some unlicensed use of material that would otherwise be copyright protected—likely protects most deepfake creators from liability for infringement. Codified in federal law as 17 U.S.C. § 107, "fair use" is a defense based in the First Amendment that allows an infringer to use the original author's work without asking permission in certain, limited circumstances.[116] These include criticism, comment, news reporting, teaching, scholarship, and research.[117] Parody may also claim fair use under 17 U.S.C. § 107.[118]

To determine whether a particular unlicensed use of a copyrighted work qualifies as "fair," courts consider four factors: (1) the purpose and character of the creator's use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion taken; and (4) the effect upon the use upon the potential market.[119] In the 1994 case *Campbell v. Acuff-Rose Music*, the Supreme Court honed in specifically on the first of the four fair use factors—the purpose and character of the use—and emphasized that the important aspect of the analysis was whether the purpose and the character of the use was "transformative."[120]

Whether a work qualifies as "transformative" depends largely on whether the work builds upon a copyrighted work in a different manner or for a different purpose from the original—i.e., it transforms or modifies the original work in some creative way so that it creates content with new expression, meaning, or message—or whether it merely copies from the original.[121] However, deepfakes—which take a photo or video and transform it into something vastly different from the purpose or character of the original work—may be the epitome of transformative use.[122] Further, the typical deepfake is not likely meant to replace the original work. Copyright law, therefore, is not a promising source of redress for victims of nonconsensual deepfake content in most circumstances.[123]

C. *Nonconsensual Pornography Laws*

While the term "nonconsensual pornography" is defined as the nonconsensual sharing of intimate imagery and encompasses both deepfake pornography and revenge pornography, most nonconsensual

116. 17 U.S.C. § 107.

117. *Id.*

118. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994) ("[P]arody has an obvious claim to transformative value.").

119. 17 U.S.C. § 107; Schapiro, *supra* note 113.

120. *Campbell*, 510 U.S. at 579.

121. *See id.* ("The central purpose of this investigation is to see . . . whether the new work merely 'supersede[s] the objects' of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is 'transformative.'").

122. Reid, *supra* note 98, at 221.

123. *Id.* at 221–22.

pornography statutes are too narrowly drawn to provide an effective remedy for individuals depicted in nonconsensual pornographic deepfakes and instead only address revenge pornography offenses.[124] Revenge pornography typically occurs when an individual is seeking revenge against a former intimate partner by "sharing sexually explicit images that the individual obtained during the period of their intimacy," even if the image was originally taken with the subject's consent.[125]

The majority of states have enacted laws to address the growing epidemic of nonconsensual pornography.[126] However, the language of most of these laws prevents them from applying to deepfakes, as many state laws against nonconsensual pornography require that the perpetrator had an intent to harm the subject of the images or video to be liable.[127] For example, Arizona's nonconsensual pornography statute makes it illegal to disclose an image of a person depicted in a state of nudity or engaged in specific sexual activities only if the image was disclosed with the intent to "harm, harass, intimidate, threaten or coerce" the depicted person.[128] Similarly, Colorado law makes "[p]osting a private image for harassment" a misdemeanor offense where a person posts any photograph or video that displays the private intimate parts of another person "with the intent to harass the depicted person and inflict serious emotional distress upon the depicted person" and where "the conduct results in serious emotional distress of the depicted person."[129] These intent-to-harm requirements are problematic for victims of deepfake pornography because deepfake creators may not intend to hurt their subject; perpetrators may be motivated by voyeurism, profit, or a variety of other

124. *Nonconsensual Pornography (Revenge Porn) Laws in the United States*, BALLOTPEDIA (Apr. 12, 2023), https://ballotpedia.org/Nonconsensual_pornography_(revenge_porn)_laws_in_the_United_States [https://perma.cc/TGU5-MSXD].

125. Reid, *supra* note 98, at 224.

126. As of November 2021, forty-eight states plus the District of Columbia and Guam had specific laws criminalizing revenge porn. *See* Chance Carter, *An Update on the Legal Landscape of Revenge Porn*, NAT'L ASS'N OF ATT'YS GEN. (Nov. 16, 2021), https://www.naag.org/attorney-general-journal/an-update-on-the-legal-landscape-of-revenge-porn/#identifier_7_21493 [https://perma.cc/XHC3-R4FC].

127. *See* OHIO REV. CODE ANN. § 2917.211(B)(5) (West 2022) ("No person shall knowingly disseminate an image of another person if . . . The image is disseminated with intent to harm the person in the image."); MO. REV. STAT. § 573.110.2.(1) (2018) (requiring that a person must "intentionally disseminate" sexual imagery "with the intent to harass, threaten, or coerce an image of another person"); WASH. REV. CODE § 9A.86.010(2)(a) (2015) ("A person who is under the age of eighteen is not guilty of the crime of disclosing intimate images unless the person: (a) Intentionally and maliciously disclosed an intimate image of another person."); OR. REV. STAT. § 163.472(1)(a) (2021) ("The person, with the intent to harass, humiliate or injure another person, knowingly causes to be disclosed an identifiable image of the other person whose intimate parts are visible or who is engaged in sexual conduct.").

128. ARIZ. REV. STAT. ANN. § 13-1425 (2016).

129. COLO. REV. STAT. § 18-7-107 (2012).

reasons.[130] Yet deepfake creators that share their content online without any harmful intent would not be liable in states with these intent-to-harm requirements.

Further, many nonconsensual pornography laws also require the subject to have had a reasonable expectation of privacy in regard to the content for the distributor to be liable.[131] That is because the basis for these laws is that what is being shared is private, true information that is being disclosed without the subject's consent.[132] However, deepfakes are generally produced using photographs the victims themselves have posted online.[133] The deepfakes themselves, therefore, are not legally in violation of privacy; the victim had no reasonable expectation of privacy in regard to the source material they posted.[134]

Additionally, many state statutes have language that specifies that the reasonable expectation of privacy occurred in regard to the taking of the nude images or videos. For example, Tennessee's nonconsensual pornography law requires that the "image was photographed or recorded under circumstances where the parties agreed or understood that the image would remain private."[135] Sharing a deepfake would not satisfy this law because a deepfake is neither photographed nor recorded.

Federal law remedies for nonconsensual pornography have similarly limited application when considering pornographic deepfakes. In March 2021, President Biden signed into law the Violence Against Women Act Reauthorization Act of 2022 (VAWA), which, in part, established a federal civil cause of action for individuals whose intimate visual images are disclosed without their consent and allows a victim to recover damages and legal fees.[136] However, a plaintiff must prove that the

130. Michelle Gonzalez, *CCRI Welcomes Passage of SHIELD Act as Amendment to Violence Against Women Reauthorization Act of 2021*, CYBER CIV. RTS. INITIATIVE (Mar. 16, 2021), https://cybercivilrights.org/5014-2/ [https://perma.cc/URQ6-6NR8].

131. *See* MO. REV. STAT. § 573.110.2.(2) (2018) ("A person commits the offense of nonconsensual dissemination of private sexual images if he or she: . . . (2) Obtains the image under circumstances in which a reasonable person would know or understand that the image was to remain private."); WASH. REV. CODE § 9A.86.010(1)(a) (2015) ("A person commits the crime of disclosing intimate images when . . . the person disclosing the image: (a) Obtained it under circumstances in which a reasonable person would know or understand that the image was to remain private."); D.C. CODE § 22-3052(a)(2) (2015) ("here was an agreement or understanding between the person depicted and the person disclosing that the sexual image would not be disclosed").

132. Dold, *supra* note 90.

133. Gieseke, *supra* note 58, at 1501–02.

134. *Id.*

135. TENN. CODE ANN. § 39-17-318 (2020).

136. *Fact Sheet: Reauthorization of the Violence Against Women Act (VAWA)*, WHITE HOUSE BRIEFING ROOM (Mar. 16, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/16/fact-sheet-reauthorization-of-the-violence-against-women-act-vawa/ [https://perma.cc/7NDY-G584].

defendant was aware of a substantial risk that the person depicted in an image expected it would remain private and that they did not give consent to its distribution.[137]

Currently, only four states have laws specific to deepfaked pornographic media.[138] Georgia's prohibition on nude or sexually explicit electronic transmissions makes it a criminal offense to share or post images or videos of "nudity or sexually explicit conduct of an adult, *including a falsely created videographic or still image*" without the consent of the depicted person.[139] Virginia amended its nonconsensual pornography statute to include "a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic."[140] In October 2019, California Governor Gavin Newsom signed AB 602 into state law, which provides a private cause of action for individuals to sue creators of deepfake pornography.[141] California defines "depicted individual" as any individual "who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in an altered depiction."[142] Finally, New York's nonconsensual pornography statute, which creates a private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual defines "sexually explicit material" as "any portion of an audio visual work that shows the depicted individual performing in the nude," making the language broad enough to accommodate deepfake pornography claims.[143]

D. *Section 230 of the Communications Decency Act*

Another obstacle to redress for victims of deepfakes is Section 230 of the Communications Decency Act, which protects Internet service

137. VICTORIA L. KILLION, CONG. RSCH. SERV., LSB10723, FEDERAL CIVIL ACTION FOR DISCLOSURE OF INTIMATE IMAGES: FREE SPEECH CONSIDERATIONS 2 (2022).

138. Karen Hao, *Deepfake Porn Is Ruining Women's Lives. Now the Law May Finally Ban It*, TECH. REV. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/ [https://perma.cc/2L5G-ZPJ8].

139. GA. CODE ANN. § 16-11-90(b)(2) (2021) (emphasis added).

140. VA. CODE ANN. § 18.2-386.2.A. (2014).

141. CAL. CIV. CODE § 1708.86 (West 2020); *see* Carrie Mihalcik, *California Laws Seek to Crack Down on Deepfakes in Politics and Porn*, CNET (Oct. 7, 2019, 8:32 AM), https://www.cnet.com/news/politics/california-laws-seek-to-crack-down-on-deepfakes-in-politics-and-porn/ [https://perma.cc/F4JB-VYRJ] ("[Gavin Newsom] also signed AB 602, which gives Californians the right to sue someone who creates deepfakes that place them in pornographic material without consent.").

142. CAL. CIV. CODE § 1708.86(a)(4) (West 2020).

143. N.Y. CIV. RIGHTS LAW § 52-c(e) (McKinney 2021).

providers from liability for content published by users on their portals.[144] Deepfakes come, in many cases, with an attribution problem: technologies may be employed to allow the creator to remain anonymous, such as disconnecting IP addresses from the post.[145] Identifying the creator of a deepfake, therefore, may be impossible.[146] Absent an identifiable defendant, a plaintiff may only be able to pursue the disseminator of the deepfake—the host website or social media platform.[147] Yet under Section 230, host websites may not be held liable for publication of pictures or videos posted by a third party or any damage it causes—whether illegal or not—which leaves only the producer of the deepfake potentially liable for the harm.[148] Because of this, Section 230 essentially leaves victims with no practical recourse. However, it is worth noting that the scope of the act does not cover intellectual property breaches, so if a party holds copyright to the image, the takedown request must be executed pursuant to the Digital Millennium Copyright Act.[149]

Repealing Section 230, however, would likely raise constitutional First Amendment issues. Instead, legal expert Mary Anne Franks, president of the Cyber Civil Rights Initiative and a professor at the University of Miami School of Law, has argued that federal identity theft law should be amended to frame social media users as the consumers of content and therefore invoke consumer protection rights.[150] Doing so would place the distribution of deepfake content alongside the misappropriation of information such as names, addresses, or social security numbers, and would serve as a powerful deterrent against the distribution of malicious deepfakes.[151]

144. *See* 47 U.S.C. § 230(c)(1) (providing that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider").

145. Danielle Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for National Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1792 (2019).

146. *See* Gieseke, *supra* note 58, at 1495 ("Producers of deepfake pornography can simply vanish from the internet—or take precautions to ensure that they cannot be tracked down.").

147. Reid, *supra* note 98, at 218.

148. Gieseke, *supra* note 58, at 1494.

149. Karolina Mania, *The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective*, 24 SEXUALITY & CULTURE 2079, 2086 (2020).

150. Mutale Nkonde, *Congress Must Act on Regulating Deepfakes*, MEDIUM (June 17, 2019), https://onezero.medium.com/congress-must-act-on-regulating-deepfakes-1e7e94783be8 [https://perma.cc/29M4-CC6Z].

151. *Id.*

E. *DEEP FAKES Accountability Act*

On April 8, 2021, Representative Yvette Clarke (D-NY) introduced the DEEP FAKES Accountability Act into Congress.[152] The bill, whose acronym stands for "Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act," aims "[t]o combat the spread of disinformation through restrictions on deep-fake video alteration technology."[153]

In its attempt to limit the potential damage of synthetic media which appears to be authentic, the DEEP FAKES Act would require anyone creating a piece of fabricated media that imitates a person to disclose that the video is altered or generated using AI, by placing "embedded digital watermarks" on the content, as well as textual descriptions accompanying the image or video.[154] If the altered content contains audio, the piece must also include a "clearly articulated verbal statement that identifies the record as containing altered audio and visual elements, and a concise description of the extent of such alteration."[155] Failing to do so would be a crime.[156]

The proposed Act would also establish a private cause of action for victims of deepfaked media, which it terms "advanced technological false personation," to sue the creators and vindicate their reputations in court.[157] The bill defines "advanced technological false personation" broadly, providing that "the word 'advanced' within the term advanced technological false personation record shall not be interpreted as narrowing the definition of such term," in order to apply to new technologies as they advance.[158] In order to protect a victim's privacy, these documents may be filed under seal "if such plaintiff can demonstrate a reasonable likelihood that the creation of public records regarding the advanced technological false personation record would result in embarrassing or otherwise harmful publicization of the falsified material activity in an advanced technological false personation record."[159]

Even with these safeguards, however, the proposed act fails to adequately protect victims of deepfaked content, as malicious actors can

---

152. DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. (2021). The proposed Act died in the 117th Congress. *See H.R. 2395 (117th): DEEP FAKES Accountability Act*, GOVTRACK, https://www.govtrack.us/congress/bills/117/hr2395 [https://perma.cc/FK63-RKB6] (last visited Apr. 21, 2023).

153. DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. (2021).

154. *Id.* § 2.

155. *Id.*

156. *Id.*

157. *Id.*

158. *Id.*

159. DEEP FAKES Accountability Act, H.R. 2395, 117th Cong. § 2 (2021).

remain anonymous while easily circumventing the Act's requirements. Watermark and other metadata-based markers are usually trivial to remove; text can be cropped, logos removed, and even a sophisticated whole-frame watermark can be eliminated simply by being re-encoded for distribution on a different platform.[160] Though the Act included the creation of several task forces and coordinators to provide victim assistance, it includes no real enforcement mechanism. Though the Act would create a task force at the Department of Homeland Security that would lead the charge against combatting deepfakes, the taskforce would serve more of a research and reporting function, as well as collaborating with private sector companies such as social media platforms in their attempts to prevent malicious deepfakes.[161] Altogether, the Act conceives of deepfakes as a labeling issue, whereas real prevention and redress would require measures far more tailored to the harm the technology poses.

III. RECOMMENDATIONS

Based on the earlier mentioned issues surrounding deepfakes and the existing legal remedies, the federal government should amend the Violence Against Women Act Reauthorization Act with a broad enough definition to encapsulate nonconsensual deepfake pornography. Additionally, the federal government should provide a definition of deepfakes. Even if no federal deepfake definition is ultimately provided, states should create their own deepfake laws. In order for state nonconsensual pornography laws to apply to victims of deepfake pornography too, states must amend their laws to remove intent-to-harm and reasonable expectation of privacy requirements and expand the definition to include deepfake depictions.

CONCLUSION

Regulation of deepfakes is essential due to the negative consequences that could arise on both the individual and national levels from the malicious use of the technology. A multi-faceted approach to combating malicious deepfakes is necessary, and an effective one would include amending federal and state legislation, as well as coordination with social media networks and Internet companies. The law often lags behind technology, and until proper legal measures are put into place, the best strategy to combatting deepfake harms may be education. The Zelenskyy

160. Devin Coldewey, *DEEPFAKES Accountability Act Would Impose Unenforceable Rules—But It's a Start*, TECHCRUNCH (June 13, 2019, 3:25 PM), https://techcrunch.com/2019/06/13/deepfakes-accountability-act-would-impose-unenforceable-rules-but-its-a-start/ [https://perma.cc/R2W6-JJPC].

161. *Id.*

deepfake gained no traction, in part, because the public had been warned. A knowledgeable public who is aware of the deepfake phenomena and looks at media with a questioning mind may be the best tool to combat the harms that deepfakes can inflict.