VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

EXTENDED PRIVACY FOR EXTENDED REALITY: XR TECHNOLOGY HAS 99 PROBLEMS AND PRIVACY IS SEVERAL OF THEM

Suchismita Pahi & Calli Schroeder

Americans are rapidly adopting innovative technologies which are pushing the frontiers of reality. But, when they look at how their privacy is protected within the new extended reality (XR), they will find that U.S. privacy laws fall short. The privacy risks inherent in XR are inadequately addressed by current U.S. data privacy laws or court-created frameworks that purport to protect the constitutional right to be free from unreasonable searches. Many scholars, including Ryan Calo, Danielle Citron, Sherry Colb, Margaret Hu, Orin Kerr, Kirsten Martin, Paul Ohm, Daniel Solove, Rebecca Wexler, Shoshana Zuboff, and others, have highlighted the gaps in U.S. privacy protections stemming from big data, artificial intelligence, and increased surveillance technologies.

However, the depth and breadth of what XR technology reveals about a person, the risks it poses to bystanders, and the imminent paradigm shift of a public space versus a private space are new problems. This paper provides three central contributions for technologists, legislators, and anyone interested in privacy rights: first, a brief guide to understanding XR technology; second, a survey of the current U.S. privacy landscape and the gaps in U.S. privacy protections for XR; and third, an easily digestible list of solutions that legislators and technologists can pursue to better protect privacy in XR.

EXTENDED PRIVACY FOR EXTENDED REALITY: XR TECHNOLOGY HAS 99 PROBLEMS AND PRIVACY IS SEVERAL OF THEM

Suchismita Pahi & Calli Schroeder[*]

"*I forgot I was in virtual reality and I got grounded, and now I'm grounded in real life.*"

- Leopold "Butters" Stotch[1]

INTRODUCTION

Augmented Reality, Virtual Reality, and Mixed Reality (collectively, "extended reality" or "XR") are poised to explode in use in the United States ("U.S.").[2] XR technologies present unique risks to privacy by enmeshing the real world with the imagined. XR technologies exacerbate existing privacy concerns related to artificial intelligence and big data and introduce new privacy risks for bystanders. On top of these risks, existing privacy regulations that address virtual or real-world privacy issues fail to adequately address the convergence of realities that exists in XR. These privacy risks heighten the urgency of developing substantive protections for both users and bystanders from privacy intrusions previously only imagined in cyber dystopian fiction.[3]

XR technologies typically involve one or more wearable devices that include cameras, microphones, and sensors that collect a vast array

[*] This paper is the result of 2 years of virtual collaboration during the chaos of the pandemic(s). We would like to express our deep gratitude to fellow practitioners who have taken the time to read and comment, or otherwise provide thoughtful feedback, challenge assumptions, and provide assessments and encouragement throughout this endeavor: Alyssa Feola, Madaleine Gray, Mike Hintze, Joel Scharlat, Ben Steinberger, and our families for their support, with apologies to anyone whom we might have omitted. The views in this paper do not reflect the views of either of our employers: Databricks, Inc. or the Electronic Privacy Information Center (EPIC).

[1] *South Park: Grounded Vindaloop* (Comedy Central broadcast Nov.12, 2014).

[2] 4 PERKINS COIE LLC ET AL., 2020 AUGMENTED AND VIRTUAL REALITY SURVEY REPORT (2020), https://www.perkinscoie.com/images/content/2/3/v4/231654/2020-AR-VR-Survey-v3.pdf; Magic Leap, *Demos: Waking Up with Mixed Reality,* YOUTUBE (Apr. 19, 2016), https://youtu.be/GmdXJy_IdNw (an example of "Mixed Reality").

[3] *See, e.g.,* MASAMUNE SHIROW, GHOST IN THE SHELL (1st ed. 1989); LAUREN BEUKES, MOXYLAND (2008); PHILIP K. DICK, UBIK (1969); Ray Bradbury, *The World the Children Made*, SATURDAY EVENING POST (Sept. 23, 1950).

of information about the user and their environment.[4] And XR data collection and use does not stop at external data or solely physical data or even inferences from that data. XR technology also includes neural activity tech, such as brain-computer interfaces (BCI), that companies are developing to make the XR experience less clumsy and more intuitive.[5] As the technology advances, these devices will inevitably become more ubiquitous. They can collect information about not just the user, but also bystanders—which could be children, strangers, intimate partners, or anyone else. And their portability means that they collect information not just within the intimacy of the user's own home (which itself raises a several potential privacy and safety concerns) but also a wide range of public and private places—including hospitals, shelters, restrooms, places of worship, and more.

Current U.S. privacy regulation has failed to evolve with technology, leaving Americans at the mercy of a personal privacy trade-off that is often made without the individual's full knowledge. XR technologies are making inroads into businesses, healthcare,[6] schools, marketing, and leisure, generating millions of data points that can be used to extrapolate, infer, and create profiles on users and bystanders alike—and may subsequently be used to manipulate, target, provide, and deny services with limited or no meaningful choices or options for those users and bystanders.[7] This paper enumerates the privacy risks present in and unique to XR and the regulatory gaps in privacy protections from this technology. Please note that the terms "XR," "XR technology," and "XR technologies" may all be used within the paper and collectively refer to the devices and systems used to create and support extended reality.

Potential privacy risks from XR include legal and real-world harms ranging from expanded surveillance and data collection methods for law enforcement and intelligence agencies to long-term harms

---

[4] Keiichi Matsuda, *Hyper-Reality,* YOUTUBE (May 19, 2016), https://youtu.be/YJg02ivYzSs (Keiichi Matsuda, former director of Microsoft and current director of LiquidCity, created a video that demos what to many is the worst case scenario of XR).

[5] *See, e.g.*, OpenBCI, https://openbci.com/ (last visited Nov. 9, 2022) (the open source efforts by OpenSourceBCI to assist in enabling biosensing).

[6] *See, e.g.,* DEEPVR, https://www.exploredeep.com/#about-deep (last visited Nov. 9, 2022) (Deep VR, a meditative reality game developed to interface with head mounted gear and purporting to reduce user anxiety).

[7] Frank Pasquale, *7 Ways Data Currently Being Collected About You Could Hurt Your Career or Personal Life,* HUFFPOST (Nov. 6, 2014, updated Dec. 6, 2017), https://www.huffpost.com/entry/data-collected-hurt-career-personal_b_6110682; Will Knight, *Job Screening Service Halts Facial Analysis of Applicants,* WIRED (Jan. 12, 2021), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.

stemming from corporate black box decision-making for users, bystanders, and households.[8] Our analysis explores the limits of existing U.S. privacy doctrines and of Fourth Amendment protections against unreasonable searches. Current U.S. privacy regulation largely fails to recognize privacy harms for individuals when grounded in loss of data or impacts from data without a direct tie to a financial, physical, or otherwise calculable loss or a historically recognized harm, such as intrusion or unlawful disclosure.[9] This failure is magnified in the big data analytics context and proves particularly insufficient to meaningfully protect individuals in the XR context.[10]

Various technologists recognize that there are privacy problems with big data, including big data processed in XR, and attempt to mitigate these privacy problems through technical measures.[11] However, these attempts are not a substitute for substantive legal privacy protections that fully address XR technologies themselves. Existing regulations are likely to exclude XR due to narrowly tailored scope meant to address a

---

[8] *See* United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001); Carpenter v. United States, 138 S. Ct. 2206 (2018); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (Harvard Univ. Press, 2015).

[9] *See* Jackson v. Abendroth & Russell, P.C., 207 F. Supp. 3d 945 (S.D. Iowa 2016); Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641 (N.D.W. Va. 2016); Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN MONEY (Sept. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide (Ashley Madison's parent company, Avid Life Media, acknowledged the connection between an affected user's suicide and the privacy violation in its statement "Dr. Gibson's passing is a stark, heart-wrenching reminder that the criminal hack against our company and our customers has had very real consequences for a great many innocent people."); Letter from Senator Ron Wyden to Avril D. Haines, Director, Nat'l Intel. (Apr. 13, 2021) (on file with author) https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf.

[10] Big data is not defined uniformly in the tech industry. However, it can generally be understood to mean large volume, high velocity, and variety of data. This means a big data set is going to have a high volume of data that is increasing exponentially and is also large in scope (data types). The data may be structured, unstructured, or both. *See* Univ. Wis., *What is Big Data* (last visited Aug. 25, 2022), https://datasciencedegree.wisconsin.edu/data-science/what-is-big-data/.

[11] Zhi Xu & Sencun Zhu, *SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones*, 2015 CODASPY '15: PROC. 5TH ACM CONF. ON DATA & APP. SEC. & PRIV. 61 (2015) (proposing method to restrict sensor data access and sharing on smartphones); Franziska Roesner, et. al., *World-Driven Access Control for Continuous Sensing*, 2014 CCS '14: PROC. 2014 ACM SIGSAC CONF. ON COMPUT. & COMM'NS SEC. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/wdac-tr.pdf (proposing a method for automated context sensing to protect privacy and limit data collection or disclosure); Jeremy Bailenson, *Protecting Nonverbal Data Tracked in Virtual Reality*, 2018 J. MED. ASS'N PEDIATRICS 905 (raising concerns about the inferences or derivations of medical diagnoses from non-verbal data points gathered by virtual reality technologies).

different technology space. For example, the types of biometrics collected in XR may not trigger regulations targeted at biometrics used specifically as identifiers in existing technologies (e.g., iPhone FaceID), even though the data itself is directly related to biological measurements (e.g. height, gait, heart rate).

In addition to the risks XR poses to user privacy, XR also creates greater and significant risks for bystander privacy. Processing of bystander data poses a crucial unaddressed privacy risk because a bystander does not have awareness that their information is being collected and does not have a way of opting out of said information collection.[12] This is especially problematic in the case of biometric data since neither users nor bystanders have the ability to change that information without surgical intervention or other highly-invasive and class-accessible actions. You can't change your faceprint.

Facebook recently revealed a partnership with Ray-Ban to create eyeglasses that can be used for XR purposes.[13] The glasses are unobtrusive and have to be linked with the user's Facebook account.[14] The only indication to bystanders of these glasses' XR capability is a small red light on the frames.[15] While the Ray-Ban capabilities are currently relatively limited, it is a foray into XR that can only grow and immediately implicates bystander privacy by allowing recordings that are not easily detectable by the bystander. These recordings are not necessarily secret, but they are also not easily detected and are unexpected by the general U.S. public. Facebook's repeated overtures into the "metaverse," including rebranding as "Meta Platforms, Inc." to demonstrate its commitment to XR, add to already existing concerns about the massive data repository that will be available to Facebook to use at will if it moves virtually unregulated into the space.[16]

---

[12] While notice and choice paradigms are common, post-user experience and user interaction design phases, the choice/consent opt-in opt-out format often leads to an overwhelming set of choices for users. This problem has been explored by others in much more detail and we will not rehash these arguments here. *See, e.g.*, Richard Warner, *Notice and Choice Must Go: The Collective Control Alternative*, 23 SMU SCI. & TECH. L. REV. 173 (2020); Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy,* NEW AM. (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/.

[13] Lucas Matney, *Review: Facebook's Ray-Ban Stories Make the Case for Smart Glasses,* TECHCRUNCH (Sept. 9, 2021, 12:02 PM), https://techcrunch.com/2021/09/09/facebooks-first-smart-glasses-make-the-case-for-face-worn-wearables.

[14] *Id.*

[15] *Id.*

[16] *Facebook Wants to Lean into the Metaverse. Here's What It Is and How It Will Work,* NPR (Oct. 28, 2021, 8:20 PM),

Setting aside legislative approaches or judicial norms, we also explore industry standards as a risk-mitigation measure. Users are unlikely to be able to rely on industry self-regulation, as industry expectations can, and often do, diverge from user expectations and may be changed with little notice to or input from users. Industries often make decisions regarding data processing activities that the public is uncomfortable with, highlighting the disconnect in public expectations and industry norms. As a real-world example, Facebook decided to collect data from and keep shadow profiles about non-users.[17] Notably, there are no state or federal regulations preventing companies from creating "shadow" profiles on behalf of users who aren't engaged with a product. Facebook, from a legal perspective, could assume creating profiles in this manner was a reasonable choice. But, from a transparency and user expectations perspective, it was evident that Facebook shot far above the target, as many non-Facebook users demonstrated discomfort with the concept of profiles created for them without any affirmative actions on their part.[18] This conflict demonstrates the misalignment between permitted uses within self-regulatory systems and individual expectations. Further, this example could easily expand in the XR space to detailed profiles being created on bystanders, including sensitive information, such as biometric information, location information, and more.

As another example of the unreliability of industry self-regulation, Facebook reassured Oculus users that they would not be required to tie their devices to a Facebook account.[19] This provided users with some assurance where they may have been interested in the gaming

---

https://www.npr.org/2021/10/28/1050280500/what-metaverse-is-and-how-it-will-work.

[17] *See, e.g.*, Russell Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense,* VERGE (Apr. 11, 2018, 3:53 PM), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy; Andrew Quodling, *Shadow Profiles - Facebook Knows About You, Even If You're Not on Facebook,* THE CONVERSATION (Apr. 13, 2018, 2:41 AM), https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804; Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account*, VOX (Apr. 20, 2018, 1:02 PM), https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg.

[18] Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met,* GIZMODO (Nov. 7, 2017), https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691.

[19] Adi Robertson, *Facebook Is Making Oculus' Worst Feature Unavoidable*, VERGE (Aug. 19, 2020, 7:04 PM EST), https://www.theverge.com/2020/8/19/21375118/oculus-facebook-account-login-data-privacy-controversy-developers-competition.

environment but did not want to include personal information in a Facebook account for other Facebook uses. Facebook later pivoted and announced that Oculus users would now require a Facebook account to login and use new headsets, leaving users no recourse but to tie their Facebook account identities (including the identities that had been previously built by Facebook for users without a formal account) to an XR device.[20] The only other option for users was to stop using Oculus, a device which they'd purchased based on Facebook's prior representations. These examples demonstrate the potential harms of leaving XR solely to self-regulation without representation for user and bystander interests. Not only is there the risk of a disconnect between public expectation and company decisions, but individuals are often left with few options to mitigate or control any exposure or damage to themselves and their personal information. Increasing forays into XR carry correspondingly increasing privacy risks and must be addressed with privacy protections before becoming irrevocably ingrained in our society.

Current privacy protections in the U.S. have proven unable to adapt to changing privacy risks, including those raised by XR.[21] Similarly, in the context of the Fourth Amendment, existing legal protections from government intrusion are stretched thin in their applications to new technologies.[22] Between the U.S. Supreme Court's discomfort with the third party doctrine, which removes privacy protections surrounding information provided to a third party, and its decision in *Carpenter*, it appears that the judiciary is catching on to the threats that newer technologies pose to constitutional rights.[23] However, applying Fourth Amendment law as it stands today would still allow the government to ask for and receive a company's records of a user's interactions with XR technologies. This could include not just standard data points, but telemetry, metadata, and derived or inferential information—sleeping habits, travel patterns, social interactions, communications content with other users, emotional state, behavioral or cognitive patterns, and

---

[20] *Id.*

[21] *See* Katitza Rodriguez & Kurt Opsahl, *Augmented Reality Must Have Augmented Privacy,* ELEC. FRONTIER FOUND. (Oct. 16, 2020), https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy.

[22] *See* Charles Ornstein, *Privacy Not Included: Federal Law Lags Behind New Tech*, PROPUBLICA (Nov. 17, 2015, 11:00 AM EST), https://www.propublica.org/article/privacy-not-included-federal-law-lags-behind-new-tech.

[23] United States v. Jones, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring); Carpenter v. United States, 138 S. Ct. 2206 (2018).

more.[24] Any restrictions on this type of data sharing would rely on both the discretion of the third party company and whether a court chose to apply the framework in *Carpenter*, as we discuss in more depth later in this paper.

In Part I, we aim to explain XR technologies, the scale of data collection within XR, and the personal data collection and use that these systems enable. Once we have established the technology and some of the privacy risks therein, Part II supplies a summary of existing privacy regulation and case law—both in the private sector and within government—and identify privacy risks inherent in XR technologies currently unaddressed in the U.S. regulatory framework. Finally, we propose some possible approaches to bridge these privacy gaps and ensure privacy protections for both users and bystanders in XR.

I. BACKGROUND

A. What is Extended Reality?

Extended Reality (also sometimes referred to as "crossed reality" and referred to herein as "XR") is an industry term referring to a spectrum of immersive computing that enables users to cross boundaries and build real-time connections between the physical world and the virtual world.[25] XR allows users to interact with an environment that is on a sliding scale of real and virtual elements. Users see and interact with characters or objects that are not "real" or "physical" using hardware and software.[26] Though initially developed primarily for gaming, XR uses are rapidly expanding into other areas, such as enabling remote surgeries or

---

[24] *See* INFO. COMM'R'S OFF., 2.2 BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 6–7 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[25] Clay Bavor, *Virtual and Augmented Realities: Asking the Right Questions and Traveling the Path Ahead*, MEDIUM (May 17, 2017), https://medium.com/@claybavor/virtual-and-augmented-realities-asking-the-right-questions-and-traveling-the-path-ahead-2428b9d13c01 (Clay Bavor (Google) suggests that the various types of extended reality are better described with terms that underscore how these systems can be layered on top of one another or layered together. His suggested terms include: "computing with presence, physical computing, perceptual computing, mixed reality, or immersive reality."); *see also Extended Reality (XR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/extended-reality-xr (last visited Nov. 9, 2022) (Defined therein as "a fusion of all the realities—including Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR)—which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures.").

[26] *See also Extended Reality (XR), supra* note 25.

creating interactive virtual classrooms.[27] Experts predict that consumer spending on XR will rise from $5 billion spent in 2018 to $40 billion in 2023 while industry spending outstrips it, surging from $4 billion to $121 billion in that period.[28]

Perhaps most critically, XR is enabled by millions of different data points that, among other uses and purposes, identify the user and incorporate them into the XR world.[29] These data points include physical body movements and patterns (hands, eyes, head, gait, full body tracking), feedback from the environment and surroundings (sound, visuals, location), biometrics (blood pressure, pulse oximetry, respiration, voice prints, face prints), and responses to haptics.[30] Many of these data points, including physical body movements and patterns, biometrics, individual haptic responses, and more, will also be considered personal data, as they link to an individual.

1. Types of XR

XR is generally used as an umbrella term, referring collectively to three types of digital and physical reality combinations: Mixed Reality ("MR"), Augmented Reality ("AR"), and Virtual Reality ("VR").[31] At the leftmost point of the reality spectrum, you'll find the real-world environment. As you slide along the spectrum to the midpoint, Augmented Reality, you'll find Snapchat and Pokémon GO as the services exist now—overlaying characters, items, and scenery enhancements over a user's existing physical environment.[32] As you reach the rightmost

---

[27] Laurence Morvan, Francis Hintermann, & Armen Ovenessoff, *Preparing for the Risky World of Extended Reality*, MIT SLOAN MGMT. REV. (Dec. 17, 2019), https://sloanreview.mit.edu/article/preparing-for-the-risky-world-of-extended-reality/.

[28] *Id.*

[29] *See, e.g.*, Bailenson, *supra* note 11.

[30] *See, e.g.,* Jeremy Greenberg, *Seven Questions to Ask if You Have XR on Your Holiday Wish List,* FUTURE PRIV. F. (Dec. 16, 2020), https://fpf.org/blog/seven-questions-to-ask-if-you-have-xr-on-your-holiday-wish-list/; Smarter Every Day, *A Real Life Haptic Glove (Ready Player One Technology Today),* YOUTUBE (Mar. 1, 2018), https://youtu.be/OK2y4Z5IkZ0 (as an example of what haptics can look like in VR interfaces).

[31] *See, e.g.,* National Institute of Standards and Technology (NIST) Extended Reality Community of Interest (XR COI); *Extended Reality (XR)*, *supra* note 25.

[32] *See* Julia Tokareva, *The Difference Between Virtual Reality, Augmented Reality and Mixed Reality*, FORBES (Feb. 2, 2018, 5:28 PM EST), https://www.forbes.com/sites/quora/2018/02/02/the-difference-between-virtual-reality-augmented-reality-and-mixed-reality/?sh=3c89df892d07; *Demystifying the Virtual Reality Landscape*, INTEL, https://www.intel.com/content/www/us/en/tech-tips-and-tricks/virtual-reality-vs-augmented-reality.html; Bernard Marr, *The Important Difference Between Augmented Reality and Mixed Reality*, BERNARD

point, you'll find Virtual Reality, where we tip into Oculus Rift or Google Daydream and the entire physical reality is replaced by an artificial reality.[33] Finally, we have Mixed Reality. MR lies between AR and VR on this spectrum, but it is not simply a blend of AR/VR and the real-world environment.[34] It is instead an experience that blends the real-world environment with digitally created content, be it sound, sight, or touch, in such a way that the environments coexist and interact with each other.[35] Perhaps the best example of MR, as of the date of this writing, is Microsoft HoloLens 2 and Phillips' Azurion platform, in which surgeons wear a headset designed to enable them to manipulate 3D images and models and guide them during minimally invasive surgeries.[36]

2. Technical Definitions

While these are commonly understood definitions of the terms below, we do not purport that these definitions are universally accepted.[37] However, definitions are critical for policymaking, so we have provided the definitions we are generally using in this paper for clarity.[38]

MARR & CO., https://bernardmarr.com/default.asp?contentID=1912 (last visited Aug. 27, 2022).

[33] *See* Tokareva, *supra* note 32; *Demystifying the Virtual Reality Landscape*, *supra* note 32; Marr, *supra* note 32.

[34] *See* Nancy Gupton, *What's the Difference Between AR, VR, and MR?*, FRANKLIN INST. (last updated Jan. 6 2020), https://www.fi.edu/difference-between-ar-vr-and-mr; Tokareva, *supra* note 32.

[35] *See* Tokareva, *supra* note 32; *Demystifying the Virtual Reality Landscape*, *supra* note 32; Marr, *supra* note 32.

[36] *See* Michele Cohen Marill, *Hey Surgeon, Is That a HoloLens on Your Head?,* WIRED (Nov. 21, 2019, 7:00 AM), https://www.wired.com/story/hey-surgeon-is-that-a-hololens-on-your-head/; *Philips and Microsoft Showcase Augmented Reality for Image-Guided Minimally Invasive Therapies,* DIAGNOSTIC & INTERVENTIONAL CARDIOLOGY (Feb. 25, 2019), https://www.dicardiology.com/content/philips-and-microsoft-showcase-augmented-reality-image-guided-minimally-invasive-therapies.

[37] Franziska Roesner et al., *Augmented Reality: Hard Problems of Law and Policy,* 2014 ACM INT'L JOINT CONF. ON PERVASIVE & UBIQUITOUS COMPUT. (UBICOMP '14): ADJUNCT PUBLICATION 1283 (2014). Other legal scholars have distilled the general properties of XR to include: sensing properties about the physical world; processing in real time; outputting information to the user, including via visual, audio, and haptic means, often overlaid on the user's perception of the physical world; providing contextual information; recognizing and tracking real-world objects; and being mobile or wearable.

[38] These definitions are taken and expanded from The XRSI Definitions of Extended Reality (XR). *See The XRSI Taxonomy of XR*, XR SAFETY INITIATIVE, https://xrsi.org/definitions.

Augmented Reality[39] typically "overlays digital or digitally-created content on top of a real-world environment," such that a user viewing the combination through a device (for example, a smartphone, AR headset, or smart glasses) will see both the digital and real-world components integrated into a real-time combination with one another to produce an enhanced and (theoretically) seamless version of reality. Both digital and virtual stimuli (e.g., graphics, sounds) may be incorporated into the AR environment in order to complete the full immersive experience. This combination allows for cohesive display, but the digital elements do not interact with the real-world environment as they do in Mixed Reality.

Mixed Reality[40] fully blends the real-world environment with digital and digitally created content, enabling the environments to coexist and interact with one another. In MR, the virtual objects are intended to commingle with and react to the real world as if they are a part of it. For example, an MR display may include digital elements that would display similar lighting patterns as if lit from the same real-world source present in the real-world environment, or sounds may echo or muffle as though they are in the same physical space as the user. As the user interacts with the combined real and virtual objects, the virtual objects should reflect the changes in the environment as would any real object in the same space.

Virtual Reality[41] is a wholly artificial digital environment. VR is composed entirely of three-dimensional virtual images experienced by users via special electronic equipment designed to display an immersive virtual environment to the user, such as a Head Mounted Display ("HMD"). The VR environment may (or may not) be modeled on real-world structures but does not actually display any physical world elements to the user—all visuals and sounds are entirely digitally generated.

B. What Kinds of Data Does XR Collect, Share, or Create?

Much of the data that XR collects, uses within its services, shares with other vendors or third parties, uses to create additional inferences,

---

[39] *Augmented Reality (AR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/augmented-reality-ar (last visited Jan. 19, 2023).
[40] *Mixed Reality (MR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/mixed-reality-mr (last visited Jan. 19, 2023).
[41] *Virtual Reality (VR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/virtual-reality-vr (last visited Jan. 19, 2023).

or otherwise processes are similar to that commonly collected by other tech services. This includes usernames, accounts, logs and records, actions taken, purchases, other users interacted with, preferences, dates of birth, age, and gender. The data may also include location data. However, XR's technical capabilities and broad reach translate into unique and heightened privacy risks to a larger cross-section of individuals.[42] These XR technologies take the existing privacy risks from virtual reality, big data analytics, and biometric data, and merge them together, adding three additional components that are particularly interesting: haptics (and related biometric responses), gathering data in near real-time, and comprehensive bystander risks.[43] While future papers may examine security concerns of XR technology, we focus specifically on the unique privacy challenges and risks in XR.

1. Personalizing Services and Profiling Users

XR collects data in a few ways, key among them being: i) from the end user with knowledge and directly; ii) from end users or bystanders indirectly and likely without knowledge or awareness; and iii) directly from third parties through contractual agreements.

End users input data directly when creating their accounts, setting up their devices, and using those devices. The data collected via this input can include name, username, age, gender, ethnicity, date of birth, sexual preference, physical identification (for example, hair, eye, or skin color), billing address, permanent residential address, financial information, search queries, preferences, and settings.

End users also—frequently without awareness or real knowledge—provide massive amounts of data points about themselves and their environments through their use of XR or XR-enabled devices. The volume of data input is often larger in scale than nearly any other form of technology thus far, particularly relating to recording and analysis of individual movement. A 2018 survey revealed that commercial XR systems typically tracked body movements 90 times per second— meaning that "spending [twenty] minutes in a VR simulation leaves just under 2 million unique recordings of body language."[44] The range of data types include location, verbal communication, physical

---

[42] *See, e.g.*, *CXOs Should Map the Risks of Extended Reality: Study*, CXO TODAY (May 17, 2019, 5:22 PM), https://www.cxotoday.com/news-analysis/cxos-should-map-the-risks-of-extended-reality-study/.
[43] *See, e.g.*, Roesner et al., *supra* note 37, at 1284.
[44] Bailenson, *supra* note 11.

movements and patterns (such as posture, gaze, gestures, physical dimensions, facial expressions, and gait), environment data (such as background, surrounding noises, or visuals), biometrics (such as blood pressure, pulse, breathing patterns, voice, or face prints), or haptic responses.[45] Several of these data types may also be collected relating to any bystanders picked up by the system sensors or the surrounding environment. These data sets may be combined with additional information from third party sources for additional inferences or other use cases. Examples of such data sets include personal details and account information from third-party systems and services (e.g., XR tech partners) or entirely separate data sets sold or shared with XR companies, such as marketing or advertising files.

The types and scale of data available from XR and third-party sources enable companies with access to the data sets to not just analyze readily viewable patterns and information, but to draw various inferences from the existing data, expanding profiles and overall information. While inferences are already drawn from existing data sets through other technical means, the inferences from XR are set apart by the sheer volume, scale, and type of data collected—particularly involuntary data—and the invasive nature of the inferences beyond those already made accessible by existing technologies. The inferences generated from XR data sets may vary widely by type.[46] They may be health or health-related inferences such as likely illness or injury from changes in activity level or motion types or ongoing physical patterns.[47] For example, researchers compared the reactions and behaviors of students diagnosed with ADHD in a VR environment with neurotypical students' reactions and behaviors to explore hypotheses about

---

[45] *Id.*; Léa Paule, *Data in the XR Industry: Why Do We Need It?*, LAVAL VIRTUAL (May 12, 2021), https://blog.laval-virtual.com/en/data-in-the-xr-industry-why-do-we-need-it/.

[46] *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 506–09 (2019); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

[47] *See* Anthony Cuthbertson, *Google AI Can Predict When People Will Die with '95 Per Cent Accuracy'*, INDEP. (June 19, 2018, 3:32 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-predict-when-die-death-date-medical-brain-deepmind-a8405826.html; Alvin Rajkomar et al., *Scalable and Accurate Deep Learning with Electronic Health Records*, NPJ DIGIT. MED., May 8, 2018, at 1, 2–4; James Cook, *Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine*, TEL. (Oct. 9, 2018, 6:04 PM), https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/.

distractibility.[48] If researchers believe results of studies like this to be accurate in identifying particular reactions and behaviors indicative of the presence of ADHD in a user, this information could then be used to identify or diagnose ADHD through VR, potentially without the knowledge of the user.

Other inference types may include sociological inferences, such as trying to determine a user's economic status based on the type of hardware used with the XR software (possibly by combining this with their geolocation data) or based on a user's engagement in a virtual or augmented reality shopping experience.[49] XR may also be able to draw relational or networking inferences, including social groups in which an individual is active or will be active given the user's profile within XR technologies (this may include any active conditions, preferred XR software, existing ethnic, cultural, religious, or other affiliations, etc.).[50]

Existing technologies run into similar problems. For example, Tesla vehicles process location data, driver profile data, video recordings of environments while driving, and maintenance information.[51] Tesla is also planning to include haptic feedback.[52] However, unlike the Tesla, XR technologies are not limited to one industry, and can include or combine real-time processing, haptics, social interactions, audiovisual engagement, profiles, location data, and maintenance information. The convergence of this information, and the details that XR technologies can gather, is well beyond that seen in existing technologies.

---

[48] Thomas Parsons et al., *A Controlled Clinical Comparison of Attention Performance in Children with ADHD in a Virtual Reality Compared to Standard Neuropsychology Measures*, 13 CHILD NEUROPSYCHOLOGY 4, 363, 374–78 (2007).

[49] *See* José González Cabañas, Ángel Cuevas & Rubén Cuevas, Facebook Use of Sensitive Data for Advertising in Europe (Feb. 14, 2018) (unpublished manuscript) (on file with the 27th USENIX Security Symposium), https://arxiv.org/abs/1802.05030; Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, FIRST MONDAY (Oct. 5, 2009), https://firstmonday.org/article/view/2611/2302; Astra Taylor & Jathan Sadowski, *How Companies Turn Your Facebook Activity into a Credit Score*, NATION (May 27, 2015), https://www.thenation.com/article/archive/how-companies-turn-your-facebook-activity-credit-score/.

[50] *See* Kristen M. Altenburger & Johan Ugander, *Monophily in Social Networks Introduces Similarity Among Friends-of-Friends*, 2 NATURE HUM. BEHAV. 284, 284 (2018).

[51] Brittany Martin, *Your Tesla Is Watching – and Recording – You All the Time,* L.A. MAG. (Mar. 14, 2019), https://www.lamag.com/citythinkblog/tesla-recording-data-privacy/.

[52] Alistair Charlton, *Tesla Wants to Reinvent the Steering Wheel with Touch Control and Haptics*, GEARBRAIN (Feb. 7, 2020), https://www.gearbrain.com/tesla-patent-reinvents-steering-wheel-2645059533.html.

2. Risks of Profiling and Inferences

As we've noted above, XR has enormous potential for wide-spread use across every industry. Technologists are heralding XR as the new internet and investing heavily in it.[53] Current advertising for XR seems to focus on the gaming capabilities of the technology, but XR companies are rapidly expanding. Proposed XR uses include the health industry, the military, and practices such as explosive deactivation or conflict management, education, and workforce training (including surgical, mechanical, and emergency response training), among many other uses.[54]

The risks of XR technology must be carefully considered in light of the broad scope of potential XR use. For example, an XR device may pull data points that enable a company to conclude that a person fits into sensitive or vulnerable categories, such as transgender, labelling them as such within the system. This inference could be used for inappropriate, unethical, or offensive stereotyping by the service itself, by third parties the data is shared with, or the information could be stored in a database that is later hacked. At that point, the individual, through no affirmative action of their own, would purportedly be identified as transgender within the affected data set, now potentially available to the public. This raises questions of what XR technology could mean for individuals belonging to high-risk communities.[55]

3. Let Me Count the Ways - Privacy Risks in XR

While several of the privacy risks in XR technology are also present in other technologies, there are aspects of XR that exacerbate existing risks and, at times, create a level of privacy risk not present elsewhere. For clarity, we break the potential risks into broad categories below:

- Bystander Anonymization

---

[53] Tripp Mickle, *Apple's New Big Bet: Augmented Reality*, WALL ST. J. (June 7, 2017, 8:29 AM), https://www.wsj.com/articles/apples-new-big-bet-augmented-reality-1496779717.

[54] *See Hololens 2 x Healthcare*, MICROSOFT, https://www.microsoft.com/en-us/hololens/industry-healthcare (last visited Aug. 27, 2022) (describing Microsoft's mixed reality device and services for the healthcare industry).

[55] While this threat is not wholly unique to XR, it is still important to highlight the risk.

- Data Type and Volume
- False Data Points and Timeliness
- Misuse
- Special Categories of Persons: Children, LGBTQIA, and Other Marginalized Persons

i. Bystander Anonymization

XR technology is unlikely to solely impact the end users. It will also create almost all of the same risks for bystanders as well, although the severity of the risks may differ. For example, assume that a particular XR technology is built in such a way that it filters or blurs background sound and images, but, during the process, actually retains any verbal communications, facial geometric scanning, and precise location of a bystander(s) that were collected prior to applying the blurring effect, in its data storage. In this case, the risks to the bystander from this XR technology's database (which could result in a skeleton profile of the bystander, among other uses) are arguably at or near the same degree as to the end user of the XR technology. Privacy risks may even be higher. Bystanders have a more difficult time exercising any rights over their data as they are generally unaware that personal information has been collected, likely would not know which company or entity to contact regarding that information, and are largely left unprotected by privacy law.

It is also possible, and even probable, that technologists would prefer to incorporate technological methods to pre-emptively anonymize bystander data or enable users to do the same in the system—through blurring, selective options to enable/disable technology based on signaling, or other means, solely for the efficiency of data storage and surfacing the tech to the end user.[56] For example, engineers may introduce code that ensures certain wearable XR technology is responsive to an environment that looks like a public restroom or

[56] Jaybie A. De Guzman et al., *Security and Privacy Approaches in Mixed Reality: A Literature Survey,* ACM COMPUT. SURV., Oct. 23, 2019, at 1, 4, 13 (A survey of existing research to protect security and privacy in XR technologies.). It is probable that intrinsic input sanitization (e.g., via user-defined policies) or extrinsic input sanitization (e.g., environmental cues to anonymize or replace data) would assist in meeting the need for anonymization. This may also be true of enabling the ability to pseudo-anonymize data. However, there still remains the hazard that on some level, prior to surfacing to the user, the device or service provider is viewing identifiable information of the person. We do not have the technical knowledge to opine as to whether there are hashing, tagging, or filtering methods that may prevent identifiable information from touching the XR devices or services at all.

changing room. At that time, the wearable would cease recording or transmitting in real-time and instead delay the data flow until the wearable no longer detects the restroom environment. This would significantly reduce the privacy risks to bystanders. Again, these types of identity obfuscation or anonymization of bystander data are generally not required by the current U.S. regulatory environment, an environment which we will discuss in detail in Part II.

ii. Data Type and Volume

As mentioned earlier, a single twenty-minute session using XR technology may result in literally millions of data points collected through recordings.[57] These data points are collected for some functional purposes, such as to make the user's movements within the XR as smooth as possible and ensure that reaction time is effectively communicated within the system. However, multiple other uses of these data sets are possible. Due to the volume, consumers are unlikely to have much control or knowledge of all data points collected. For example, micromovements, frequently collected within XR technology, are largely involuntary, and individuals are not able to control them to protect or screen themselves while using the devices.[58] Tracking these micromovements could result in inferences about health conditions or injuries that the individual may not be willing to share or may be wholly unaware of. For example, in non-XR application, researchers have previously been able to use virtual classes and observe movements that indicated a higher likelihood of a particular individual having attention deficit hyperactivity disorder (ADHD) or being on the autism spectrum.[59] A company gathering these data points would then be free to use those health inferences as they choose, including targeting the individual with advertising related to, or attempting to take advantage of, the condition, or potentially sharing their inferences with third parties, such as employers.

---

[57] Bailenson, *supra* note 11 (reviewing the potential inferences about mental and behavioral health that a VR tech product could allow due to its high volume of data points on nonverbal behaviors).
[58] *Id.*
[59] *Id.*

iii. False Data Points and Timeliness

False or old data points are a significant risk of XR technology. Not only could old or inaccurate data lead to improper profiling or potential wrongful actions against the individual, but if a company makes inferences, any inferences based on or including inaccurate information will further skew data about the individual. This could result in concrete harm to the end user or bystander. For example, if the XR device determines that an individual is moving slower when compared to other individuals who are participating in a competition that requires precision and micromovements and combines that with data related to how often the user uses a particular hand to compete, it is possible that the company may profile the user as "average" for reaction time or precision. If a company buys a data set relating to persons who play said type of games, seeking to employ top players, then this could affect job opportunities for that individual. Moreover, the person would never know. If this information was incorrect or based on a temporary injury that has since healed, the individual is unfairly affected by this inaccurate information.

iv. Misuse

XR technology is being put in place by multiple entities, many of which are unlikely to fully disclose data use and sharing practices.[60] This also means that there may be potential for other individuals or entities to access the data collected or inferred from that data set, some of which may be dangerous or discriminatory to the individuals linked to the data. For example, data on movements could be shared with employers to contest work injuries. Discrete functions of XR technology, such as facial or emotional recognition, could be unethically used to discriminate against individuals who are neurodivergent, have physical disabilities affecting their facial expressions, or come from cultures with physical expressions of emotion that vary from the expressions programmed into the facial recognition technology. In addition, depending on access controls, abusive partners may be able to misuse the information to surveil and further control individuals. For example, an abusive partner could access their partner's XR gaming account and track their partner's location, either by viewing real-time locations or location history. They

[60] *See, e.g.*, Edward Ongweso Jr., *Amazon's New Algorithm Will Set Workers Schedules According to Muscle Use*, VICE (Apr. 15, 2021), https://www.vice.com/en/article/z3xeba/amazons-new-algorithm-will-set-workers-schedules-according-to-muscle-use (highlighting an employer's unforeseen use of biometrics and physical information to manage employees).

could access communication logs or interactions to see who their partner has been engaging with. This information may be used to exert control or as a basis for "punishing" their partner by stalking, harassing, or otherwise abusing their partner, either within the virtual environment or by using the XR information to do so in the physical world. Problems of misuse are already cropping up in the virtual reality experience, such as the recent news article describing an immersive sexual assault experience.[61]

v. Sensitive Categories of Persons, Children, Bystanders, LGBTQIA, and Other Marginalized Persons

Certain privacy risks are heightened based on the category of individual to whom the information pertains. The ability to identify and track a person, constrained only by regulations that are not tailored to XR technologies, poses a heightened risk to children, LGBTQIA, immigrants, religious and racial minorities, and other vulnerable and marginalized persons, such as political or social activists. We discuss the nuances of current regulations for sensitive categories of persons below.

An example of a sensitive category of personal information is health data. XR technology is very likely to collect health information, including any health condition that may affect gait, micromovements, gestures, or facial expression. Collection and use of this data is left to the discretion of the XR company. This enables companies to create massive data sets that make motions uniquely telling and could enable companies to theoretically detect deviations from an individual's expected movements, potentially extrapolating injuries, illnesses, or other medical conditions.[62]

Finally, the technology itself may be more likely to make incorrect assumptions of an individual for reasons out of the individual's control. Various facial recognition algorithms that would likely be used for gesture and facial expression tracking have historically had a much higher rate of incorrect identification on darker skin tones and transgender or non-binary individuals.[63] For example, "emotion

---

[61] *Metaverse Builders Grapple with Sex Harassment Conundrum,* FRANCE24 (Jan. 4, 2022), https://www.france24.com/en/live-news/20220401-metaverse-builders-grapple-with-sex-harassment-conundrum.

[62] Bailenson, *supra* note 11.

[63] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROC. MACH. LEARNING RSCH., Feb. 2018, at 1-2; Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image*

detection" for facial expressions may fail in accurately detecting an emotion and displaying the same during a corporate XR off-site, but only for persons for whom the machine learning model had poor data during training and validation, or persons for whom no data was included during training and validation (e.g., darker-skinned individuals or culturally different individuals).[64] There could be real-world consequences for these individuals in terms of management and career trajectory. This incorrect identification problem may affect individual ability to use XR systems easily, which could impact occupational or educational opportunities, or be used maliciously by the state against the persons affected.

II. LEGAL APPLICATIONS AND POSSIBILITIES

To understand why our existing legal structure does not fully address the risks raised by XR technology, we must first delve into the current system of privacy regulation, control, and enforcement. We have divided the U.S. privacy regulatory system into two parts: private sector and law enforcement. Below, we describe how the current U.S. privacy regulatory system works, its scope, its weaknesses, and possible options for closing enforcement gaps related to XR.

A. Private Sector Regulation

U.S. privacy is generally regulated by a patchwork of sector-specific laws, resulting in coverage gaps where personal data falls through the cracks and leaves individuals without recourse for privacy violations, particularly as relates to new and developing technology. This is certainly the case when it comes to the relationship between XR technology and the privacy regulatory landscape in the U.S. We will examine the current state of private sector privacy regulation in the U.S., identifying where it fails to fully cover risks raised by XR technology. After establishing the current state of potentially applicable privacy laws and identifying gaps, we will discuss some possible solutions for addressing those gaps and the remaining privacy risks inherent in XR technology.

Labeling Services, PROC. ACM HUM.-COMPUT. INTERACTION, Nov. 2019, https://dl.acm.org/doi/10.1145/3359246.

[64] We strongly oppose digital phrenology (also known as emotion detection) and want to make clear that mention of it here is in no way a validation.

1. Current State of Privacy Law Overview

The unique risks presented by XR technology pose a complex regulatory problem. As is frequently the case, technology has developed faster than regulations can keep up, creating gaps in privacy protections and standards for U.S. residents. While industry standards, frameworks, or other self-regulatory mechanisms may help to set expectations for ethical behavior, they are often voluntary by nature and lacking in meaningful enforcement, rendering them unable to act as a substitute for substantial regulation.[65]

Existing U.S. privacy laws address individual rights over personal information, place appropriate restrictions on collecting and using personal information, and impose publicity and notice requirements for personal data breaches, particularly where the breaches include certain data elements. However, these laws are not comprehensive in their protections and do not fully capture the risks posed by XR technology. Several are limited according to geography or sector as well. We briefly discuss some examples of inherently limited statutes below.

- The California Consumer Privacy Act ("CCPA") is solely applicable to California residents, leaving other U.S. residents without the same privacy protections. While companies can opt to use the CCPA as a baseline and extend protections to their entire user population or user base, they are not required to do so and individuals not subject to the CCPA cannot make legal claim to those protections.
- The Children's Online Privacy Protection Act ("COPPA") applies to collection and processing of children's information online. However, these protections apply only to information from children under 13 years of age. COPPA may also protect bystander children under 13 years of age if the company has actual knowledge that the bystander children are under 13. However, this still leaves any children over the age of 13 without protections.
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") solely applies to data that is defined as "protected health information" and within the context of processing by covered entities and business associates. Health data or wellness

---

[65] *See* Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, IAPP (June 24, 2014), https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward/; *see also XR Association*, XRA, https://xra.org/ (last visited Nov. 10, 2022); *XR Safety Initiative*, XRSI, https://xrsi.org/ (last visited Nov. 10, 2022); *VR/AR Association*, VRARA, https://www.thevrara.com/ (last visited Nov. 10, 2022).

data that exists outside of the scope of HIPAA is afforded some protections if it falls within the scope of the FTC Health Breach Notification Rule.[66] Note that this does not include genetic information, which falls under the Genetic Information Nondiscrimination Act ("GINA").[67] GINA bars discrimination based on genetic information—however, GINA is not considered a true data protection regulation.[68]

In addition to these statutory regulations, there are also some historically-recognized privacy harms, such as torts of intrusion upon seclusion or public disclosure of private facts. As with the regulations, these are limited in scope and application. Below, we provide a brief summary of many of the existing U.S. privacy regulations and traditionally recognized privacy harms, including the shortcomings of each when applied to XR.

i. The Limited Applicability of Existing Federal and State Statutes

While current U.S. privacy regulations exist at both a state and federal level, these regulations do not constitute full privacy protections. The lack of protections may at times stem from lack of enforcement resources at both the state and federal level. States (Attorneys General) and the Federal Trade Commission are often tasked with investigating allegations of privacy violations and bringing enforcement actions.[69] However, the broad scope of these bodies' remit and the limited resources and staff available can leave individual cases and privacy violations unaddressed due to authorities prioritizing more high-profile cases, allocating resources away from less clear-cut cases that the authorities could potentially lose, or a lack of technical expertise within the groups to take on certain cases.

---

[66] 16 C.F.R. § 318 (2009).
[67] Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff.
[68] *See, e.g.*, Rachele Hendricks-Sturrup, *A Closer Look at Genetic Data Privacy and Nondiscrimination in 2020,* FUTURE PRIV. F. (Mar. 2, 2020), https://fpf.org/blog/a-closer-look-at-genetic-data-privacy-and-nondiscrimination-in-2020/.
[69] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583 (2014); Chair Lina M. Khan, Fed. Trade. Comm'n, Remarks as Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022) (stating that "the realities of how firms surveil, categorize, and monetize user data in the modern economy invite us to consider how we might need to update our approach further yet.").

Beyond regulatory restrictions, the regulations themselves contain scope limitations that leave broad swathes of individuals unprotected. Many state regulations are not only restricted solely to individuals with residency in that specific state, but also exclude various data types, such as information already covered under federal regulations, like health information, financial data, or entity types (bounded by number of employees, revenue, customer-base size, or explicitly excluding non-profits or other entities). Similarly, federal laws are often limited narrowly to an individual industry area or information type (or may apply solely to particular data elements). While bystander data is not intentionally excluded by existing regulation, it is also not explicitly included. In addition, only one existing statute mentions inferential data, which we will later explore in more detail. This leaves both bystander data and inferential data either unprotected or, at best, in a grey area.

In order to provide a broad picture of the major privacy regulations currently in place, what data or individuals are covered by the regulation, and the specific privacy protections provided, we have created the following chart.[70]

[70] We exclude cybersecurity regulations or security-focused data protection regulations from the scope of this paper to remain focused purely on privacy. We have selected certain state laws that are the strongest examples of their particular type (providing for broad data subject privacy rights, addressing biometric information, etc.). This is certainly not an exhaustive list of state regulations, but we note that any state regulation would not provide comprehensive privacy protections across the U.S. as they are limited to solely that state. For a more detailed list of state privacy regulations, please check the International Association of Privacy Professionals' State Privacy Legislation Tracker, available at https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Statutes	**Scope**	**Protections Provided**
California Consumer Privacy Act ("CCPA") and California Privacy Rights Act ("CPRA")	Solely personal data of California residents, includes household information and inferential data.[71] Biometric data is also specifically addressed within the regulation.[72]	Together, the CCPA and CPRA provide the data subject rights similar to those under the GDPR: the right to delete,[73] right to access or right to know,[74] right to correct inaccurate information,[75] right to limit use or disclosure of sensitive information,[76] and the right to opt out of the use of automated decision-making technology on personal data,[77] with the addition of the ability to restrict the sale or sharing of personal data.[78]
Electronic Communications Privacy Act of 1986 ("ECPA")	Wire, oral, and electronic communications, including email, telephone conversations, and electronically stored data. Includes data in transit, at creation, and in storage.[79]	ECPA, which updated the Federal Wiretap Act of 1968 and includes both the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act, prohibits the interception, use, disclosure, or procurement of another person to do so, of any wire, oral, or electronic communications.[80] Interception in this case means accessing the contents of any wire, oral, or electronic communication via electronic, mechanical, or other device.[81] It also protects the contents of

[71] CAL. CIV. CODE § 1798.140(v)(1) (noting that inferential data drawn from personal data elements is, itself, a form of personal data protected under the CCPA).
[72] CAL. CIV. CODE § 1798.140(b) (stating that biometric information includes, among other things, "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.").
[73] CAL. CIV. CODE § 1798.105.
[74] CAL. CIV. CODE §§ 1798.110, 1798.115.
[75] CAL. CIV. CODE § 1798.106.
[76] CAL. CIV. CODE § 1798.121.
[77] CAL. CIV. CODE § 1798.185(a)(16).
[78] CAL. CIV. CODE § 1798.120.
[79] 18 U.S.C. § 2511.
[80] 18 U.S.C. § 2511(1).
[81] 18 U.S.C. § 2510(4).

		files stored by service providers,[82] and mandates court orders for government use of pen registers and trap and trace devices.[83]
Section 5 of the Federal Trade Commission Act ("FTC Act")	Unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[84] This applies to all U.S. consumers affected by the applicable methods, acts, or practices.	The FTC is empowered to bring actions against companies or individuals that engage in unfair and deceptive practices.[85] "Deception" includes any representation, omission, or practice likely to mislead a consumer.[86] "Unfairness" includes any act or practice causing or likely to cause (i) substantial injury; (ii) not reasonably avoidable by consumers; and (iii) not outweighed by benefits to consumers or competition.[87]
Illinois Biometric Information Privacy Act ("BIPA")	The biometric information of Illinois residents (explicitly limited to biometrics used to identify an individual).[88]	Biometric information cannot be collected without the written consent of the data subject.[89] In addition, the regulation limits dissemination or disclosure of biometric identifiers or biometric information to solely circumstances where there is consent or where necessary for a specific purpose (acceptable purposes are limited to completing a financial transaction,

[82] 18 U.S.C. § 2701(a).
[83] 18 U.S.C. § 3121(a).
[84] 15 U.S.C. § 45(a).
[85] 15 U.S.C. § 45(b).
[86] Letter from the Federal Trade Commission, Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[87] 15 U.S.C. § 45(n). In addition, a recent Executive Order urged the FTC to, among other actions, exercise rulemaking authority to address unfair data collection and surveillance practices and other areas that inhibit competition and damage consumer privacy protections. Exec. Order No. 14,036, 86 F.R. 36987 (July 9, 2021), at Section 5(h).
[88] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (including both biometric identifiers (retina or iris scan, fingerprint, voice print, or scan of a hand or face geometry) and biometric information (information based on a biometric identifier and used to identify an individual)).
[89] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b).

		fulfilling a subpoena or warrant, or as otherwise required by law)[90] and completely prohibits private entities profiting off of individuals' biometric information.[91] Data subjects are granted a private right of action under BIPA and may recover significant fines per violation.[92]
Children's Online Privacy Protection Act ("COPPA")	COPPA applies to the personal information of children under the age of 13 on the Internet or online services (meaning services available over or connected to the Internet).	COPPA has a number of requirements for operators of websites or online services directed at children that wish to collect or process personal data obtained from children. These requirements include providing notice and receiving verifiable parental consent prior to collection,[93] limiting what personal data is collected to what is reasonably necessary for the applicable activity,[94] providing information relating to what personal data is being processed for an individual child (when properly requested by a parent or guardian), and providing opportunity to exercise rights to cease processing.[95]
Family Educational Rights and Privacy Act ("FERPA")	FERPA applies to personally identifiable information of children contained in their education records.	FERPA provides parents with certain rights to review and correct their children's education records and generally requires parents to provide written consent before schools receiving certain federal funds share children's personally identifiable information with other parties.[96] These rights of review, correction, and consent pass to students

[90] 740 ILL. COMP. STAT. 14/15(d) (2008).
[91] 740 ILL. COMP. STAT 14/15(c) (2008).
[92] 740 ILL. COMP. STAT 14/20 (2008).
[93] 15 U.S.C. § 6502(b)(1)(A).
[94] 15 U.S.C. § 6502(b)(1)(C).
[95] 15 U.S.C. § 6502(b)(1)(B).
[96] 20 U.S.C. § 1232g(a).

		once they are over the age of eighteen.[97] Institutions receiving the applicable program funds must inform parents and students of these rights as well.[98] However, several exceptions allow for records sharing in certain circumstances,[99] and this regulation is solely applicable to institutions receiving federal funding under an applicable program.[100]

[97] 20 U.S.C. § 1232g(d).
[98] 20 U.S.C. § 1232g(e).
[99] 20 U.S.C. § 1232g(b).
[100] 20 U.S.C. § 1221(c)(1) (defining applicable program as "any program for which the Secretary or the Department has administrative responsibility as provided by law or by delegation of authority pursuant to law.").

Health Insurance Portability and Accountability Act ("HIPAA")[101]	HIPAA applies to Protected Health Information, which is defined as health information created, transmitted, received, or maintained by the following entities, collectively referred to as "Covered Entities" (not exhaustive): health plans, healthcare clearinghouses, healthcare providers, and their Business Associates who process Protected Health Information on behalf of these Covered Entities.[102]	HIPAA provisions are typically divided into what are commonly referred to as the Privacy Rule and the Security Rule.[103] The Security Rule mandates that covered entities maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality of electronic health information in transmission, at rest, and from breaches.[104] The Privacy Rule places limits on how protected health information can be used and disclosed.[105]

ii. Recognized Privacy Harms

In addition to the federal and state statutory privacy protections, the U.S. also has four categories of traditionally recognized privacy torts: intrusion upon seclusion,[106] public disclosure of private facts,

[101] Other federal regulations, such as the Gramm Leach Bliley Act ("GLBA") or the Fair Credit Reporting Act ("FCRA"), regulate data elements, privacy, and security within the financial sector. HIPAA is a portability/data protection regulation, not a privacy regulation specific to privacy rights. However, HIPAA is perceived in the U.S. as a privacy regulation for patient information and has significant privacy impacts, and so we have included it here for that reason.

[102] 45 C.F.R. § 160.102(a)–(b) (2013).

[103] *See Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 11, 2022) , *see also Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Nov. 11, 2022).

[104] 45 C.F.R. § 164.306 (2013).

[105] 45 C.F.R. § 164.502(a) (2013).

[106] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

appropriation of name or likeness, and false light.[107] Of the four categories, intrusion upon seclusion is the most likely to apply within the XR technology context because of XR technology's erosion of the barriers between public and private spaces. XR brings outside viewers and listeners into the user's private space or, through use of visual and auditory sensors, into the bystander's private space, essentially making those private spaces public. Unlike the other three privacy torts, the mere act of XR technology gathering personal information in an "invasive" manner may be enough to constitute an intrusion upon seclusion privacy violation, because intrusion upon seclusion does not require publication of information or use of information.[108]

Intrusion upon seclusion requires that a party "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, [and] the intrusion would be highly offensive to a reasonable person."[109] Initially, court decisions related to this tort turned on physical intrusion. The application of the tort has expanded over time to include any type of intrusion into anything the victim would consider private.[110]

While this single privacy tort may be applicable to XR technology in some cases, the ability of existing tort law to meaningfully address digital threats is suspect.[111] Intrusion upon seclusion is generally understood to only protect information that has been kept wholly secret

---

[107] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[108] Tigran Palyan, *Common Law Privacy in a Not So Common World: Prospects for the Tort of Intrusion upon Seclusion in Virtual Worlds*, 38 SW. L. REV. 167, 171 (2008) ("Moreover, the other three privacy torts deal with the use of information once it has been acquired. Only intrusion redresses invasions of privacy where the acquired information is not used.").
[109] RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).
[110] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (AM. L. INST. 1977) (listing eavesdropping and wiretapping as examples of intrusion).
[111] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 58–59 (2004) (Stating that privacy torts "are not well adapted to regulating the flow of personal information in computer databases and cyberspace."); Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013) (reading that "torts and their standards regarding information privacy are outdated and have not been adequately adapted to take into account new technologies and their effects on information privacy."); Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call For New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J.L. COMM. 393, 423 (2002) ("The tort of intrusion upon seclusion and public disclosure is rejected as a solution to online privacy concerns because most of the personal information obtained online is provided voluntarily by the user."); *see, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997) (holding that the openness of a chat room diminishes a reasonable expectation of privacy in chat).

previously.[112] This reflects a traditional understanding of privacy in law, where privacy exists solely within entirely private spaces or only where information has been kept private to the point of complete secrecy.[113] Because XR technology blurs the line between private and public spaces and collects vast stores of personal data that include publicly-observable information (such as gait, appearance, or physical location), there is arguably a low probability that a plaintiff could demonstrate complete secrecy and, therefore, receive protection under tort law.

Example: Ryan shares interior decorating tips through an XR service that maps her home space and projects spatial dimensions, such as furniture shape, size, depth, and the same for decorations, colors, or other living space components to an audience. This map is then shared with other users of the XR service, enabling other users to "walk" through the space, overlay parts of the space and features of it onto their own space to compare fit, and identify characteristics and details like paint colors and brands, the source of different furniture and decorative pieces, and other materials used. In a recent image of Ryan's living room captured through the service, the door to Ryan's bedroom was cracked open in the background. Through the cracked door, a user was able to zoom in on some visible objects, including a picture frame in which the framed picture was an intimate picture of Ryan and her fiancée. The user enlarged and distributed the image, using it to shame Ryan for her appearance and to out her as being in a relationship with a woman.

Ryan may argue that the use of the image constitutes intrusion upon seclusion since she did not intend to share the image with a broader audience. However, under existing law, this may not rise to the level of intrusion upon seclusion since Ryan's relationship with a woman is known to certain other people (family, friend groups) and therefore has not been kept wholly secret. More importantly, the element of intentional intrusion into private affairs may be difficult to establish in the XR context. Ryan knowingly allowed the XR app to scan her living room and the inclusion of the visible bedroom and the items inside could be considered part of that choice.

---

[112] *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."); SOLOVE, *supra* note 111 at 59.

[113] Benjamin Zhu, *A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations*, 89 N.Y.U. L. REV. 2381, 2396 (2018) (stating that, under current tort frameworks, "an individual maintains a privacy interest in information that has been kept secret, but that interest evaporates if the information is disclosed or made public").

iii. XR Poses Risks Above and Beyond Those Contemplated by Existing Law

It may appear at first glance that the patchwork of state and industry privacy laws affords users a form of informational privacy that could be leveraged to address privacy concerns in XR. However, as discussed above, the statutes are limited in application. They offer protections only for a specific subset of information or a single geographic jurisdiction, carve out information that is regulated by federal statutes (e.g., HIPAA or GLBA or other primary federal regulators), and often include exemptions for certain entities or operations. Similarly, existing tort law is restricted by the idea that the intrusion upon seclusion must be an "intentional" intrusion into something the victim considers "private" and has kept entirely secret. This may not stand against the test of XR technology, where the private and public distinction is blurred. Taken altogether, the patchwork regulatory system leaves large swathes of individuals and their personal data inadequately unprotected and at the mercy of the processing entities.

Of the statutes explored above, the CCPA incorporates the broadest definition of personal information and also specifies that "inferences" constitute personal data.[114] Though this represents the highest level of privacy protection currently available, it is only applicable to California residents and expressly excludes certain federally-regulated entities and information types.[115] In addition, the CCPA mainly focuses on marketing uses of personal information, imposing few limits on information that may be used for "business purposes" and only applying to personal data processed by for-profit entities.[116] Some may argue that the CCPA and CCPA-like statues would cover XR technology if expanded to residents of other states. However, upon close examination, it is apparent that, even if expanded, the CCPA falls short.

Example: Leah is coming up on her third annual review at her software engineering company, BigTech Co., headquartered in California. During her review, her manager pulls up reports from her most recent two sets of Virtual Reality training results and highlights that, while her performance in the training was successful, her heart rate and blood pressure did not meet the company's established internal benchmarks. According to BigTech Co., the benchmark was set by analyzing data en masse across the company and is a reliable indicator

[114] CAL. CIV. CODE § 1798.140(v)(1)(K) (West 2023).
[115] CAL. CIV. CODE § 1798.145(c)(1) (West 2023).
[116] *Id.*

of the ability to work effectively and efficiently in high stress situations and environments. The evaluation states that Leah's results indicate she will likely be a low performer unable to effectively handle stress and BigTech Co. has decided to suspend any raises, bonuses, or promotion considerations. She is now on a performance improvement plan.[117]

Setting aside the employment law ramifications of the example above as beyond the scope of this paper,[118] we first examine the limitations of Leah's privacy rights under the CCPA. Leah's account or user information within the Virtual Reality training certainly constitutes personal data, as does the information related to her heart rate and blood pressure, which is not only personal data, but could constitute biometric information under the CCPA if used to identify Leah.[119] In addition, under the updates to the CCPA contained in the CPRA, biometric information used for identification is considered "sensitive personal information" and would be subject to additional restrictions and protections.[120]

These rights, restrictions, and protections give Leah the right to see the data, understand if the data is being sold to third parties, and also to rectify incorrect data. They do not give Leah a right to restrict the use of the data within BigTech Co., prohibit decisions made internally on the basis of the data, or challenge the benchmarks or interpretation of the data as indicative of potential.

Let us examine the differences in statutory privacy protections if this scenario took place in Illinois. While it may appear that heart rate and blood pressure would be addressed by a biometric regulation like BIPA, this information is actually not protected since it is neither one of the listed biometric identifiers in the regulation (retina or iris scan,

---

[117] *See* Yuki Noguchi, *Virtual Reality Goes to Work Helping Train Employees,* NAT'L PUB. RADIO (Oct. 8, 2019, 7:18 AM), https://www.npr.org/2019/10/08/767116408/virtual-reality-goes-to-work-helping-train-employees (describing current uses of VR to train employees in the workforce).

[118] We also note that, with the passage of the California Privacy Rights and Enforcement Act of 2020 ("CPRA"), the employee data exemption that allows companies to treat employee data differently than consumers for a limited transitional period of time has been extended to January 1, 2023. This scenario treats employee information as it will be treated once this exemption period ends.

[119] CAL. CIV. CODE § 1798.140(c) (West 2023) (stating that biometric information includes, among other things, "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.") (Note that what constitutes using the information to identify an individual may vary in interpretation).

[120] CAL. CIV. CODE § 1798.140(ae)(2)(A) (West 2023).

fingerprint, voiceprint, or scan of hand or face geometry),[121] nor is it clearly being used to identify an individual (a requirement to be considered "biometric information" under the regulation). In fact, BIPA explicitly states that "biometric information" does NOT include information derived from items or procedures excluded under the definition of biometric identifiers.[122]

Leah also has limited rights under tort law. It is unlikely that she could successfully claim intrusion upon seclusion, as she cannot claim the information was meant to be wholly secret. Leah potentially could make a claim that the use of the haptics (here, blood pressure and heart rate) to produce a work plan and evaluate her abilities as a worker constitute a physical intrusion and invasion of her privacy, as she was expecting solely to be graded on her performance in the actual substantive training, but by no means is this argument certain to prevail.

Leah's circumstance above demonstrates a significant privacy concern for end users under the current patchwork system of privacy regulations. There are only certain states in which end users are able to exercise any control over how their data is used or collected. Even in those states, these rights are very limited and insufficient in the XR context. The situation is even more problematic for bystanders. Bystander personal data, including images, voice, or other information, will be picked up by XR technology if they are present in the same area that a user is operating the technology.

Example: It's a cool summer evening and Rob is enjoying a cold beer and a virtual poker game with some friends in his driveway, each of them using their head-mounted displays to do so. About 10 minutes into his hangout, he sees someone in his peripheral vision running down his street. Several minutes later, he hears the sound of tires squealing against the pavement. Three weeks go by and he opens his email to find a note that his poker game account data has been requested by law enforcement in connection with an incident in his area on the date of his virtual poker game.[123]

In this scenario, the bystander whose data was picked up in Rob's poker game may have had certain rights to that data, depending on the area. For example, the CPRA update to the CCPA includes a data subject

[121] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008).
[122] *Id.*
[123] *See, e.g.*, Anastasios Nikolas Angelopoulos et al., *Enhanced Depth Navigation Through Augmented Reality Depth Mapping in Patients with Low Vision*, 9 SCI. REPS., 11230 (2019) (describing the use of Augmented Reality depth mapping to aid visually impaired individuals in navigating the real-world environment).

right to deletion where an individual can request that their data be deleted by the company holding that data, subject to certain exemptions.[124] However, in order to exercise this right, an individual must first be aware that the personal data has been collected by the company—why would a person submit a deletion request to a company unless they suspect that it has any of their personal data? In the example above, the bystander would have to have noticed that Rob was using an XR device, recognized that their activities may have been within the range of capture, be able to identify the company behind the XR device, and possibly have additional information required to fulfill the request (for example, information of the date and time of the collection or the account on which the personal data may have been captured). This level of knowledge on the part of bystanders is nearly impossible to meet and unduly burdensome in the rare cases where bystanders may notice the collection and have the information necessary to make the deletion request.

It may also be tempting to try addressing bystander risks under the protections offered under ECPA—however, that is unlikely to prevail. To successfully bring suit under ECPA, a plaintiff must demonstrate that the defendant intentionally sought to intercept content, as defined within the Wiretap Act.[125] First, as mentioned earlier, a bystander may not be aware that their data is being collected, processed or otherwise accessed by an XR company in real-time and know to bring suit. In this case, the bystander would likely be unaware that they were recorded on Rob's XR device. Second, even if the bystander was aware, they would still need to demonstrate standing (injury in fact and violation of a legally protected interest) and, to date, mere access to information has not been sufficient to establish standing.[126] Third, even if a bystander's suit survived Article III standing challenges, the plaintiff/bystander is likely to face challenges in demonstrating intent. If an XR technology company purposefully collects data in real-time to process it and create profiles, then it is likely that a bystander could demonstrate intent.

The distinction between private and public spaces has been slowly eroded over time by various new technologies (e.g., live video streaming). Bystander information collection and processing through XR technology further blurs the distinction. Bystanders in public spaces may have a reasonable expectation that they will be observed by traditional methods, such as CCTV or news videos. However, the amount of individual

---

[124] CAL. CIV. CODE § 1798.105(a) (West 2023).
[125] 18 U.S.C. § 2511(1).
[126] 18 U.S.C. § 2520.

impressions that may be collected in a short period by XR systems and the analysis of these impressions in a big data context are less anticipated. Put simply, bystanders may anticipate casual observation by a human in a public space, but not observation by or through technology that connects the real-time observation to other data about them.[127] Further, bystander data may be collected in spaces such as private businesses, other individuals' private residences, or even the bystanders' residence, if shared with an individual using an XR system.

These examples demonstrate the pitfalls and gaps inherent in the current privacy regulatory landscape for the private sector in the U.S. While certain claims may be possible in individual cases, protections are far from comprehensive and privacy rights often are restricted to certain geographic and industry areas. We now turn to similar coverage gaps in regulations applicable to law enforcement data collection and use.

B. Government and Law Enforcement

1. Existing Law: Reasonable Expectation of Privacy in a Tech World

Fourth Amendment protections struggle to keep up with developing and new technologies as these technologies increasingly blur the line between public and private areas.[128] XR technology exacerbates the problems facing the courts in applying Fourth Amendment protections to novel situations in which these public and private areas are intermingled or overlaid in not only the physical world, but also an alternate reality. XR data is an entire world in which a person can continuously operate and provides an enormous volume of data—from the second-to-second way someone physically moves, to physical and virtual location history, to information as invasive as blood pressure and heart rate. In this section, we'll briefly discuss the *Katz* test for evaluating

---

[127] *See, e.g.*, Mark Sullivan, *The Making of Mojo, AR Contact Lenses That Give Your Eyes Superpowers*, FAST CO. (Jan. 16, 2020), https://www.fastcompany.com/90441928/the-making-of-mojo-ar-contact-lenses-that-give-your-eyes-superpowers (A startup company is making contact lenses that augment a user's reality. These lenses are not easily identifiable by bystanders, and the device privacy policy is not publicly available on Mojo's website, although there is a contact email address to acquire the same. We did not request this policy.).

[128] *See* Ellysse Dick*, How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces,* INFO. TECH. & INNOVATION FOUND. (Dec. 14, 2020), https://itif.org/publications/2020/12/14/how-address-privacy-questions-raised-expansion-augmented-reality-public/ (Ellysse Dick reviews the history of technology changing the balance between public and private over time and makes policy recommendations for augmented reality in public spaces.).

Fourth Amendment protections for direct government searches and the privacy risks inherent in XR under *Katz*. From there, we will move to *Carpenter* and the third-party doctrine.

Fourth Amendment law purportedly balances protecting the right of people to be secure from unreasonable searches with law enforcement evidence-gathering and investigation procedures.[129] When examining Fourth Amendment protections, the courts assess whether a search by law enforcement abrogates the "reasonable expectation of privacy" discussed in *Katz*.[130] If the court does not find that a reasonable expectation of privacy exists, then it concludes that the search is reasonable and a warrant is not required. While the Fourth Amendment is generally presented as protecting a "reasonable expectation of privacy," a closer examination of Fourth Amendment case law demonstrates that "privacy" is frequently entangled with concepts of ownership and property rights.[131] This conflation of privacy with ownership or property has ushered in an understanding that "private" spaces are those that are privately owned or controlled. The way in which *Katz* has been applied creates a scope problem for Fourth Amendment protections as technological developments increasingly bring the public sphere into private spaces and change what we find to be "reasonable" for privacy expectations in public spaces.[132]

Example: Eliza is suspected of trafficking controlled substances, but authorities do not yet have enough information for a warrant. Eliza is playing an XR massively multiplayer online role-playing game (MMORPG) that incorporates players and their surroundings into the game using headgear and motion sensors placed around the room. Anyone above the age of 13 years can play this game from any part of the world. Eliza likes to play with a background

---

[129] Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 861 (2004) (describing the goal of the Fourth Amendment rules as "a rule-structure that simultaneously respects privacy interests and law enforcement needs").

[130] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (presenting a two-part test in which there must be an actual (subjective) expectation of privacy, and society must be prepared to recognize that expectation as reasonable).

[131] *Id.*; *see also* Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define Limits of the Right Against Unreasonable Searches and Seizures,* 102 MICH. L. REV. 889, 894 (2004) (describing how historically "protecting property . . . has in the past largely encompassed protecting privacy as well").

[132] While we do not address this concept here in this paper, it appears to us there is also simultaneously a thread of broad discretionary authority for the government in its law enforcement capacity, similar to allowances for general warrants, that sneaks its way into the gaps left by the way the courts have currently addressed Fourth Amendment issues in the technology space.

masking filter for location protection. Eliza does not notice that her filter is glitching out whenever she interacts with an object in the game.

The FBI finds out that Eliza is an active player of the MMORPG. An undercover agent poses as a fellow player in the game and observes during gameplay that Eliza has what could be suspicious paraphernalia in a basket when the filter glitches out during a fight between members of the party and several werewolves.

The FBI wants to use a series of screenshots that they have taken from the game which show the suspicious paraphernalia as evidence in the case they are building against Eliza. They contend that their prior actions in obtaining the screenshots are not a warrantless search because Eliza intentionally broadcasted her home to the public by playing the MMORPG and they had lawful right of access to the paraphernalia by virtue of being game players.[133] They argue that the objects they saw were suspicious paraphernalia in plain view.[134] Eliza's attorney argues that her home is not a public space, that Eliza deliberately sought to protect the details of her home from other players to maintain her home as a private space, and that the undercover agent's viewing and screenshots fall outside the scope of the plain view doctrine and instead constitute a warrantless search in violation of the Fourth Amendment.[135]

---

[133] For the purposes of this section, we are setting aside the application of the third-party doctrine, which we will address later in this section; *see also* Dick, *supra* note 128 (describing how augmented reality technology may exacerbate privacy concerns, allowing the public into what were previously considered private spaces and essentially collapsing the boundaries between the two).

[134] Under existing criminal procedure doctrine, evidence in the "plain view" of an officer who has a right to be in a location allowing them to perceive the evidence can gather the evidence without a search warrant. Washington v. Chrisman, 455 U.S. 1, 9–15 (1982) (explaining that an officer lawfully in the dorm room may seize marijuana seeds and pipe in open view). This is the plain view doctrine and is limited by probable cause (e.g., the officer must have probable cause to believe that the items in plain view are contraband).

[135] *See* Ogletree v. Cleveland State University, No. 1:21-cv-00500, 2022 WL 3581569, at *24 (N.D. Ohio Aug. 22, 2022) (The court granted plaintiff's motion for summary judgment, finding that a remote proctoring software room scan of plaintiff's bedroom was an unreasonable search under the Fourth Amendment. The Court dismissed defendant's argument that plaintiff did not have a reasonable expectation of privacy from the room scan in his house, noting "[r]ooms scans go where people otherwise would not, at least not without a warrant or an invitation."); Joseph Cox, *FBI Asked Sony for Data on User Who Allegedly Used PlayStation Network to Sell Cocaine*, VICE (Dec. 3, 2019, 5:24 PM), https://www.vice.com/en/article/zmjp73/fbi-asked-sony-playstation-4-user-data-cocaine-dealer (FBI requests information about PlayStation 4 player's email, chat, game progress, and account interactions in drug investigation).

Under the *Katz* test, it is possible that the court will find: (1) that the screenshots fall within the scope of the plain view doctrine *if* they consider lawful right of access to include viewing Eliza's home through the XR game space instead of actual physical access and acquisition; and (2) that Eliza's participation in the MMORPG is a "knowing exposure" of her home to the FBI and removes her privacy protections for her home. There is also a far-fetched possibility that the court will consider Eliza's attempt to mask her physical reality sufficient to give a head nod to the *Katz* test of a reasonable expectation of privacy and choose to protect the idea of privacy in one's home under property theories.[136] This is an oversimplified example of the struggle that a court applying *Katz* is likely to experience when determining how to protect XR data.

There is substantial debate regarding the nature of the right to a reasonable expectation of privacy, with many eminent scholars arguing that the Fourth Amendment is not the ideal basis for protecting privacy.[137] We agree. Decisions using the *Katz* test, centered on a reasonable expectation of privacy, have resulted in situational rules that seem to only meaningfully protect privacy where information is "private from public perception" or concealed from potential public exposure, leaning into an idea of synonymous privacy and secrecy instead of into a test that equips courts to meaningfully evaluate a reasonable expectation of privacy.[138]

As one might imagine, cases involving analyses of "reasonable expectations" of privacy typically hinge on "knowing exposure" and the

---

[136] Katz v. United States, 389 U.S. 347, 351 (1967) ("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.").

[137] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1519–21 (2010) (capturing perspectives on the circular nature of the reasonable expectation of privacy test and also on the difficulty in determining what is normatively reasonable for society); *see, e.g.*, Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 742 (2019) ("The test is tautological, incoherent, ignores important Fourth Amendment values, gives judges free reign to impose their policy preferences, and, as a practical matter, is notoriously unhelpful. It has failed to protect privacy in many digital forms of information, will shrink the Fourth Amendment's scope as knowledge of privacy threats increases, and is increasingly useless in the Internet age.") (internal citations omitted).

[138] *See* Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1027–28 (2013) (using Fourth Amendment law as a key example in which "[t]aken to the logical conclusion, the secrecy paradigm forces a choice between living the life of a hermit or relinquishing our privacy and, in turn, a key protection against excessive government surveillance").; *see also* Kerr, *supra* note 129 (contrasting various lines of Fourth Amendment cases, such as searches of the home, closed containers, and surveillance law, and identifying the different procedures found in each).

definition of "public."[139] The public may be surprised to know that putting garbage out for the city to collect and dispose of is the same as exposing the contents publicly, allowing any law enforcement officer to go through the trash (no warrant or exception needed, no search involved).[140] Or, as in *Ciraolo*, even if you have a privacy fence around your house, if law enforcement were to fly above the house and view anything problematic within your privacy fence, it is still considered publicly exposed and not protected by warrant or probable cause requirements—regardless of whether you had taken steps, like the fence, to mitigate the risk of it being public to any average viewing perspectives.[141] The courts' strange interpretations of "public exposure" include that one has no reasonable expectation of privacy from surveillance or GPS tracking if you are in a vehicle off of your private property.[142] Then, of course, there are the later in time, more tech-focused decisions in *Kyllo*, *Jones*, and *Carpenter*, which bring us back to one of the core questions posed by the creation and adoption of XR technologies—what is public and what is private for the purpose of Fourth Amendment protections?[143]

---

[139] Katz, 389 U.S. at 351–52; Colb, *supra* note 131 (describing the development of Katz and the way that courts approach the "reasonable expectation of privacy" in a search).
[140] *See* California v. Greenwood, 486 U.S. 35 (1988) (Law enforcement searched through Greenwood's trash bags twice after Greenwood placed the trash on his curb for trash pick-up and seized illegal content. The Court found that this did not violate the Fourth Amendment because of the public accessibility of the trash bags and Greenwood's intent to convey the trash to the trash collector, a third-party.).
[141] *See* California v. Ciraolo, 476 U.S. 207 (1986).
[142] *See* United States v. Knotts, 460 U.S. 276 (1983) (Law enforcement embedded a radio transmitter in a container of chloroform Knotts had ordered from a third party so law enforcement could track the container movement. The Court held that there was not a reasonable expectation of privacy for the container's movement or for the surveillance of the car, while publicly viewable, carrying the container. While the opinion was unanimous, the concurrences marked a wariness to greenlight "augmenting" law enforcement capabilities, and concerns around whether the application of the radio transmitter was truly not a privacy intrusion. The case did not reach the question of whether this was a search under property law because the radio transmitter was added prior to Knotts' possession); *see* United States v. Karo, 468 U.S. 705 (1984) (The installation of a beeper by the DEA in a can the DEA owned prior to being passed off by a confidential informant to a potential suspect was neither a search nor a seizure, however monitoring the beeper while it was within a private residence and not publicly viewable was a search for some of the defendants.).
[143] Kyllo v. United States, 533 U.S. 27, 29 (2001) (considering whether warrantless thermal imaging of a home is a search in violation of the Fourth Amendment); United States v. Jones, 565 U.S. 400, 402 (2012) (considering whether attaching a GPS tracker to the bottom of a car without a warrant and tracking it onto private property is a search in violation of the Fourth Amendment); Carpenter v. United States, 138 S. Ct. 2206, 2214–15 (2018) (considering whether cell site location information (CSLI) collected without a warrant from a third party is a search in violation of the Fourth Amendment).

The distinction is particularly important in an XR-enabled world where employers, healthcare entities, leisure activity providers, education entities, and other industries can choose to provide XR technology that requires a person to provide access to places that were previously private in order to participate in a desired or necessary activity. For example, a dance school may offer students XR-enabled classes using avatars. Perhaps instead of a traditional studio, the courses will be taught in each instructor's personal home studio. Assuming the technology maps more space than solely the studio within the instructor's home, has the instructor knowingly publicly exposed their entire home? For how long? How much data is law enforcement entitled to obtain through this technology? Under *Katz*, the answer is unclear. Perhaps solely the studio will be considered knowingly publicly exposed and the rest of the home would remain a constitutionally protected space that is unknowable without physical intrusion and, therefore, protected under the later decision in *Kyllo*, which we will discuss below. Conversely, perhaps the map of the home—both studio and the remaining rooms/property—will be considered part of the employer's property and not a constitutionally protected area.

2. Moving Away from *Katz*? Fourth Amendment Law Tackles Technology

When the physical and technological realms were more clearly delineated and, in turn, public versus private spheres were more clearly delineated, the pre-*Katz* approach to balancing privacy and law enforcement needs appeared functional. But when new technologies were introduced that blurred the private-public distinction, this balance shifted. It more heavily favored law enforcement needs and *Katz*'s reasonable expectation of privacy test fell apart.[144] Even in *Kyllo*, where the Court grappled with privacy considerations as applied to a new technology and subsequently developed a test that expanded upon a reasonable expectation of privacy, the Court attempted to hold onto the idea of a "home" as inviolable.[145]

In *Kyllo*, law enforcement used a thermal-imaging device trained on a suspect's home to see if the thermal readings would provide evidence

---

[144] *See* Katz, 389 U.S. 347 at 361 (setting forth the test that law enforcement investigations that violate a reasonable expectation of privacy are unconstitutional unless there is a warrant or other exception).
[145] Kyllo, 533 U.S. at 40.

that the person was growing marijuana inside his house.[146] The Court held "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[147] While intended to accommodate the development of new technologies, the decision in *Kyllo* hinges on two factors that when applied do not cleanly provide privacy protections for new technology. According to the Court,

> 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," *Silverman*, 365 U. S., at 512 . . . constitutes a search at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[148]

In the first factor, the Court circumscribed the government's use of devices or technologies to those devices or technologies that are "in general public use." Taken to its logical conclusion, it is possible, though unlikely, that the Court can choose to find that this exact search would be appropriate without a warrant in the event that thermal-imaging technology use becomes widespread and, thus, in general public use. As a second factor, the Court considered whether the thermal reading by the device that enabled law enforcement to conclude that Kyllo had grow lamps for marijuana within the house was information that would "previously have been unknowable without physical intrusion" into a constitutionally protected area. This second factor is dead on arrival in the XR-enabled world where private companies are focused on "erasing the borders between digital and physical" such that physical intrusion will not be required to actually know the layout and content details of an area. While in *Kyllo* the police were using a thermal imaging device from outside the home, XR, if adopted across the general public,[149] will create situations in which users will have to enable "public" access to areas that

---

[146] *Id.* at 29–31.
[147] *Id.* at 40.
[148] *Id.* at 35.
[149] *The Future of Extended Reality*, SKIDMORE CONSULTING GRP., https://skidmore-consulting.com/resources/the-future-of-extended-reality/ (last viewed Aug. 27, 2022) (stating that "extended reality market projected to grow from $42.55 billion in 2020 to $333.16 billion by 2025").

"would have previously been unknowable without physical intrusion" in order to participate in society—including in areas such as workforce training, healthcare visits, education, and more.[150] Physical intrusion will not be necessary in XR instances where companies build entire environments using real-world existing physical characteristics (wind, ambient noises, voices), combined with haptics (smells, sensory feedback for touch) and near real-life avatars or projections of people—the intrusions can be much simpler and be accomplished with the aid of the XR companies.[151] As we will explore later in this paper, it is possible for technology companies to implement design choices that are more privacy-protective and help mitigate this risk.

For at least two reasons, it is likely that a court confronted with an XR-enabled society will consider observations in the XR environment to be lawful searches if they continue to use the reasonable expectation of privacy standard and its offshoots. First, XR will at that point likely be in general public use and the mapping will be novel in a way that defies comparisons made to the "physical intrusion" context. Second, some courts will likely consider using XR-devices or programs to fall within the "third party doctrine," a much-criticized doctrine that we'll address next. It is also entirely possible that a court confronted with an XR-enabled society will continue to draw tortured comparisons to non-technological situations and provide protections to individuals participating in mapped versions of previously constitutionally protected places that exist in the physical, real world. It is equally likely that such comparisons will leave significant gaps and continue the trend of fact-based or situational attempts at protecting privacy through the Fourth Amendment.

Would enabling XR devices to cross-map your reality for the game be the same thing as inviting or trusting a law enforcement person with the details of your home?[152] Will the court carve out areas that are XR

---

[150] *See* Hartzog, *supra* note 138 at 1027–28 (reviewing Daniel Solove's "Nothing to Hide: The False Tradeoff Between Privacy and Security" and declaring that "[T]he secrecy paradigm forces a choice between living the life of a hermit or relinquishing our privacy, and in turn, a key protection against excessive government surveillance").
[151] Sebastian Veldman, *Extended Reality: A New Window in the Digital World*, ACCENTURE INSIGHTS (Mar. 22, 2018), https://www.accenture.com/nl-en/blogs/insights/extended-reality-a-new-window-on-the-digital-world; Jennifer Langston, *"You Can Actually Feel Like You're in the Same Place": Microsoft Mesh Powers Shared Experiences in Mixed Reality*, MICROSOFT: INNOVATION STORIES (Mar. 2, 2021), https://news.microsoft.com/innovation-stories/microsoft-mesh/ (Microsoft introduces Mesh mixed reality functions in office workspaces and medical workspaces).
[152] Hoffa v. United States, 385 U.S. 293 (1966) (finding no Fourth Amendment violation where a confidential informant, trusted by the defendant, remained in the defendant's hotel room while the defendant spoke to his attorneys and shared that

enabled from areas that are blocked from view by physical items?[153] Will the court revisit the "informed consent" used for terms and conditions or click-wrap license agreements, modify it for XR, and determine that societal expectations (here, user expectations) about XR software or hardware can protect "private" spaces or otherwise provide a "reasonable expectation of privacy?"

As we examine the potential interplay between XR technology and existing Fourth Amendment law, it appears very likely that continuing to apply *Katz*, in which the Court referenced "knowing public exposure," will undercut the right to privacy in an XR-enabled society. Even if an XR technology does not seek to map the inside of a home, that same technology can still capture, share, retain, analyze, transmit, and use a house layout, down to the smallest detail, effectively making what was previously a private space knowable to private companies.[154] Furthermore, participation in a society where employment, healthcare, leisure, and general existence moves into various XR environments owned by various private companies will subject a person to being knowable and "in public" or, alternately, knowable and to have made a "choice" to provide information to a private company, with that information then subject to the third-party doctrine.

3. Third Party Doctrine

Prior to 2018, law enforcement could acquire data about individuals from third parties with no limitations or considerations for the individual's "reasonable expectation of privacy." This was true even if the individual assumed that the information wouldn't be redisclosed. The only restrictions on what a third party could disclose were voluntarily created or undertaken by the third party and often dictated by the third

---

information to the government); United States v. Garcia, 997 F.2d 1273 (9th Cir. 1993) (finding no Fourth Amendment violation where police officers posing as apartment hunters arrived at the back entrance of a person's home and saw the person using cocaine).

[153] *See* Maryland v. Macon, 472 U.S. 463, 469 (1985) (Law enforcement may enter a public store front while posing as a customer for the purposes of law enforcement but may not enter areas that are only accessible for employees.).

[154] Roberto Baldwin, *Google Maps' AR Adds Navigation Hints to the Real World,* ENGADGET (Feb. 11, 2019, 3:41 PM), https://www.engadget.com/2019-02-11-google-maps-ar-directions.html (Google Device engaged in reality mapping with AR); *see* Solarflare Studio, *BP Future - Magic Leap Experience*, YOUTUBE (Feb. 1, 2020) (demonstrating a Mixed Reality use of a Virtual Reality headset in which an engineer is manipulating various items within the virtual layout of a space from the comfort of his own home).

party's terms of service, privacy policy, or other internal processes or policies. This was the result of the Third Party Doctrine, first set forth by the Supreme Court in 1976.[155] In the XR environment, the doctrine would easily allow a company to provide any of the following types of data to law enforcement:

- Physical body movements and patterns: hands, eyes, head, gait, full body tracking, responses to haptics
- Environment and surroundings: sound, visuals, detailed location maps
- Biometrics: blood pressure, pulse oximetry, respiration, voice prints, face prints, iris recognition
- Geolocation: This may be detailed or generalized geolocation information.
- Device Information: The types of devices used and how they are connected.
- Behavioral Patterns: Similar to social media, this would include who people interact with, how often, and how they interact.
- Bystanders: physical traits, potentially biometrics, any recorded audio or video, and location information

This is not an exhaustive list by any means and raises the same questions that have been raised many times before by privacy scholars—what happens when this data is combined with other data from data brokers? What will the information reveal? How thoroughly is an individual tracked?[156] It seems that the Supreme Court is cognizant of the troubles posed by advances in technology and the continuation of the third party doctrine and has accordingly expanded Fourth Amendment protections with new technology developments in mind.[157] In a recent case, *Carpenter v. United States*, the Court held that law enforcement's request for cell site location information from the cell company for a

[155] United States v. Miller, 425 U.S. 435, 443 (1976).
[156] *See Surveillance city: NYPD can use more than 15,000 cameras to track people using facial recognition in Manhattan, Bronx and Brooklyn,* Amnesty International (last viewed Aug. 27, 2022) https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/ (Law enforcement data sets that can be combined with XR-enabled device information).
[157] JOSEPH JEROME & JEREMY GREENBERG, AUGMENTED REALITY + VIRTUAL REALITY: PRIVACY & AUTONOMY CONSIDERATIONS IN EMERGING, IMMERSIVE DIGITAL WORLDS at 18 (Future of Privacy Forum, Apr. 2021), available at https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf (Noting *Jones*, *Carpenter*, and *Riley* appear to recognize protections for certain granular types of data despite provision to a third party, and that certain data sets "reveal much more in combination than any isolated record.").

seven-day period constituted a search under the Fourth Amendment because of the depth and breadth of the data this type of request would produce.[158] The Court reached this decision under the *Katz* test, aided by several factors, such as volume of data, the sensitivity of the data (what it reveals about a person), and "the inescapable and automated nature of its collection."[159] Since *Carpenter*, Fourth Amendment scholars have found that lower courts have applied a mix of the "reasonable expectation of privacy" test and the factors set forth in *Carpenter* to determine whether information is protected by the Fourth Amendment, both in cases that would normally be third party doctrine cases, and in cases of direct government surveillance.[160] If courts continue to adopt *Carpenter* for both third party doctrine and direct government surveillance, there is a decent chance that XR technology data will be better protected from Fourth Amendment searches that are at odds with a person's expectation of privacy in their data than XR data would otherwise be under the *Katz* test.

While we wait and see where the Fourth Amendment search cases will go next, we cannot lose sight of the fact that judicial opinions and decisions are, for the most part, retrospective. The harm to an individual will have already occurred before the case arrives in front of a judge, and privacy harms are for the most part, irreparable harms. Instead of waiting for such harms to occur, we encourage both legislators and technologists to act first.

C. Solving for Privacy in the XR-Enabled Environment

There are two possible options we see to address current XR privacy issues. First, legislators could pass new legislation or amend existing legislation to address the existing gaps in privacy regulations. These legislative efforts ought to recognize XR-specific privacy harms

---

[158] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[159] *Id.* at 2223 (The Court specifically held that "In light of the deeply revealing nature of [cell site location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."); *see also* Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law,* UNIV. ILL. L. REV. (forthcoming 2022), available at https://ssrn.com/abstract=4094166 (Tokson sums up the *Carpenter test* as follows: "The revealing nature of the data collected; the amount of data collected; and whether the suspect voluntarily disclosed their information to others." We also recommend reading this paper for an up to date and in-depth treatment of *Katz* and *Carpenter*, as well as for the proposal that the *Carpenter* factors replace the *Katz* test entirely.).
[160] Tokson, *supra* note 159, at 20–23.

and provide protections and remedies for individuals. Second, courts could address the gaps in privacy protections by using case law to expand existing regulations to include XR cases. Practically, the first of these is most likely to prove effective. For this reason, we focus on legislation below and briefly address the potential for courts to bolster privacy and the possibility of XR industry standards.

1. Legislative Solutions

The most promising potential approach to addressing regulatory gaps in privacy protections related to XR technology is through passing updated privacy regulations.[161] Ideally, these updated regulations will strive to be technology neutral with a scope of protections expansive enough to address risks associated with new technologies as they develop and mature. As mentioned earlier in this paper, U.S. privacy law protecting the privacy of personal data in many cases is often limited in scope, applying either on a state-wide or industry basis. However, new regulations need not necessarily follow this trend and could be implemented at the federal level, joining federal regulations that are somewhat broader in scope, such as ECPA or the CFAA. Alternately, regulation could be introduced that incorporates existing privacy law and updates certain portions of those laws for more complete regulatory coverage. Regardless of scope, effective regulation that addresses privacy risks of XR technology should include certain measures. We briefly touch upon inclusions that must be present in any effective XR privacy legislation.

i. Definitions

Personal Data

First, a regulation that effectively addresses privacy risks in XR technology must have a clear definition of personal data.[162] Current regulations can vary widely in their definitions of personal data, in particular when a law is specific to an industry or group.[163] While it is generally agreed that information which clearly identifies an individual

---

[161] *See* JEROME & GREENBERG, *supra* note 157, at 22.

[162] Note that even the agreed-upon term varies across regulations: "personal data," "personal information," and "personally identifiable information" all act as variants without delving into the more sensitive forms of personal data.

[163] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); Gramm-Leach Bliley Financial Modernization Act, 15 U.S.C. §§ 6801–6809; Video Privacy Protection Act, 18 U.S.C. § 2710.

(such as name, address, or phone number) is considered personal data, some regulations are much more expansive (including taking cues from the GDPR definition, which includes "any information . . . related to an identified or identifiable natural person," or expanding the definition to include information that could be linked, directly or indirectly, to an individual *or household* under the CCPA). Many regulations no longer consider information to be personal data if it is "fully anonymized," though the standard for anonymization varies, and some experts have demonstrated that it may not actually be possible to render any personal information completely anonymous.[164] Regulations may also have exclusions for data covered by other privacy regulations.[165]

In order for any new regulation to fully address the privacy challenges raised by XR technology, we propose that its definition of personal data must include both identified and identifiable data (meaning, both data that on its own identifies an individual and data that could, in combination with other data, be used to identify an individual).[166] This distinction would include anything short of fully anonymized data that cannot through any combination or reidentification method be linked to an individual. The definition must explicitly include both inferences made from personal data and pseudonymized data.[167]

XR Technology

In the event that legislators choose to draft regulation that specifically addresses XR technology, there must be a clear definition of what constitutes extended reality to avoid inadvertent loopholes for XR or other technologies from which legislators seek to proactively mitigate privacy risks. For example, the Extended Reality Association (XRA) adopts a broad definition and defines XR to include AR, VR, MR (also defined terms), and "other forms of alternate, expanded, or immersive reality applications, including those not yet invented."[168] The Extended Reality Safety Initiative (XRSI) considers XR to be "a fusion of all the realities—including Augmented Reality (AR), Virtual Reality (VR), and

---

[164] Paul Ohm, *Broken Promises of Privacy*, 57 UCLA L. REV. 1701, 1737–38 (2010).
[165] *See* California Consumer Privacy Act, CAL. CIV. CODE § 1798.130 (exemption for information covered by HIPAA, GLBA, FCRA, and other federal regulations).
[166] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1817 (2011).
[167] Pseudonymized data is not meaningfully masking the identity of an individual in XR technology considering the volume of data points collected and the analysis, combination, and compilation abilities of the technology processing those data points.
[168] *XR at a Glance*, XRA ASS'N, https://xra.org/xr-at-a-glance (last visited Aug. 27, 2022).

Mixed Reality (MR)—which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures."[169] Unlike the XRA definition, this definition doesn't clearly define AR, VR, or MR. We recommend that legislators adopt a definition that at the very least defines the core terms (AR, MR, VR, immersive realities) and is scoped broadly enough to include hardware and software directly connected to the use, provision, or support of AR, MR, VR, and other immersive realities.

ii. Consistency, Correlation, Conformity

Legislators should take care to ensure that proposed legislation incorporates or references (and does not reduce) existing privacy protections. For example, where a business associate uses an extended reality technology that may access and use PHI, any new privacy regulation should not undermine the protections afforded by HIPAA or stymy the portability and sharing of PHI specifically permitted by HIPAA. Legislators may also choose to help bring the U.S. into step with the privacy regulatory environment abroad by adopting requirements that technology companies provide stronger protections for sensitive data ("special categories of data" as defined by GDPR).[170] This would both make the companies developing these technologies competitive on the international stage and also provide greater protections to the end users.

iii. Privacy Principles

Legislators may also choose to include several "privacy principles"—basic requirements of privacy frameworks that exist in the U.S. and internationally that provide clear guardrails for companies developing XR technology. There are some slight variations on the principles throughout the world, but many remain consistent.[171] For

---

[169] *Extended Reality (XR)*, *supra* note 25.
[170] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 38.
[171] *See, e.g.*, *Ten Principles of Privacy Protection*, BRITISH COLUMBIA, https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles (last visited Aug. 27, 2022); Ann Cavoukian, *The 7 Foundational Principles*, PRIV. BY DESIGN (last modified Jan. 2011),

example, the NIST Privacy Framework subcategories include (1) assessing data inputs and outputs for bias, (2) limiting observability and linkability of data (increasing dissociability), (3) limiting inferences, and (4) enabling end users to have control over the processing of their data.[172] The OECD framework includes concepts such as (I) data minimization, (II) data accuracy, and (III) individual data rights (transparency and rectification).[173]

Ideally, a privacy-focused regulation that will impact XR will include requirements addressing the following, pulled from privacy principles across the world:

- Transparency - Individuals must be clearly able to understand the types of data collected from them, the derivative data that may be developed, the purpose of the collection, use, or development, and to where that data is or may be transferred or sold. Individuals should also be informed of and able to understand any automated decision-making processes based on their data (e.g., explainable artificial intelligence).
- Choice - End users must be able to opt-in or opt-out from further collection, use, development, or sharing or sale of their data. This could be granular or it could be at high-level categories. Users must also be able to refuse any data processing not necessary for delivery of the services or use of the technology. The strongest standard would be that any data use that is not strictly necessary be opt-in only.[174]
- Individual Rights - End users must be able to obtain copies of their data, including derived data, correct their data if it is incorrect, and have their data deleted. They should also be able to contest automated-decision making practices based on their data (including inferences).
- Risk Assessments - Companies must be required to assess the impact of the way they plan to collect, use, share, sell, or create personal data (derived or other) and implement greater privacy and/or security controls (including granular opt-in/opt-out) for

---

https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf; Regulation (EU), *supra* note 170, at 35.

[172] U.S. DEP'T OF COM., NAT'L INSTITUTE OF STANDARDS AND TECH., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT VERSION 1.0 (2020).

[173] *See* Ben Gerber, *OECD Privacy Principles*, OECD, http://oecdprivacy.org/ (last modified Aug. 9, 2010).

[174] *See* discussion *supra* note 12.

higher risk data impacts (and higher risk data) or abstain from those data processing practices where risks cannot be mitigated.

- Data Minimization and Retention - Companies should carefully consider the amount of data they collect and otherwise process and lean towards only having purpose-driven collection with robust deletion policies so that they do not hoard databases filled with data.
- Dark Patterns - Companies must be barred from using dark patterns or manipulative design (e.g., forced continuity on subscriptions or user interfaces that automatically opt users into the most disclosure of personal data).
- Bystander Data/Environmental Data - The company must actively engage privacy-protective technology for non-end users and must not collect environmental data where the data may include minors or vulnerable populations (e.g., pregnant women, LGBTQIA+ persons). This would be something companies would assess and tailor depending on the environment in which the technology is deployed.
- Law Enforcement - Requests for data held by companies must require a warrant for law enforcement to be able to access the data.

iv. Bystander Data

As noted above in the example where bystander information is picked up in Rob's XR poker game, XR technology is able to pick up bystander information both in greater volumes than may be reasonably anticipated and within spaces the bystander may believe to be more private than public. In addition, bystanders have a much greater challenge before them to exercise any rights they may have in their personal data. Proposed regulations should take into consideration bystander risk and enshrine bystander rights. Possible approaches to establishing privacy rights for bystanders could include technical fixes, such as mandating XR technology automatically blur or distort images or audio of bystanders (non-direct persons), or administrative fixes, such as notice-based data collection and deletion. Another possible approach is requiring XR companies to provide publicly available data subject request options. However, we note that the first listed option is preferable, since requests to delete still place too much onus on bystanders to locate XR companies and proactively seek out whether their information has been collected—at a high cost of time, information, and effort.

v. Enforcement and Remedies

Legislation would be incomplete without meaningful enforcement against violations of statutory requirements. Any effective XR regulatory scheme must indicate what body—either existing or created within the regulation—will be tasked with ensuring that requirements are met and violations penalized. Effective enforcement is necessary both to serve as a disincentive for businesses to ignore or improperly fulfill legal obligations and as a bulwark for individual privacy rights. Remedies for violations, such as monetary penalties, payment to individuals negatively affected, public notification, or other legal actions, must also be explicitly accounted for within the regulation.

vi. Private Right of Action

Enshrining private rights of action in proposed XR technology regulations could serve several privacy and safety purposes. For example, a private right of action could function as a means to more fully empower the individual to have more control over their personal data. If individuals are able to bring suit for improper collection or use of their information, sharing without permission, or other potential misuse, it gives those individuals more say over their information and may prompt more engagement from individuals with the collection and use of their personal information.

In addition, a private right of action serves as a way to spread enforcement obligations and counteract the limited resources of many enforcement bodies and agencies to pursue regulatory violations. Many agencies and enforcement bodies are unable to pursue every privacy violation due to time and resource restrictions and competing priorities.[175] A private right of action would serve as an additional incentive for companies using XR technology to strictly follow regulatory requirements. In the interest of avoiding potential lawsuits related to breaches, misuse, harms, or other causes, companies are more likely to adopt risk-mitigating practices, such as data minimization, anonymization, strong security measures, and more.

---

[175] *See* Joseph Jerome, *Private Right of Action Shouldn't Be a Yes/No Proposition in Federal Privacy Legislation,* INT'L ASS'N PRIV. PROFESSIONALS (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/.

Private rights of action are not necessarily common in privacy laws and, in fact, have more than once been the sticking point in a proposed privacy bill's passage.[176] Businesses tend to see private rights of action as more of a potential "gotcha" and states have been leery of the vigorous industry pushback that often accompanies private rights of action in privacy bills. Proponents of private rights of action contend that the private rights of action can be tailored in such a way that they achieve the desired goals listed above but are sufficiently limited (for example, there can be huge variances in the level of harm or potential harm thresholds required to bring suit, how individuals can establish standing, types of personal data the private right of action may apply to, or types of violations that may be applicable).[177]

Considering both the concerns of businesses and the benefits that a private right of action would provide to individuals and enforcement agencies, we feel that private rights of action are a meaningful addition to bills addressing privacy issues in XR technologies and should be considered and incorporated where possible. When compared with industry-based self-regulatory approaches, legislation is the more effective and consistent approach to ensuring privacy protections in XR technology, particularly in the private sector. But to ensure limits on law enforcement or government overreach, there should also be continued movement towards privacy protections in the judiciary.

2. Judicial

As we've already discussed, courts are currently using a mix of Fourth Amendment approaches to analyze both the law enforcement collection of data from third parties and law enforcement direct search and surveillance. It is possible that the courts will be able to create a path forward for either of these two areas by using the framework that the Supreme Court has created in *Carpenter*. However, there are several potential problems with this approach.

Judicial action is unlikely to apply to private sector risks in XR due to the lack of a private right of action in most privacy legislation. In

---

[176]*See* Aaron Nicodemus, *Private Right of Action Proving Problematic for State Privacy Laws,* COMPLIANCE WEEK (May 5, 2021), https://www.complianceweek.com/data-privacy/private-right-of-action-proving-problematic-for-state-privacy-laws/30343.article.

[177]*See supra* note 57; Cameron F. Kerry and John B. Morris Jr., *In Privacy Legislation, a Private Right of Action Is Not an All-Or-Nothing Proposition*, BROOKINGS (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/.

addition to lack of private sector coverage, there are three typical weaknesses of common law which would apply to the Judicial approach. First, the length of time required to establish enough case law and precedent to create common law is incompatible with the speed at which new technology—including new methods of infringing on privacy rights—develops. XR technology is already in use and collecting personal data at breakneck speeds. In the time it may take to establish common law that would address the use of XR technology, it may have expanded and advanced even further, becoming enmeshed with day-to-day life and making disentanglement more challenging. In this case and others, while individual cases may be able to address specific problems more quickly than other methods, broad privacy common law would be forever playing catch-up to new violations.

Second, the nature of common law is reactive rather than proactive. It would be developed after violations have already occurred rather than proactively prevent violations. By the time privacy violations have occurred, it is highly unlikely the harm from the privacy violation can be undone, especially when it comes to sensitive information (e.g., biometrics). In the case of XR technology, we would need clear and arguable examples of violations combined with willingness to pursue judicial redress in order to begin establishing the necessary case law. Finally, common law can be overridden at any time by new legislation. The time and effort required to establish a common law privacy protection could be instantly undermined by regulations and may not be considered stable.

While many look to the courts to provide clarity around existing protections, it is unlikely that courts can effectively develop protections through decision-making and, perhaps, inappropriate to look to the courts to set the tone on privacy protections in XR without guidance from legislators, technologists, and privacy specialists in the XR space.

3. XR Governance

There are several XR industry groups at this point in time, and there are bound to be many more as XR continues to take hold with the public.[178] At this point in time, there does not appear to be a framework

[178] Existing XR industry groups include the Extended Reality Association (XRA), a trade association; the XR Safety Initiative (XRSI), a non-profit focused on privacy, security, and ethics in XR across a broad set of industry sectors; the VR/AR Association, another trade association; and the EuroXR Association, a group focused on XR (AR/VR/MR) in Europe.

for XR development that is used across the industry. XRSI has recently put forth a XR Privacy Framework that maps controls to general categories of privacy in an effort to aid XR developers with privacy by design.[179] While this is a strong first step, without widespread adoption and conversation around the framework, it is unlikely that an industry standard for XR governance will appear. It is critical that the industry move towards published standards for XR to help protect XR technology *and* mitigate or prevent harms. We note, however, that industry standards are not a substitute for regulatory limitations and fall prey to several pitfalls in enforcement and stability.

CONCLUSION

Despite the proliferation of development in XR technology, the existing U.S. privacy framework addressing it remains weak, both in the private and public sectors. Throughout this paper, we have detailed possible scenarios of privacy harms. We recommended solutions that legislators can embrace to protect privacy as it currently exists and even enhance individual privacy rights and protections. XR technology is moving quickly and our legislators must work with technical specialists and privacy advocates to match the speed. Even as we write our assessments of the dangers of XR without strong regulations, we see that XR technology has moved from specialized gaming and industrial/corporate uses into technology that is available to the masses through existing social media giants. We urge legislators to address the gaps we have identified before XR technology further embeds itself into the fabric of our lives.

[179] THE XRSI PRIVACY AND SAFETY FRAMEWORK, XR SAFETY INITIATIVE (Kelly J. Cooper, ed., v 1.0, 2020) (We provided high-level review of the privacy framework during early-stage development. We are not affiliated with or employed by XRSI).

VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

ENTITY OF THE STATE: THE TRANSPARENCY OF RESTRICTING TELECOMMUNICATIONS FIRMS AS THREATS TO AMERICA'S NATIONAL SECURITY

Benjamin W. Cramer

ENTITY OF THE STATE: THE TRANSPARENCY OF RESTRICTING TELECOMMUNICATIONS FIRMS AS THREATS TO AMERICA'S NATIONAL SECURITY

Benjamin W. Cramer[*]

INTRODUCTION

Telecommunications networks are now considered to be crucial for national security, and there is growing awareness of how foreign adversaries could target such networks for their own gain. In recent years, the American government has subjected the telecom sector to increasing restrictions on exports and imports, usually justified by concerns over threats to national security when equipment is bought from, or sold to, suspicious foreign firms. As this article will argue, such governmental restrictions are typically the outcome of non-transparent agency decision-making procedures, with ramifications for citizen oversight of government operations and the health of the American telecommunications network.

The U.S. Department of Commerce maintains a document called the Entity List for foreign firms that American manufacturers are not permitted to export products and services *to*. This type of restriction has been common since the 1990s, but in more recent years the restrictions have been applied in the other direction as well. In 2019, President Donald Trump issued an executive order banning Americans from buying supplies from foreign telecommunications firms that have been deemed threats to national security. This added the Federal Communications Commission to the process, as that commission now maintains a document called the Covered List for foreign firms that Americans are not permitted to import *from*.

Journalists, government watchdogs, and even America's allies suspect that these export/import restrictions are politically motivated and based on poorly defined threats to national security, which is itself a poorly defined term. This turns relatively straightforward economic regulatory processes into a political drama that may lead to short-term rhetorical victories but long-term damage to the American telecom marketplace.

[*] Associate Teaching Professor, Donald P. Bellisario College of Communications, Pennsylvania State University.

The next section of this article describes the history of national security-oriented export restrictions in telecommunications, and the following section does the same for more recent import restrictions. Section three of the article deviates temporarily from legal and policy research into an analysis of the framing strategies used by politicians and the media to mold American public opinion of international economic competition, and how these viewpoints have found their way into trade policy. The fourth section analyzes the effects of opaque government agency processes, combined with poorly defined justifications, on the ability of interested citizens and companies to determine why the export/import restrictions were enacted. This is followed by an examination of how non-transparent restrictions may negatively affect the American telecom marketplace. The article concludes with a discussion of why more transparency is needed during this process, with recommendations for better methods of addressing suspicious foreign companies that do not require banning them from the American market and disrupting the development and operation of networks for consumers at home.

I. THE ENTITY LIST

Modern regulations giving the federal government oversight of exports sold by American manufacturers date back to the Export Administration Act of 1979,[1] which was passed during a period of military tension with several countries,[2] and new awareness that potential enemies might become stronger with equipment sold knowingly or unknowingly by American firms. Congressional debates at the time often used the phrase "U.S. security,"[3] which gradually became the more familiar "national security" by the new millennium. Export controls are typically enforced on items destined for countries that have been subjected to sanctions by the U.S. government, items in certain high-risk categories like nuclear power equipment, and items in some other technological categories that the government has deemed to be of

---

[1] 50 U.S.C. app. §§ 2401–20 (1979).

[2] During this period, international opinions of the United States were still recovering after the end of the Vietnam War in 1975, while the Soviet Union's aggression toward Afghanistan near the end of the decade exacerbated Cold War tensions. The United States had its own political conflict with Iran during this period, culminating in the Iran Hostage Crisis. *See* Kenneth W. Abbott, *Linking Trade to Political Goals: Foreign Policy Export Controls in the 1970s and 1980s*, 65 MINN. L. REV. 739, 756-763, 798-822 (1981).

[3] *See, e.g.*, S. REP. NO. 96-169 (1979) (concerning the Export Administration Act of that year).

strategic value.[4] In recent years, telecommunications equipment has been increasingly subjected to several types of export restrictions due to growing concerns about the industry's possible impacts on national security.[5]

The Export Administration Act instituted controls for both direct exports, in which an American company sells to a customer in a foreign nation, and "re-exports" in which that first foreign customer sells the item again to someone in a third country. Regulated product categories require an export license; American firms that mistakenly export controlled items without a license, or firms that violate an existing license, are typically charged a fine.[6] For most products, the Bureau of Industry and Security, a division of the Department of Commerce, exercises jurisdiction over exports and can require American firms to apply for licenses or outlaw certain exports altogether.[7] Current regulations require Commerce to consult with other government agencies per their areas of expertise.[8] For some items, licensing requirements and approvals from multiple agencies may be necessary.[9] As will be discussed herein, this results in many decisions by many agencies with their own procedures and definitions, which can lead to a shortage of transparency for interested citizens or companies trying to navigate through agency documents that readily announce final decisions but contain few useful references to prior decision-making processes.

The Export Administration Act eventually expired and was replaced by other statutes, and current export regulations are codified in Section 15 of the Code of Federal Regulations. That section mandates, and contains, the Entity List, which includes parties that American firms are not allowed to export *to*.[10] The Entity List was first published by the Department of Commerce in 1997 and has been regularly updated ever since.[11] While it was originally focused on preventing American products from winding up in the hands of enemies making weapons of mass

---

[4] *See* Michael T. Stewart, *U.S. Export Regulations: An Overview*, 241 N.J. LAW. 37, 37 (2006).
[5] 15 C.F.R. § 744.11(a)(2) (2022).
[6] *See* Stewart, *supra* note 4, at 37-38.
[7] *Id.* at 37.
[8] 15 C.F.R. § 730.4 (2022).
[9] *See* Stewart, *supra* note 4, at 39.
[10] 15 C.F.R. § 744.16 (2022). Note that export regulations are spread throughout various chapters of the Code of Federal Regulations, and are known collectively as Export Administration Regulations (EAR).
[11] Jeffery S. Allen, *Do Targeted Trade Sanctions Against Chinese Technology Companies Affect US Firms? Evidence from an Event Study*, 23 BUS. & POL. 330, 330-31 (2021).

destruction, it has since been expanded to encompass general foreign policy and national security interests that may be impacted by the export of American products.[12] Any American company wishing to do business with a foreign party that is on the Entity List must apply for a specific license from Commerce, and the Bureau of Industry and Security could reject the application.[13]

The Entity List identifies parties "reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States."[14] The regulations have no further definition of the phrase *reasonably believed*, nor by whom except entire Executive Branch agencies. Meanwhile, the phrase *national security* appears regularly throughout the regulations but with no definition beyond "activities that are contrary to the national security or foreign policy interests of the United States" and similar phrasing.[15] This oft-used but poorly defined term has resulted in many dubious and unaccountable export restrictions—and later, import restrictions—as will be discussed throughout this article.

As of 2023, companies headquartered in China or Russia are by far the most numerous on the Entity List, each with more than 300 listings.[16] A cursory review of those companies reveals many with some variation of "telecommunications" in their names. The lopsided representation from those two countries is largely due to longstanding suspicions of Chinese threats to American security interests, which have been festering for many years and were exacerbated during the Trump Administration. Meanwhile, American attitudes toward Vladimir Putin's regime in Russia have evolved from cooperative to frosty with Putin's gradually increasing militarism.[17] While the United States views several other nations and their companies as potential security risks, three particular telecommunications-oriented firms from China and Russia generated significant news coverage when they were banned from receiving exports from the United States.

---

[12] *See* Department of Commerce, Bureau of Industry and Security, *Entity List FAQs*, https://www.bis.doc.gov/index.php/cbc-faqs/faq/28#faq_282 (last visited Nov. 21, 2022).
[13] 15 C.F.R. § 744.16(a) (2022).
[14] 15 C.F.R. § 744.16 (2022).
[15] 15 C.F.R. § 744.11(b) (2022).
[16] 15 C.F.R. pt. 744 (Supp. 4 2022).
[17] *See* James Dobbins, Howard J. Shatz & Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue*, RAND CORP. (Oct. 2018), at 2-8, https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE310/RAND_PE310.pdf.

Huawei Technologies Ltd. of Shenzhen, China is the world's largest manufacturer of general telecommunications networking equipment and one of the largest producers of smartphones.[18] Huawei first attracted the attention of American lawmakers in 2012 due to suspicions of copying American intellectual property. By 2018, additional concerns arose about the company's close relationship with the Chinese government, which could lead to malicious surveillance of American consumers and government officials.[19] The U.S. Department of Justice also investigated Huawei during this period for reselling American networking equipment to Iran, thus violating U.S. sanctions on that country.[20] However, with the exception of a plea deal to resolve individual charges against Huawei executive Meng Wanzhou in 2019,[21] all of the investigations are still in progress at the time of this writing and the company has not yet been formally convicted of any violation of U.S. law. Regardless, the Department of Commerce placed the company on the Entity List in 2019.[22] The associated regulatory document cites those previous investigations to conclude that "there is reasonable cause to believe that Huawei . . . has been involved in activities determined to be contrary to the national security or foreign policy interests of the United States."[23] The most recent regulatory document on the matter describes the company as a "continuing threat to U.S. national security and U.S. foreign policy interests."[24] Note the nearly identical terminology.

Zhongxing Telecommunications Equipment Corp., commonly known as ZTE, is another telecommunications firm based in Shenzhen, China, that is best known for its inexpensive smartphones targeted at

---

[18] *See* Frank Chen, *Inside Huawei's Huge HQ Campus in Shenzhen*, ASIA TIMES (June 28, 2019), https://asiatimes.com/2019/06/inside-huaweis-huge-hq-campus-in-shenzhen/.

[19] *See* Grace Sullivan, *The Kaspersky, ZTE, and Huawei Sagas: Why the United States Is in Desperate Need of a Standardized Method for Banning Foreign Federal Contractors*, 49 PUB. CONT. L. J. 323, 334 (2020).

[20] *See* Steve Stecklow, *Newly Obtained Documents Show Huawei Role in Shipping Prohibited U.S. Gear to Iran*, REUTERS (Mar. 2, 2020, 9:11 AM), https://www.reuters.com/article/us-huawei-iran-sanctions-exclusive-idCAKBN20P1VA.

[21] *See* Eric Tucker & Jim Mustian, *Huawei Exec Resolves Criminal Charges in Deal with US*, ABC NEWS (Sept. 24, 2021, 2:24 PM), https://abcnews.go.com/Technology/wireStory/justice-dept-huawei-exec-poised-resolve-criminal-charges-80212658.

[22] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022).

[23] *Id.*

[24] *See* Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51,596 (Aug. 20, 2020) (to be codified at 15 C.F.R. pts 734, 744, 762).

consumers in developing countries, but is also an active player in 4G and 5G networking equipment.[25] ZTE has long been suspected of infringing on the patents of American telecommunications products, but the company first gained the notice of the export restriction regime in the mid-2010s when it re-exported American products to Iran and North Korea.[26] ZTE was added to the Entity List in 2016 with the usual obligatory reasoning: "for actions contrary to the national security and foreign policy interests of the United States".[27]

Kaspersky Lab is a cybersecurity firm headquartered in Moscow, Russia, which for a time had contracts with about 15% of U.S. government offices for antivirus software and other security services.[28] Starting in 2016, U.S. officials began to suspect that the company was closely tied to the regime of Vladimir Putin, mostly due to his longtime association with CEO Eugene Kaspersky, which in turn fed suspicions that Russia could use the company's software to spy on the U.S. government. In 2017, despite a lack of concrete evidence, the Department of Homeland Security ordered all government agencies to remove their Kaspersky software.[29] To date, Kaspersky Lab is not yet on the Department of Commerce's more expansive Entity List, though its products have been subjected to specific restrictions from the Federal Communications Commission.[30]

The most recent high-profile international firm to be added to the Entity List, this time by the Biden administration, is NSO Group of Israel,[31] which journalists exposed in 2021 for selling its smartphone surveillance technology to governments around the world, including

---

[25] *See* Rachel Layne, *3 Things to Know About ZTE and Huawei*, CBS NEWS (June 7, 2018, 3:49 PM), https://www.cbsnews.com/news/3-things-to-know-about-zte-and-huawei/.
[26] *See* Sullivan, *supra* note 19, at 331.
[27] *See* Additions to the Entity List, 81 Fed. Reg. 12,004 (Mar. 8, 2016) (to be codified at 15 C.F.R. pt. 744).
[28] *See* Dustin Volz, *About 15 Percent of U.S. Agencies Found Kaspersky Lab Software: Official*, REUTERS (Nov. 14, 2017, 11:25 AM), https://www.reuters.com/article/us-usa-cyber-kaspersky-congress-idUKKBN1DE28P.
[29] *See* Sullivan, *supra* note 19, at 337–38.
[30] *See* Dan Goodin, *FCC Puts Kaspersky on Security Threat List, Says It Poses 'Unacceptable Risk'*, ARSTECHNICA (Mar. 25, 2022, 8:38 PM), https://arstechnica.com/information-technology/2022/03/fcc-puts-kaspersky-on-security-threat-list-says-it-poses-unacceptable-risk/.
[31] *See Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities,* U.S DEP'T OF COM. (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

several dictatorships.[32] Following the largely enemy-based use of the Entity List by the Trump administration, the restriction of NSO Group by the Biden Administration was the first prominent use of this export control technique against a company residing in a staunch-allied nation after the Trump era.[33]

For any company on the Entity List, placement is decided by an "End-User Review Committee" chaired by a representative from the Department of Commerce and including representatives from the Departments of State, Energy, Defense, and (when relevant) Treasury.[34] The regulations contain few details on how this committee should reach its decision to add a company to the Entity List, except that decisions must be unanimous and that the resulting documents must properly cite that same category of regulations.[35] There is no requirement to cite decision-making documents by the Department of Commerce or other agencies that may have investigated the foreign firm. A listed company can request removal from the End-User Review Committee,[36] but the delisting process is described with the same lack of detail as the listing process.[37]

The ultimate result is a regulatory document from the Department of Commerce stating that the End-User Review Committee decided that a foreign firm was a threat to national security due to suspicious activities, or preliminary investigations of such by other agencies, that may or may not have come to fruition, and typically without citations to investigative or decision-making documents. For example, in 2018, a company from the British Virgin Islands called Evans Meridians Ltd. was added to the Entity List. The regulatory document stated that the committee had decided that the firm tried to re-export American equipment to Iran in violation of U.S. sanctions, but provided no citations to any documents that informed this decision.[38] As another example, in 2021, a company called Gensis Engineering from Turkey was

---

[32] *See* Drew Harwell et al., *Biden Administration Blacklists NSO Group over Pegasus Spyware*, WASH. POST (Nov. 3, 2021, 2:30 PM), https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/.

[33] *See* David E. Sanger et al., *U.S. Blacklists Israeli Firm NSO Group over Spyware*, N.Y. TIMES (Nov. 3, 2021), https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

[34] 15 C.F.R. § 744.16(d) (2022).

[35] 15 C.F.R. pt. 744 (Supp. 5 2020).

[36] 15 C.F.R. § 744.16(e) (2022).

[37] 15 C.F.R. pt. 744 (Supp. 5 2020).

[38] *See* Addition of Certain Entities to the Entity List, Revision of Entries on the Entity List and Removal of Certain Entities from the Entity List, 83 Fed. Reg. 44821, 44822 (Sept. 4, 2018); 15 C.F.R. pt. 744 (Supp. 4 2022).

added to the Entity List, with the regulatory document lumping that company in with more than a dozen others under suspicion for trafficking American equipment to Iran. That document states only that the committee "determined" that the company was involved in "activities that are contrary to the national security and/or foreign policy interests of the United States"—the exact same phrase that appears in the governing regulations—and once again with no citations to actual investigative documents.[39]

Furthermore, the Entity List includes a column titled *License review policy* which contains the phrase "presumption of denial" for most of the companies listed.[40] This means that if any American company wants to apply for a license to export goods to such a foreign company, the Department of Commerce has already declared that the license will likely be denied. How this decision was made, and what types of extenuating circumstances could possibly override it, are usually absent from the regulatory documents. For example, in 2020, a company called Multi Technology Integration Group from Bulgaria was added to the Entity List with a "presumption of denial" for any future export licensing requests. The regulatory document states that this company is a suspected front for operators who smuggle American products into Russia.[41] Like in the examples above, no citations are given to any outside documents in which this determination was made. Moreover, no cited evidence is given to support the "presumption of denial," but in fairness, the presumption for the Bulgarian firm is limited to specific technological categories of "sensitive electronic components" of interest to Russia.[42]

With thousands of relevant documents, finding comprehensive or qualitatively significant patterns of citations is beyond the scope of the present article, but the author has determined that these examples, plus others described herein, are indicative of the transparency of Entity List decisions by the End-User Review Committee at the Department of Commerce, or the lack thereof.

The export-only restrictions described in this section, which, in short, tell an American company who it cannot export its products *to*, have been standard practice since the late 1970s. In the 2010s, political

---

[39] *See* Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List, 86 Fed. Reg. 71557 (Dec. 17, 2021); 15 C.F.R. pt. 744 (Supp. 4 2022).
[40] *See* 15 C.F.R. pt. 744 (Supp. 4 2022).
[41] *See* Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 18, 2020); 15 C.F.R. pt. 744 (Supp. 4 2022).
[42] Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. at 83417.

motivations and non-transparent suspicions of threats to national security expanded this regime to imports as well. Now American companies have additional rules for importing raw materials or components *from* certain targeted entities.

II. TOWARDS THE COVERED LIST

In the 2010s, it became increasingly common for the U.S. government not just to restrict exports to foreign business partners, but to enact controls in the other direction as well. Federal government agencies are now often restricted from contracting with foreign firms that reside in nations that America has deemed hostile to national security, especially China and Russia, for purposes of *importing* products and services. For example, in addition to the aforementioned export restrictions, in 2017 and 2018, U.S. government agencies were banned from entering into contracts with Kaspersky, Huawei, and ZTE.[43] All three have also had their products banned by the Federal Communications Commission (FCC) from any network development efforts that receive agency funds.[44]

Until 2019, these import restrictions were usually accomplished via annual defense budget authorization bills, which in turn often featured a specific focus on telecommunications equipment.[45] Starting in 2019, President Donald Trump adopted a strategy of restricting imports via executive orders and executive branch regulations, and this kicked off several new legislative efforts to address procedural gaps. Telecommunications equipment received particular attention during these developments. Such import restrictions have become increasingly popular, reflecting current political tensions and typically citing threats to national security, but they tend to be written with vague and expansive language that makes their effectiveness difficult to assess.[46]

On May 15, 2019, President Trump issued Executive Order No. 13873, which barred American telecom service providers from importing equipment from any foreign company that has been deemed a national

---

[43] *See* Sullivan, *supra* note 19, at 325.
[44] *See* Goodin, *supra* note 30. The FCC restrictions will be discussed at *infra* notes 168-173 and accompanying text. Note: While export/import controls are under the jurisdiction of the Department of Commerce, the FCC has authority over publicly-funded telecom development projects within the United States.
[45] *See, e.g.*, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917-18 (2018). This statute specifically targeted ZTE and Huawei in § 889(f)(3).
[46] *See* Sullivan, *supra* note 19, at 324.

security risk.[47] Carrying the telecom-specific title, *Securing the Information and Communications Technology and Services Supply Chain*, the executive order uses very broad language, encompassing:

> services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries [that] augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.[48]

The executive order's language is particularly expansive and vague, beyond obvious hyperbole like "catastrophic" and "extraordinary." Elsewhere in the order, authority over the matters discussed is given to the Secretary of Commerce, but in conjunction with a bewildering plethora of other officials including the Secretaries of Treasury, State, Homeland Security, and Defense; plus the Attorney General, the U.S. Trade Representative, the Director of National Intelligence, the Chair of the Federal Communications Commission, and additional officials with expertise as needed.[49] In a reflection of current technological trends and political controversies, "information and communications technology or services" are mentioned specifically as crucial factors for "critical infrastructure" and the "digital economy."[50] The Department of Homeland Security received a specific command to continuously watch for hardware and software that could compromise such networks,[51] with a citation to an earlier executive order by President Barack Obama, which addressed the cybersecurity of critical infrastructure.[52] "Critical infrastructure" entered governmental parlance after the terrorist attacks on September 11, 2001; the term has been used in many statutes for systems in which disruption by enemies could cause

---

[47] *See* Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019) (codified at 3 C.F.R. 13873).
[48] *Id.* The word "persons" in this excerpt reflects the traditional use of that word in export/import regulations, in which it serves as a catch-all term for individuals, companies, and organizations.
[49] *Id.* at 22689-90.
[50] *Id.* at 22690.
[51] *Id.* at 22691.
[52] *See* Exec. Order No. 13636, 3 C.F.R. 13636 (2014).

major hardships for the United States. "Critical infrastructure" tends to be vaguely defined in the law, and is often mixed up with the equally vague term "national security."[53]

While the executive order focuses on American persons or companies that do business directly with telecom firms that have been deemed hostile in themselves or are housed in hostile nations, its language (particularly pertaining to re-exports) is expansive enough to encompass economic transactions that take place outside of the United States as well.[54] The order also uses very broad language for its targeted products:

> [A]ny hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display.[55]

This broad categorization can sweep up practically all computerized telecommunications networking components that can process data, and the services that keep those components connected.[56]

The executive order invoked the International Emergency Economic Powers Act[57] and the National Emergencies Act.[58] Those two statutes allow such declarations from the President in the event of "unusual and extraordinary threats," with the former statute adding particular procedures for export/import transactions with hostile adversaries. These two statutes allow the President to unilaterally declare an emergency, and Congress only needs to be informed after the declaration has been made.[59] The term "emergency" can be used at will

---

[53] *See* Benjamin W. Cramer, *Envirodemic: Unconstitutional Restrictions on Environmental Protests from the Attacks of 2001 to the Struggles of 2020*, 14 L.J. SOC. JUST. 79, 81 (2021).
[54] *See* Caroline Elyse Burks, *The Case for Presumptions of Evil: How the E.O. 13873 'Trump' Card Could Secure American Networks from Third-Party Code Threats*, 11 AM. U. NAT'L. SEC. L. BRIEF 95, 99-100 (2021).
[55] 84 Fed. Reg. 22,689, 22,691.
[56] *See* Burks, *supra* note 54, at 100. Illustrating the executive order's expansive language, the Department of Commerce later published a list of industry sectors that can be included in the regulations, consisting of twelve types of telecom service providers, seven types of Internet service providers, and six types of equipment manufacturers. *See Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 65316, 65318-19 (Nov. 27, 2019).
[57] 50 U.S.C. § 1701 *et seq*. (1977).
[58] 50 U.S.C. § 1601 *et seq*. (1976).
[59] 50 U.S.C. § 1621 (1976); 50 U.S.C. § 1701 (1977).

too, and Trump's justification for the apparent emergency in 2019 is tough to decipher.[60] Trump opined that some telecommunications-related imports and exports constituted a "national emergency" because:

> additional steps are required to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. In light of these findings, I hereby declare a national emergency with respect to this threat.[61]

The executive order did not list any specific foreign companies or what made them national security risks, and it also did not mention the Entity List in particular. However, it did instruct the Department of Commerce to draft enforcement rules[62] and to determine which companies and countries constitute national security threats.[63] Commerce, in consultation with various other knowledgeable agencies, was instructed to investigate any:

> undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States.[64]

Since Trump's executive order concerned both imports and exports, later that week Commerce added Huawei to the export-specific Entity List, as described above.[65] The timing was not a coincidence, as the department endeavored to fulfill Trump's goals. Secretary of Commerce Wilbur Ross made a public statement about his department's efforts to help the President tackle national security threats, but as is

---

[60] *See* David W. Opderbeck, *Huawei, Internet Governance, and IEEPA Reform*, 47 OHIO N.U. L. REV. 165, 173-74 (2021). *See also* 50 U.S.C. § 1701 (1977); 50 U.S.C. § 1702(a) (2001).
[61] Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019) (codified at 3 C.F.R. 13873).
[62] *See* Kendra Chamberlain, *Trump to Ban U.S. Carriers from Using Network Gear Posing Security Risk*, FIERCE WIRELESS (May 15, 2019, 10:33 AM), https://www.fiercewireless.com/tech/trump-to-direct-us-carriers-to-ban-network-gear-pose-security-risk-reuters.
[63] 84 Fed. Reg. 22,689, 22,689-22,690.
[64] *Id.* at 22,690.
[65] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022).

common in his agency's Entity List documentation, Ross avoided details on the nature of those threats.[66]

The day before Trump left office, the Department of Commerce issued a rule to extend the 2019 executive order into the incoming Biden Administration, and for the Department's new leaders to continue collecting public comments on how to protect national security interests from threats posed by adversarial foreign telecom firms.[67]

Meanwhile, since the Entity List is focused on exports, new legislation was needed to tackle the aspects of Trump's executive order that concerned imports from the same suspicious foreign companies. The first legislative action concerned the use of federal money to buy equipment *from* suspicious foreign companies, and the apparent importance of telecommunications networks during such processes received specific attention from Congress. The Secure and Trusted Communications Networks Act, passed in March 2020, prohibits the use of telecom subsidies (which are managed by the Federal Communications Commission) to purchase networking equipment that presents a national security risk.[68] The statute did not define "national security" or the types of risks it faces from unsecure telecommunications equipment. The FCC was instructed to figure this out in consultation with yet another bewildering plethora of agencies: the Department of Homeland Security, the Department of Defense, the Director of National Intelligence, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI).[69] Neither the NSA nor the FBI had been suggested for their expertise on this topic in President Trump's executive order the previous year.

The Secure and Trusted Communications Networks Act mandated the creation of another list of suspicious foreign telecom-oriented companies, this time called the Covered List, to enable import controls and to be managed by the FCC, in a fashion similar to Commerce's ongoing management of the multi-industry and export-specific Entity List.[70] The FCC also found itself with new authority to decide that

---

[66] *See* Kendra Chamberlain, *Commerce Dept. Bans Huawei, 70 Affiliates from Sourcing U.S. Components*, FIERCE WIRELESS (May 16, 2019) [hereinafter Commerce Dept. Bans Huawei], https://www.fiercewireless.com/5g/commerce-dept-adds-huawei-and-70-affiliates-to-telecom-ban-list.

[67] *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021).

[68] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 3(a), 134 Stat. 158, (2020).

[69] *Id.* at § 9(2).

[70] *See* Federal Communications Commission, Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization

something is a threat to national security.[71] Huawei and ZTE were among the first companies to be placed on the Covered List, with the commission's Public Safety and Homeland Security Bureau determining, per its new authority under the Secure and Trusted Communications Networks Act, that those companies were indeed threats to national security.[72] Given recent political controversies, that may have been a straightforward decision, regardless of the lack of a comprehensive definition of "national security". But, things were not so easy when it came to less newsworthy firms. More than a year after the Secure and Trusted Communications Networks Act was passed, the FCC issued a call for public comments as it attempted to put together the Covered List and procedures for maintaining it into the future.[73] Kaspersky Lab, which, as discussed above, is not yet on the Department of Commerce's export-only Entity List,[74] was added to the FCC's import-oriented Covered List in March 2022.[75]

The 2019 Secure and Trusted Communications Networks Act had a flaw in that it only applied to the use of federal subsidies for the purchase of items to be imported from suspicious foreign firms.[76] Another statute applying to purchases by private American companies, known as the Secure Equipment Act, was passed in October 2021 to close this loophole.[77] This statute also prohibited the FCC from allowing case-by-case exceptions (e.g., emergency network repairs in remote areas) to the restrictions mandated by a foreign firm's placement on the Entity List or Covered List, which it had been able to do thanks to another loophole in the 2019 statute.[78] Now, American firms were prohibited from both

---

Program, ET Docket No. 21-232/21-233, FCC 21-73 (June 17, 2021) at ¶ 13. The statute originally called the proposed list the "Covered Communications Equipment or Services List".

[71] *Id.* at ¶ 15.

[72] *See* Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program and the Competitive Bidding Program, 86 Fed. Reg. 46645-46 (Aug. 19, 2021) (to be codified at 47 C.F.R. pt. 2).

[73] *Id.* at 46653.

[74] *See Id.*

[75] *See* Federal Communications Commission, Public Notice on Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act (Mar. 25, 2022), https://www.fcc.gov/document/announcement-additions-covered-list.

[76] H.R. REP. NO. 117-148, at 2 (2021).

[77] Secure Equipment Act of 2021, 47 U.S.C. § 1601, Pub. L. 117-55, 135 Stat. 423-424 (2021).

[78] *See* Ron Amadeo, *The US Closes Huawei Loophole, Will No Longer Grant Exceptions for ISPs*, ARSTECHNICA (Nov. 12, 2021, 2:02 PM), https://arstechnica.com/gadgets/2021/11/the-us-will-no-longer-approve-exceptions-for-huawei-networking-gear/.

exporting *to* such foreign firms, via the older Entity List, and importing *from* them, due to the new statutes of 2020 and 2021.

III. POLITICAL AND NEWS FRAMING OF NATIONAL SECURITY THREATS

These new restrictions on both the import and export of telecommunications equipment from apparently untrustworthy foreign firms can be traced to several concurrent trends that gained traction in the 2010s. First was the obviously growing importance of interconnected global telecom networks and the equipment needed to sustain them. Second was the increasing use of the term "national security" in U.S. law with a definition that is incongruously tough to nail down. Third is a longstanding trend in the framing of America's geopolitical conflicts, particularly with China, which underwent a transformation during the Trump administration and exacerbated political arguments that in turn found their way into trade policy. These trends have continued under the Biden Administration, perhaps due to political inertia.

President Donald Trump's framing of collective threats, be they economic or otherwise, was rooted in right-wing populism, which promises to alleviate a nation's insecurities by naming enemies and drawing public support by vowing to counter those enemies.[79] Amplifying the threats themselves, and then amplifying how those threats contradict the values of the politician's supporters, is a fundamental aspect of this framing strategy.[80] Trump intensified this strategy with China in particular, linking America's longtime anti-Communist ideals with frequent references to "the Chinese Communist Party" and claims that the country was committed to an ideological struggle with the West.[81] Meanwhile, Trump's frequent use of the term "trade war," for what was in fact a complex economic and geopolitical entanglement, may have been intended to emphasize the simplistic term *war* as either the nature of the Chinese threat, or the nature of America's need to respond to that threat.[82]

In the realm of political discussion and understanding, framing is a well-researched phenomenon. In its most basic definition, the fashion in which an issue is "framed" has an impact on someone's opinions

---

[79] *See* Daniel Béland, *Right-Wing Populism and the Politics of Insecurity: How President Trump Frames Migrants as Collective Threats*, 18 POL. STUD. REV. 162, 164–65 (2020).
[80] *Id.* at 167.
[81] *See* Jacques deLisle, *When Rivalry Goes Viral: COVID-19, U.S.-China Relations, and East Asia*, 65 ORBIS 46, 50–51 (2021).
[82] *Id.* at 58.

toward and understanding of that issue.[83] Or in other words, the ordinary person uses mental shortcuts (frames) to comprehend a complex issue, but those mental shortcuts can be influenced by the source of the information. That source is likely to be a media outlet that the person consumes, a politician that the person admires, or the political party that the person supports.[84]

For politicians and policymakers, the framing process includes decisions on whether they should speak publicly about their substantive policy positions or emphasize the "horse race" competition with their political rivals. A similar choice must be made between emphasizing specific issues (like climate change or export/import policy) or generic values (like democracy or national security).[85] In particular, Donald Trump positioned geopolitical disagreements within his "America First" and "Make America Great Again" frames, in which other parties, be they political opponents or hostile nations, were depicted as threats to his supporters' values,[86] with "national security" frequently added to any such discussions that involved foreign affairs.[87] In the case of China, Trump's political framing of that nation as a threat to American values and safety intensified during the COVID-19 pandemic, with this adversarial stance finding its way into trade policy.[88]

Meanwhile, news framing is the process in which media professionals pick and choose portions of a complex topic for emphasis when explaining that topic to the audience, based on either explicit or implicit editorial guidelines that are themselves influenced by economic, cultural, and political perceptions among the news staff.[89] In other words, the news both influences and is influenced by the audience and

---

[83] *See* Fernando R. Laguarda, *Think of an Elephant? Tweeting as 'Framing' Executive Power*, 8 LEG. & POL'Y. BRIEF 32, 42-43 (2019).
[84] *Id.*
[85] *See* Britta C. Brugman & Christian Burgers, *Political Framing Across Disciplines: Evidence from 21st-Century Experiments*, 2018 RSCH. AND POL. 1, 1-2 (2018).
[86] *See* Darrius Hills, *Back to a White Future: White Religious Loss, Donald Trump, and the Problem of Belonging*, 16 BLACK THEOLOGY 38, 39, 46 (2018).
[87] *See* K. Jill Fleuriet & Mari Castellano, *Media, Place-Making, and Concept-Metaphors: The US-Mexico Border During the Rise of Donald Trump*, 42 MEDIA, CULTURE & SOC'Y 880, 890-91 (2020).
[88] *See* Angie Y. Chung et al., *COVID-19 and the Political Framing of China, Nationalism, and Borders in the U.S. and South Korean News Media*, 64 SOCIO. PERSP. 747, 752-53, 758 (2021). This trend arose from the widespread belief that China was responsible for the worldwide COVID-19 pandemic, regardless of whether it was purposeful or accidental.
[89] *See* Claes H. de Vreese, *News Framing: Theory and Typology*, 13 INFO. DESIGN J. 51, 55 (2005).

the country in which journalists reside, while political leaders also influence such editorial decision-making.[90]

There has been extensive professional research on how the American news media frames its home country's geopolitical conflicts with China. Attitudes toward that country are obviously relevant to the export/import trade policies discussed in this article because Chinese companies have received disproportionate attention during the supposed trade war. Researchers have detected a framing strategy among American news outlets that typically explains US-China relations as a zero-sum competition based on mistrust.[91] Such news coverage patterns in the American media, in which economic competition is framed as a conflict between enemy nations, is descended from coverage of true wars of military engagement in the 20th century, as opposed to peacetime coverage of mundane regulations and policymaking.[92] Such coverage frequently frames the disagreeing nations as "enemies" rather than "opponents," or as "adversaries" rather than "partners," [93] while the *war* in "trade war" is frequently emphasized.[94] Editorial viewpoints on purported conflicts in the race to develop new technologies have also been shown to influence news coverage, and therefore public opinion, of U.S.-China relations and the fortunes of the relevant high-tech companies.[95]

Specifically for U.S.-China relations, other researchers have found that this type of framing strategy in the American media can be traced to ancient perceptions among Westerners of themselves as civilized and rational while the Orient (the common term at the time) was perceived as backward and irrational, often to the point of imagining a good vs. evil dichotomy.[96] That dichotomy has its roots in the "Yellow Peril" of the 19th century, in which Asia was seen as a cultural threat to Western cultural values, followed by the "Red Peril" of the mid-20th century in

---

[90] *See* Dennis Nguyen & Erik Hekman, *A 'New Arms Race'? Framing China and the U.S.A. in A.I. News Reporting: A Comparative Analysis of the Washington Post and South China Morning Post*, 7 GLOB. MEDIA & CHINA 58, 60-61 (2022).
[91] *See* Peter Gries & Yiming Jing, *Are the US and China Fated to Fight? How Narratives of 'Power Transition' Shape Great Power War or Peace*, 32 CAMBRIDGE REV. INT'L. AFFAIRS 456, 460, 474 (2019).
[92] *See* Louisa Ha, Yang Yang, Rik Ray, Frankline Matanji, Peiqin Chen, Ke Guo, & Nan Lyu, *How US and Chinese Media Cover the US–China Trade Conflict: A Case Study of War and Peace Journalism Practice and the Foreign Policy Equilibrium Hypothesis*, 14 NEGOT. & CONFLICT MGMT. RSCH. 131, 133—34 (2021).
[93] *Id.* at 136.
[94] *Id.* at 145.
[95] *See* Nguyen & Hekman, *supra* note 90, at 63.
[96] Su-Mei Ooi & Gwen D'Arcangelis, *Framing China: Discourses of Othering in US News and Political Rhetoric*, 2 GLOB. MEDIA & CHINA 269, 270 (2017).

which Asia (and especially China) was seen as a vanguard of a worldwide Communist revolution.[97]

Longstanding American viewpoints on China have manifested themselves in geopolitical policy, from America's involvement in the Opium Wars of the mid-19th century to modern territorial tensions in the South China Sea.[98] The present article contends that this pattern can be seen in recent telecom-oriented export/import restrictions as well. The policymakers who enact those regulations are not immune to the effects of these framing patterns.[99]

IV. VAGUENESS AND POOR TRANSPARENCY IN EXPORT/IMPORT POLICY

When the American government first expressed concern about the possible threats posed by Chinese telecom firms, suspicions about the theft of American intellectual property and trade secrets were the first issue of investigation.[100] In fact, Huawei and ZTE have each been sued by American firms for patent infringement numerous times.[101] Chinese patent theft is estimated to cost American companies up to $600 billion every year.[102] In the years after those suspicions emerged, government investigations into the specific and esoteric matter of patent theft have morphed into less distinct and more dramatic political grandstanding about "national security." Granted, some commentators have noted that rampant intellectual property theft can have implications for national security, particularly regarding defense systems.[103]

But, beyond mundane patent disputes, "national security" is used in much looser ways for political impact. President Donald Trump's national security policy, and its associated regulatory documents, almost always mentioned China in particular, and typically framed the policy as a response to Chinese economic skullduggery, with the complex connection between economic competition and threats to national security taken as a given.[104] In fairness, this framing practice was merely an accelerated version of a strategy that had originated in the Obama

---

[97] *See id*. at 273.
[98] *See id*. at 271.
[99] *See* Gries & Jing, *supra* note 91, at 461.
[100] *See* Sullivan, *supra* note 19, at 330.
[101] *See id*. at 347.
[102] Sherisse Pham, *How Much Has the US Lost from China's IP Theft?*, CNN (Mar. 23, 2018, 5:35 AM), https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html.
[103] *See* Vilas Ramachandran, *A Regulatory Back Door: General Prohibition Ten and America's National Security*, 20 SANTA CLARA J. INT'L. L. 31, 34—35 (2022).
[104] *See* deLisle, *supra* note 81, at 66—67.

administration, during a period in which awareness of Chinese theft of American intellectual property (an economic misdeed) was growing.[105] Converting that esoteric concern into Trump's more exciting national security focus was a fairly easy rhetorical shift, especially because national security is both suitably emotional and wretchedly defined in American law.

The statutory meaning of "national security," despite the term's preponderance in export/import policy and many other areas of American law, is difficult to nail down. After World War II, "national security" expanded beyond fairly comprehensible military objectives into an amorphous conglomeration of law enforcement, terrorism, corruption, environmental protection, public health, economic strategy, and (most recently) export/import policy.[106] Efforts to refine the term to comprehensible dimensions has become a struggle of party politics, in which adversarial groups cite national security to advance their own causes.[107] The use, or overuse, of national security as a justification for any and all political projects exploded after the terrorist attacks of September 11, 2001, to the point of making the term nearly useless as a measure of political achievement, for either economics or security.[108]

The first appearance of the term "national security" in trade policy was in a 1975 executive order that established the Committee on Foreign Investment in the United States (CFIUS), which reviews the impact of foreign investments in American companies, though that order included no definition of the term.[109] The CFIUS currently operates under a statute stating that "[t]he term 'national security' shall be construed so as to include those issues relating to 'homeland security,' including its application to critical infrastructure," which in turn includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[110] This is the most distinct definition of the term to be found in the export/import regulatory regime, but whether all this terminology nails down the CFIUS's viewpoint on national security may be a moot point. The committee has often been

---

[105] *Id.* at 67.
[106] *See* J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1034 (2020).
[107] *Id.* at 1034–35.
[108] *See id.* at 1047–50.
[109] *See* Exec. Order No. 11,858, 3 C.F.R. § 990 (1971–1975).
[110] This text is from a 1988 addendum, known as the Exon-Florio Amendment to the Defense Production Act. 50 U.S.C. §§ 4565(a)(1), (5). Various post-1975 provisions of that Act codify the CFIUS process of reviewing foreign investments.

accused of making its decisions via an unaccountable process that is incomprehensible and unreviewable for interested citizens.[111]

The phrase "national security" is used numerous times in the Export Administration Act of 1979, the statute from which modern restrictions flow.[112] That statute was renewed by several presidents, both Republican and Democrat, who cited its utility for ensuring national security.[113] Congress most recently used that justification in the Export Control Reform Act of 2018,[114] which was a precursor of the telecom-specific controls at the heart of the present article. That statute addresses "emerging and foundational technologies that . . . are essential to the national security of the United States," but with no definition of national security.[115] A related statute, the Foreign Investment and National Security Act of 2007, adds "critical infrastructure" and "critical technologies" with undefined applications for national security..[116]

Over time, those statutes have widened the focus of "national security" from short-term military threats to longer-term trends in innovation and supply chain management.[117] For export/import policy, ever-expanding ranges of industries and product categories are being lumped into threats to national security, and the associated statutes and regulations rarely attempt to define the term.[118] Section 15, Part 744 of the Code of Federal Regulations, which defines the Entity List and related export control rules, makes copious use of the phrase "national security or foreign policy interests of the United States," including in several sub-section titles, but with no precise definition of the term.[119] The Entity List itself is defined as consisting of parties "reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States."[120] Note the use of undefined signifiers like *reasonably* and *significant*. Also, that same block of text is typically copied into Department of Commerce documents as the only necessary justification

---

[111] Ioannis Kokkoris, *Assessment of National Security Concerns in the Acquisition of U.S. and U.K. Assets*, 12 J. NAT'L SEC. L. & POL'Y 349, 374 (2022).
[112] 50 U.S.C. § 2404; *see also* 50 U.S.C. §§ 2401–20.
[113] *See* Ramachandran, *supra* note 103, at 39–40.
[114] *See* 50 U.S.C. § 4811(8).
[115] 50 U.S.C. § 4817(a)(1). Recall from above that the term "critical infrastructure" also suffers from a vague regulatory definition; *see supra* note 53 and accompanying text.
[116] Foreign Investment and National Security Act of 2007, Pub. L. No. 110–49, 121 Stat. 246, §§ 2(a)(6)–2(a)(7).
[117] *See* Nathan Bush, *Chinese Antitrust in the Trade War: Casualty, Refugee, Profiteer, Peacemaker*, 84 ANTITRUST L.J. 209, 224 (2021).
[118] *See* Heath, *supra* note 106, at 1042.
[119] 15 C.F.R. § 744 (2022).
[120] 15 C.F.R. § 744.16 (2022).

for adding a company to the Entity List. Perhaps a clearer definition of national security can be inferred from the list of countries for which military-related exports are restricted: Belarus, Burma (Myanmar), Cambodia, China, Russia, and Venezuela;[121] while Iran, North Korea, and Syria are named due to various sanctions from the Department of Defense.[122] However, the Entity List includes purported national security threats from companies in many nations that are not currently involved in military disputes with the United States, including several allies like Austria and Belize.[123] Purported threats from those friendly places are usually due to rogue companies re-exporting products to America's enemies, but the regulatory documents are devoid of information on whether the allied nations are doing anything to stop such practices by their own firms, or if they are even expected to.[124]

The Trump administration, almost immediately after Trump took office in January 2017, added a new wrinkle by conflating national security with winning trade wars.[125] The administration soon adopted the mantra "economic security is national security."[126] While initially focusing his general trade policy on imports, which can cause deficits as American money exits the country, Trump later turned to export controls as well, in the belief that foreign purchasers of American products and services, particularly in the telecom sector, could infiltrate American industries and networks.[127] This has caused a conflation of economic and

---

[121] 15 C.F.R. § 744.21(a)(1) (2022). For Burma, that country's outdated name is used in the Department of Commerce regulations, but its current name Myanmar is used for actual companies in the Entity List.

[122] 15 C.F.R. §§ 744.19(a)–(b) (2022).

[123] 15 C.F.R. pt. 744 (Supp. 4 2022).

[124] For example, an Austrian subsidiary of Gulf Gate Spedition GmbH (headquartered in Dubai) is lumped in with several other international subsidiaries of the parent company for suspicion of trafficking American products through Taiwan and Hong Kong on their way to Iran. However, the regulatory document contains no information on whether the friendly nation of Austria suspects such practices, whether it is conducting any investigations of its own, or whether it contributed to the Department of Commerce decision in America. *See* Addition of Certain Persons and Removal of Certain Persons from the Entity List, 15 C.F.R. pt. 744 (2022).

The same pattern can be seen for Ecotherm-Cryo Limited of Belize, which was one of several companies lumped into a blanket accusation of providing equipment assisting Russia during its 2022 invasion of Ukraine. *See* Further Imposition of Sanctions Against Russia with the Addition of Certain Entities to the Entity List, 15 C.F.R. pt. 744 (2022).

[125] *See* Chad P. Bown, *Export Controls: America's Other National Security Threat*, 30 DUKE J. COMP. & INT'L. L. 283, 287 (2020).

[126] *See* Peter Navarro, *Why Economic Security Is National Security*, REAL CLEAR POLS. (Dec. 9, 2018), https://www.realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security_138875.html.

[127] *See* Bown, *supra* note 125, at 289.

geopolitical objectives within U.S. trade policy, particularly toward China, with economic strategy becoming confused with defense strategy in possibly deleterious ways.[128] Research has shown that nations in a conflict that is framed in this fashion are likely to invoke threats to national security in order to bypass less exciting but more established regulatory processes.[129]

To further confuse the issue, human rights concerns were unexpectedly added to the Entity List in 2020, when the Department of Commerce listed various Chinese entities that were suspected of exploitation of the Uyghur ethnic group in the Xinjiang region.[130] This indicates further politicization of the Entity List and related regulations,[131] and a possible reaction to widespread media coverage of the plight of the Uyghurs,[132] as Democrats have pushed for more use of this export control technique against companies that sell their products to regimes that abuse human rights.[133] The Biden administration has actively added human rights concerns to its policies toward China, particularly suspicions of involvement by the nation's high-tech companies.[134]

The reasons for claiming that foreign firms are threats to national security are almost never cited in detail in the executive orders issued by presidents or in regulatory documents from the Department of Commerce or the Federal Communications Commission. Instead, vague political reasoning must often be gleaned from the associated press releases.[135] Regarding business with China in particular, national security rhetoric slowly emerged during the Obama administration but was amped up significantly during the Trump administration. This added increasingly expansive concerns about financial manipulation, military expansion, data surveillance, and telecommunications industry

---

[128] *See* Heath, *supra* note 106, at 1024.
[129] *Id.* at 1032.
[130] 15 C.F.R. pt. 744 (Supp. 4 2022).
[131] *See* Kokkoris, *supra* note 111, at 363.
[132] *See* James Griffiths, *From Cover-Up to Propaganda Blitz: China's Attempts to Control the Narrative on Xinjiang*, CNN (Apr. 17, 2021, 6:59 PM), https://www.cnn.com/2021/04/16/china/beijing-xinjiang-uyghurs-propaganda-intl-hnk-dst/index.html.
[133] *See* HOUSE COMM. ON OVERSIGHT & REFORM, 117ST CONG., MALONEY, WYDEN, SCHIFF, AND MEEKS LEAD HOUSE AND SENATE DEMOCRATS IN CALLING FOR MAGNITSKY ACT SANCTIONS AGAINST COMPANIES THAT ENABLE HUMAN RTS. ABUSES (Dec. 15, 2021), https://oversight.house.gov/news/press-releases/maloney-wyden-schiff-and-meeks-lead-house-and-senate-democrats-in-calling-for.
[134] *See* deLisle, *supra* note 81, at 72-73.
[135] *See* Kokkoris, *supra* note 111, at 366-67.

dominance to the catch-all term "national security."[136] This indicates a rising concern, if undeveloped, about the presence of Chinese firms in the American telecom marketplace, mixed with overuse of national security concerns to justify changes to trade policy.[137]

A plethora of statutes with inconsistent but equally vague definitions of national security, and oversight by many different agencies with their own definitions of the same, creates a non-transparent regime in which American watchdogs and listed firms are less able to review the effectiveness of export/import regulations in the telecom sector. Combined with inconsistent and inarticulate definitions of national security among the many agencies involved, there is no uniform method for enacting such restrictions or for the public to review the process. This also allows decisions to become politicized, and often with a retaliatory flavor.[138]

In a further twist, the Department of Commerce, when deciding that a foreign company should be added to the Entity List or subjected to other trade restrictions for national security reasons, is not required to provide that company or anyone else with an explanation, if that explanation would *also* endanger national security or if any of the relevant agency documents are classified,[139] thus creating a "catch-22" effect that can lead to non-transparent and politicized decision-making.[140] The Federal Communications Commission has added its own rule about withholding classified documents from citizen watchdogs and the companies that are denied subsidies under its own efforts to protect national security.[141] By definition, classified documents can never be released to citizens or journalists; this is often a valid concern for the government, but there is no way to tell if the decision to classify those documents is justified or legitimate in its own right, thus reducing transparency even further.[142]

---

[136] *Id.* at 369-71.
[137] *See Trump Blocks Broadcom's Bid for Qualcomm on Security Grounds*, BBC NEWS (Mar. 13, 2018), https://www.bbc.com/news/business-43380893.
[138] *See* Sullivan, *supra* note 19, at 325.
[139] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65321 (proposed Nov. 19, 2019) (to be codified at 15 C.F.R. § 7.104).
[140] *See* Burks, *supra* note 54, at 110-11.
[141] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. 11423, at ¶ 41.
[142] *See* Benjamin W. Cramer, *Old Love for New Snoops: How Exemption 3 of the Freedom of Information Act Enables an Irrebuttable Presumption of Surveillance Secrecy*, 23 COMMC'N L. & POL'Y. 91, 99 (2018).

Trump's restrictions, particularly on Huawei and ZTE, have been retained and only slightly modified (with some more focus on personal data security) by the Biden administration,[143] with the new President stating that China is "the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system."[144] With so much telecom networking equipment coming from that country, this statement creates a conflict with Biden's goals of expanding broadband networks into underserved areas of the country.[145] Biden's multi-trillion-dollar infrastructure spending bills, introduced in 2021, placed special emphasis on extensive broadband network development;[146] such plans will require a lot of components that have now been restricted via the recent import regulations, and this dilemma seems to not have occurred to the Biden administration beforehand.

Some critics have claimed that recent governmental investigations into Chinese firms like Huawei and ZTE, and suspicions about their equipment in American telecom networks, is based on longstanding anti-Chinese rhetoric that frames the nation as a threat, but as of 2023 those investigations have failed to find a "smoking gun" of irrefutable evidence that the equipment is being used to funnel sensitive American data back to the Chinese government.[147] Thus, a corresponding "smoking gun" of

---

[143] *See* Exec. Order No. 14034, 40 Fed. Reg. 31423 (June 9, 2021).

[144] *See* THE WHITE HOUSE, INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE 8 (Mar. 2021).

[145] *See* John Hendel, *Why Suspected Chinese Spy Gear Remains in America's Telecom Networks*, POLITICO (July 21, 2022, 4:30 AM), https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045.

[146] *See* Michael Laris, *How the House Spending Bill Funds Additional Infrastructure*, WASH. POST (Nov. 19, 2021, 9:55 AM), https://www.washingtonpost.com/transportation/2021/11/19/infrastructure-biden-spending-bill/.

[147] In 2022, journalists uncovered evidence that ByteDance (the Chinese parent company of the popular TikTok social media application) had reprimanded some employees who violated company policies about accessing users' personal data. Such revelations have not yet fueled investigations by the U.S. government, and it should be noticed that these revelations concern the management of data that users supply to international networks voluntarily, as opposed to Chinese government theft of secured data as a national security offense.

See, e.g., Emily Baker-White, *Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China*, BUZZFEED (June 17, 2002), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access; Drew Harwell, *TikTok's Chinese owner Fires Workers Who Gathered Data on Journalists*, WASH. POST (Dec. 22, 2022), https://www.washingtonpost.com/technology/2022/12/22/tiktoks-chinese-owner-fires-workers-who-gathered-data-journalists/.

widespread national security threats remains elusive as well. Subsequently, journalists have questioned if this xenophobic attitude prevents American officials from separating legitimate Chinese trade and investment from old-school espionage, and thus, national security.[148]

All of this leads to government documents that are not sufficiently informative for American watchdogs and listed firms. Documents announcing final decisions by the Department of Commerce or Federal Communications Commission to restrict exports/imports are readily available at U.S. government websites, and many are directly cited in this article. Such documents are usually thousands of words long, but with some crucial missing pieces. In short, they reveal the *what* of the decision but usually not the *why*. Supporting documents detailing the investigative and research processes that led to those ultimate decisions are not readily available, so the interested person must take the ultimate agency decision as a given. Per the themes of this article, this is not true transparency, and such practices could possibly be regarded as secrecy and obfuscation.

This pattern raises contradictions with American government transparency standards that may be ripe for litigation. For instance, the Administrative Procedure Act mandates that federal agencies must observe mandated decision-making processes, and includes rules for making the relevant documents available to the public.[149] Neither that statute nor its transparency requirements are mentioned in the federal regulations that govern the Entity List, or in President Trump's 2019 executive order, or in the statutes that instruct the FCC to maintain the newer Covered List of suspicious international telecom firms. This may be an honest oversight, but the practical result is that there is no mandated procedure for interested citizens or companies to find deliberative documents that influenced the ultimate decisions to restrict exports and imports.[150]

---

[148] *See* Katie Bo Lillis, *FBI Investigation Determined Chinese-Made Huawei Equipment Could Disrupt US Nuclear Arsenal Communications*, CNN (July 25, 2022, 4:12 PM), https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

[149] *See* Administrative Procedure Act of 1946, 5 U.S.C. §§ 551-59.

[150] As a partial counterexample, the website for the Bureau of Industry and Security offers free access to official letters that were sent to individuals and companies that were charged for specific export violations. These documents typically offer evidence of regulatory or criminal transgressions. For example, in 2021, Princeton University was fined $54,000 for 37 incidents in which its scientific researchers shipped animal pathogens to researchers in other countries, which was a violation of export restrictions. *See* U.S. Dep't of Com., Bureau of Indus. and Sec., *Order Relating to Princeton University*, charging letter E2642, Feb. 1, 2021,

Meanwhile, the vague definition of "national security" in the regulations and statutes described herein causes another problem. Interested persons could possibly obtain obscure agency decision-making documents under the Freedom of Information Act (FOIA), but that statute includes an exemption that allows agencies to withhold any document deemed relevant for national security and they do not have to provide evidence on *why* it is relevant for national security.[151] That exemption is frequently abused by agencies that would like to keep certain documents secret.[152] As concluded by one legal researcher writing about the use of export/import restrictions during the Trump administration: "[i]f everything is about national security, nothing is about national security."[153]

And finally, the present article makes use of many *final* documents that are easily found online via Department of Commerce websites and the online version of the Federal Register, and the availability of these documents satisfies the requirements of a 1996 amendment to FOIA, known as eFOIA, that mandated online access for agency documents created after that year.[154] However, *decision-making* documents that informed those final decisions are typically unavailable through such channels, if they were ever recorded at all. In addition to unsupported claims of threats to national security, the lack of information on who arrived at those conclusions and how they arrived at those conclusions does further damage to the transparency of the process.

---

https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=1287&Itemid=.

However, such documents apply to specific incidents in which charges were filed and either settled or sent through agency adjudication processes. Decision-making documents leading to wide export/import bans into the future for purposes of national security, which are the focus of the present article, cannot be found anywhere at the Department of Commerce website or linked to any of the final decision documents regarding the Entity List and related regulations as discussed herein.

[151] *See* Freedom of Information Act of 1966, 5 U.S.C. § 552(b)(1).

[152] *See, e.g.*, Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public's Right to Know About the CIA*, 17 STAN. L. & POL'Y. REV. 353 (2006); Susan Nevelow Mart & Tom Ginsburg, *[Dis-]nforming the People's Discretion: Judicial Deference Under the National Security Exemption of the Freedom of Information Act*, 66 ADMIN. L. REV. 725 (2014); David B. McGinty, *The Statutory and Executive Development of the National Security Exemption to Disclosure Under the Freedom of Information Act: Past and Future*, 32 N. KY. L. REV. 67 (2005).

[153] *See* Bown, *supra* note 125, at 286.

[154] Electronic Freedom of Information Act Amendments of 1996, Pub. L. 104-231, 110 Stat. 3048.

V. THE RAMIFICATIONS OF EXPORT/IMPORT RESTRICTIONS IN TELECOMMUNICATIONS

Upon the issuance of President Trump's 2019 executive order banning American telecom firms from doing business with companies that purportedly pose national security risks, the Chinese Foreign Ministry urged the United States to "stop using the excuse of security issues to unreasonably suppress Chinese companies."[155] Huawei, which was banned from doing business in the United States by the Department of Commerce a few days later, argued that the restrictions "will not make the U.S. more secure or stronger; instead, this will only serve to limit the U.S. to inferior[,] yet more expensive alternatives, leaving the U.S. lagging behind in 5G deployment, and eventually harming the interests of U.S. companies and consumers."[156]

According to many experts, America needs Chinese telecom networking equipment. For instance, Huawei's 5G components are widely regarded as affordable and reliable, and they have been adopted worldwide, particularly in less developed regions that need inexpensive telecom infrastructure.[157] These advantages have been highlighted by the Pentagon, indicating that some parts of the U.S. government would like to continue using Huawei's components,[158] and those components have been adopted by many smaller American service providers, particularly those serving rural areas.[159] Policymakers in the European Union have noted that any risks apparently posed by Huawei equipment can be tackled via security protocols or contractual negotiations, rather than threats or restrictions.[160] Instead, the United States has taken a less-nuanced stance based on perceived national security threats but with little articulation on what exactly those threats may be, mixed in with economic goals related to gaining advantage in the U.S.-China trade war.[161]

---

[155] Chamberlain, *supra* note 62.
[156] Commerce Dept. Bans Huawei, *supra* note 66.
[157] *See* Opderbeck, *supra* note 60, at 166.
[158] *See* Kimberly A. Houser, *The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World*, 57 SAN DIEGO L. REV. 549, 589-90 (2020).
[159] *See* Katie Mellinger, *TikTokers Caught in the Crossfire of the U.S.-China Technology War: Analyzing the History & Implications of Chinese Technology Bans on U.S. Domestic Expression and Access to Communications*, 11 WAKE FOREST J.L. & POL'Y. 689, 703-04 (2021).
[160] *See* Drew Hinshaw, *Allies Wary of U.S. Stance on Huawei and 5G*, WALL ST. J. (Apr. 9, 2020, 3:29 PM), https://www.wsj.com/articles/allies-wary-of-u-s-stance-on-huawei-and-5g-11586460582.
[161] *See* Russell Brandom, *Trump's Latest Explanation for the Huawei Ban Is Unacceptably Bad*, THE VERGE (May 23, 2019, 7:35 PM),

This gives the impression of political revenge against particular countries or companies rather than a coherent economic strategy.[162] Trump's executive order from 2019, which remains in effect, also allows the Department of Commerce to collect concerns about telecom-related national security threats from any private party that it deems credible.[163] This could lead to competitors tattling on each other, thus slowing down telecom network development for everyone. The inclusion of many different government agencies in the process can lead to mission creep as departments like Defense and Homeland Security meddle in telecom exports/imports to advance their own concerns about China or Russia.[164] Thus, a previously routine administrative process of assessing the export/import interests of American companies has been politicized to gain bargaining points in the trade war.[165] Even America's allies suspected that Trump's restrictions abused the "national security" frame for purposes of economic or political retaliation.[166] Those allies largely rebuffed Trump's efforts to push them into imposing their own restrictions against those firms.[167]

This has had an immediate impact on the Federal Communications Commission and its ability to foster advanced network development, which it is required to do by law.[168] When Trump issued his executive order, and when Commerce added Huawei and ZTE to the Entity List, the FCC adopted the administration's use of the national security frame and held a workshop in which various participants concluded that Huawei and ZTE equipment allows a hostile regime (China) to spy on American citizens and control the worldwide flow of information.[169] The commission next prohibited equipment from either company from being included in any telecom network development project that receives money from the Universal Service Fund,[170] because such funds should not be used to endanger national security, citing

---

https://www.theverge.com/2019/5/23/18637836/trump-huawei-ban-explanation-trade-deal-national-security-risk.

[162] *See* Burks, *supra* note 54, at 106.

[163] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65320-21 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).

[164] *See* Burks, *supra* note 54, at 107-08.

[165] *See* Bown, *supra* note 125, at 286.

[166] *Id.* at 300.

[167] *See* Zhao Minghao, *US Perception of and Response to the Digital Silk Road*, 84 CHINA INT'L. STUD. 84, 93 (2020).

[168] Telecommunications Act of 1996, 47 U.S.C. § 706(a).

[169] *See* Opderbeck, *supra* note 60, at 171-72.

[170] *See* Brian Fung, *US Regulators Rule That China's Huawei and ZTE Threaten National Security*, CNN (Nov. 22, 2019, 12:07 PM), https://www.cnn.com/2019/11/22/tech/fcc-huawei-zte/index.html.

suspected company links to the Chinese government.[171] The commission added suspicions that those companies' telecom network equipment could collect personal data or inject malware and viruses into American networks.[172] These claims were supported with citations to the 2019 Department of Commerce document that added Huawei to the Entity List, which as previously described, mentions national security many times without defining it or presenting specific evidence that it had been threatened by those firms.[173]

American telecom service providers have noted the disconnect when an equipment ban is framed as an urgent national security solution, but on-the-ground replacement of network components is not given the same consideration.[174] After deciding that equipment from Huawei and ZTE should not be used in American telecom networks in 2019, the FCC mandated a "rip and replace" policy requiring network providers to remove such components from their networks and replace them with others from supposedly friendlier firms.[175] The offending components are not so easy to remove from an integrated telecom network, and can be found in many different locations around such a network, including inside subscribers' homes and under busy streets.[176] FCC funding for this laborious effort was not made available until late 2020.[177] After being ordered to remove offending equipment from their networks, American service providers have claimed costs of $5.6 billion to remove those components and replace them with new ones, and this assumes that non-threatening replacements will be easily available and in sufficient quantities. In June 2022 Congress proposed emergency funding to cover about two-thirds of those costs in the form of direct subsidies, with the rest to be covered by the FCC.[178]

---

[171] *See* Fed. Commc'ns Comm'n, *Protecting National Security Through FCC Programs*, Report and Order, WC Docket No. 18-89, 34 FCC Rcd. 11423 (Nov. 26, 2019), at ¶¶ 48-54.
[172] *See* Todd Shields, *Huawei and ZTE Targeted While Security Ban Advances at U.S. FCC*, BLOOMBERG (Apr. 17, 2018, 11:06 AM), https://www.bloomberg.com/news/articles/2018-04-17/huawei-zte-targeted-as-security-ban-advances-at-u-s-fcc#xj4y7vzkg.
[173] *See* Additions to the Entities List, 84 Fed. Reg. 22,961, 22,961–62 (May 21, 2019); 15 C.F.R. pt. 744 (Supp. 4 2022)
[174] *See* Hendel, *supra* note 145.
[175] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. 11423, at ¶¶ 108-17.
[176] *See* Hendel, *supra* note 145.
[177] *Id.*
[178] *See* Joseph Marks, *A Plan to Strip Huawei from Rural Telecoms Is Still Short Billions,* WASH. POST (June 15, 2022, 7:36 AM),

Until those funds are in place, there are several possible ramifications for America's advanced telecom services. Some smaller (and especially rural) service providers will be unable to remove Huawei equipment for the time being; leaving their networks open to the suspected security risks; while other providers may be able to remove the Huawei equipment in the short term but will be unable to replace it rapidly, thus leaving their customers underserved.[179] There is another problem with existing Huawei or ZTE network equipment: if components that are currently in use malfunction or suffer wear and tear, they now cannot be easily replaced unless equivalents from approved firms can be found and integrated into the networks immediately. The recent regulations even prevent providers from calling Huawei or ZTE customer service when there are problems with currently installed components.[180] In fact, many of the 3G and 4G networks that still serve much of the United States contain networking equipment from Huawei and ZTE, and will continue to do so, until the unlikely advent of upgrades to 5G networks made up entirely of equipment from nations with which America is not engaged in trade wars.[181]

There is yet another way that these export/import restrictions can create negative impacts, and this time American high-tech firms will feel them. For example, Google could face a significant setback if it is unable to export its Android operating system to smartphones manufactured overseas by Huawei or ZTE.[182] Other American companies have been known to suffer sharp hits to their revenues, and stock valuations, if they are suddenly restricted from selling their products and services to Chinese customers in the world's largest marketplace.[183] Meanwhile, the recent export restrictions will have immediate effects on the U.S. economy. For instance, Huawei purchased $11 billion in equipment and services from American firms in the year before the company was placed on the Entity List—a sizeable amount of incoming money that was suddenly cut off by the export restrictions.[184] Restrictions on Huawei's

---

https://www.washingtonpost.com/politics/2022/06/15/plan-strip-huawei-rural-telecoms-is-still-short-billions/.

[179] *Id.*

[180] Hendel, *supra* note 145.

[181] *See* Houser, *supra* note 158, at 565.

[182] *See* Yang Jie & Dan Strumpf, *Who Needs Google's Android? Huawei Trademarks Its Own Smartphone OS*, WALL ST. J. (May 24, 2019, 6:19 AM), https://www.wsj.com/articles/who-needs-googles-android-huawei-trademarks-its-own-smartphone-os-11558693195.

[183] *See* Jay Greene, *In ZTE Battle, U.S. Suppliers Are Collateral Damage*, WALL ST. J. (Apr. 24, 2018, 5:30 AM), https://www.wsj.com/articles/in-zte-battle-u-s-suppliers-are-collateral-damage-1524562201.

[184] *See* Houser, *supra* note 158, at 584.

business have also resulted in significant layoffs of American workers at Huawei-affiliated facilities in the United States.[185]

And while export restrictions may result in an American firm's products remaining in the country rather than being sold to someone else, this is not a guarantee that the American marketplace can absorb the quantities that would have been exported. Thus, the benefits for national security are unlikely to outweigh the economic losses for American companies and consumers. Furthermore, restricting American exports can cause the items in question (or their technological equivalents) to become more expensive on the international market, thus hurting consumers and economies in all nations, including America and its allies.[186]

There is more bad news on the geopolitical front. Per Chinese law, companies are required to support government requests for espionage or the dissemination of propaganda. This is an offshoot of the country's history of Communist ideology, and the new breed of Chinese high-tech firms are not yet fully independent from government demands.[187] A 2021 investigation by the *Washington Post* revealed documents showing collaboration between Huawei and Chinese government agencies that conduct surveillance of the population,[188] and an investigation by the British Parliament the previous year found the same.[189] The company has long claimed that its relationship with the government is "no different" than that of any other private Chinese firm and it is unable to resist such demands.[190] It should also be noted that neither investigation uncovered evidence that the company's tactics inside China are repeated in other countries where its products are used.

Regardless, the close corporate/government ties in China mean that an attack (either rhetorical or economic) on a company is felt by the

---

[185] *See* Zak Doffman, *Huawei Blacklisting Is Forcing 'Extensive Layoffs' in U.S.*, FORBES (July 14, 2019, 2:20 AM), https://www.forbes.com/sites/zakdoffman/2019/07/14/huawei-blacklisting-now-forcing-extensive-layoffs-in-u-s-reports/?sh=5bcfa0fd67e9.
[186] *See* Bown, *supra* note 125, at 301.
[187] *See* Mellinger, *supra* note 159, at 696-97.
[188] *See* Eva Dou, *Documents Link Huawei to China's Surveillance Programs*, WASH. POST (Dec. 14, 2021, 4:00 AM), https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.
[189] *See* Gordon Corera, *Huawei: MPs Claim 'Clear Evidence of Collusion' with Chinese Communist Party*, BBC (Oct. 8, 2020), https://www.bbc.com/news/technology-54455112.
[190] *See* Li Tao, *Huawei Says Relationship with Chinese Government 'No Different' from Any Other Private Company in China*, S. CHINA MORNING POST (Dec. 26, 2019, 5:02 PM), https://www.scmp.com/tech/big-tech/article/3043558/huawei-says-relationship-chinese-government-no-different-any-other.

nation's leaders much quicker in China than in the United States. For Chinese companies like Huawei and ZTE, those firms are so closely tied to the Chinese regime that restricting them from doing business with or in the United States is likely to have serious geopolitical repercussions, as Premier Xi Jinping has been known to frame criticism of such companies as attacks on China itself.[191] This may result in poorly-considered retaliation, leading to a sense of burgeoning threats in the United States, which in turn leads to more retaliation and a cycle that ultimately benefits neither country.[192]

Export/import restrictions have thus emerged as a weapon in trade wars, but they are blunt and clumsy.[193] Overuse of such controls for political purposes can create an atmosphere of uncertainty in which America becomes a less attractive environment for research, development, and production by international firms. This can have direct economic effects if those activities are no longer performed on American soil, while other countries could take the lead in crucial emerging markets like 5G.[194] The development of 5G and future telecom technologies will require the two leading manufacturing nations—the United States and China—to admit their interdependence and to cooperate instead of engaging in short-term trade war tactics.[195]

Back-and-forth trade war restrictions are likely to increase tensions between the two nations, and they may no longer cooperate on mutually beneficial matters of bilateral trade. Thus, the restrictions achieve neither national security nor improvements to the balance of trade,[196] which is the apparent goal of recent statutes and regulations that tie those two concerns together. In telecommunications, the United States has a robust manufacturing sector for chips and coding, but the leading hardware manufacturers are in other countries, especially China.[197] While America was a leader in the development of 3G and 4G technologies, its newfound refusal to cooperate with China is likely to allow that nation to become a dominant force in 5G, with American firms that need components being relegated to navigating their own country's

---

[191] *See* Sullivan, *supra* note 19, at 348.
[192] *See* Biao Zhang, *The Perils of Hubris? A Tragic Reading of "'Thucydides' Trap'" and China-US Relations*, 24 J. CHINESE POL. SCI. 129, 139 (2019).
[193] *See* Bush, *supra* note 117, at 247.
[194] *See* Bown, *supra* note 125, at 294-95.
[195] *See* Houser, *supra* note 158, at 551-52.
[196] *Id.* at 592.
[197] *See* Brian Fung, *How China's Huawei Took the Lead over U.S. Companies in 5G Technology*, WASH. POST (Apr. 10, 2019, 4:01 PM), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

export/import regulations plus whatever retaliatory sanctions China may enact. In the meantime, China (and possibly the European Union) may enjoy the opportunity to set 5G technical standards.[198]

Upon the advent of the Trump administration's trade war strategy against China, China instituted some of its own retaliatory restrictions on American products and services.[199] In fact, the two nations may be headed toward what political scientists call "the Thucydides Trap," in which adversarial leaders try to one-up each other with emotional accusations that drift away from political realism, to the point at which both nations are disadvantaged.[200] The Thucydides Trap also arises when an established power (in this case, the U.S.) perceives threatening competition from a rising upstart (China), while the upstart gains exaggerated self-confidence from watching the established power stumble. This leads to even more emotional battles at the expense of reasoned negotiations.[201] Non-transparent export/import restrictions, that are based on vague definitions and closed-door processes in deciding that something is a national security risk, are unlikely to lead to the reasoned decision-making that is necessary for avoiding the Thucydides Trap.

Geopolitical conflicts are not always played out on the battlefield, and may instead take the form of regulatory battles within economic and administrative institutions. The overuse of "national security" as a justification for such battles degrades those institutions and increases the likelihood of non-transparent economic warfare in which established regulations are flouted, the affected parties are unable to evaluate what happened, and obscure policymakers remain unaccountable.[202]

CONCLUSION

The transparency of governmental operations requires more than just final documents. Understanding such documents requires context that may be found in related documents that are not so easily available, or which describe deliberations that may have never been recorded in the

---

[198] *See* Houser, *supra* note 158, at 601-03.
[199] *Id.* at 560-61.
[200] *See* Gries & Jing, *supra* note 91, at 456-57. Thucydides (c. 460-400 BCE) was an ancient Greek historian who theorized that emotional one-upmanship among leaders rather than reasoned political negotiations caused the Peloponnesian War between Athens and Sparta.
[201] *See* Zhang, *supra* note 192, at 131.
[202] *See* Heath, *supra* note 106, at 1096.

first place.[203] While Department of Commerce documents explaining that a company was added to the Entity List are plentiful, this may only serve as a convenient diversion away from a true understanding of the decisions announced therein. Thus, the interested person's attention is monopolized by the big picture, with a loss of much-needed details.[204]

This article has examined two different manifestations of non-transparency: (1) confusing agency procedures, and (2) poorly defined terminology that is used to justify final agency decisions. The first is the result of a mishmash of government agencies taking part in discussions of whether a foreign firm and its products are a threat, while the final regulatory documents are issued by two different agencies. The regulatory documents from the Department of Commerce and the Federal Communications Commission, in which companies are forbidden from conducting exports or imports because of national security threats, give the strong impression of being based on suspicions rather than hard evidence. This may not be the intention, but documents that are released to the public on this matter typically say that the entity in question has been determined to be a threat to national security, with occasional citations to related documents in which some other inscrutable agency practically said the same thing. This is circular logic at best and the interested citizen is unable to find actual deliberations that led to the ultimate decision.

The second manifestation of non-transparency revolves around the elusive definition of "national security," and sometimes related terms like "critical infrastructure." The same circular logic is at play. National security is named in many American statutes and regulations, but they often cite each other on the term's definition, or assume that it needs no definition at all. It becomes difficult, if not impossible, for the interested person to know which agency applied which working definition of national security to determine a threat that is then announced by either the Department of Commerce or the Federal Communications Commission.

On the matter of foreign threats, it is no secret that most (possibly all) telecom networks and applications can collect personal information, trade secrets, government documents, and any other unsecured digitized data and store it in databases. And some of that sensitive material may

---

[203] *See* Benjamin W. Cramer, *What the Frack: How Weak Industrial Disclosure Rules Prevent Public Understanding of Chemical Practices and Toxic Politics*, 25 S. CAL. INTERDISC. L.J. 67, 89 (2016).

[204] *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 94-95 (2014).

very well be leaked or even sold to unsavory characters. The present author acknowledges that foreign telecom equipment probably is being used by foreign governments to collect data on Americans and would not be surprised if the long-elusive "smoking gun" comes to light. But, for purposes of international policy, the present author also believes that this is a red herring because the U.S. government spies on its own citizens with impunity and has openly roped American telecom firms into the effort.[205] The only difference is that American officials say it is for our own safety,[206] while foreign governments who do the same thing are condemned as malicious.[207] When American government officials condemn foreign countries and their firms for spying on us, with a burning need for retaliation, those officials should look in the mirror. The facial images they will see are already plastered across the Internet.

More specifically for the telecommunications matters discussed in this article, banning foreign firms like Huawei and ZTE from the American marketplace will have significant impacts on a national network that requires imported components for building much-needed infrastructure, and that marketplace also benefits from exports that keep American manufacturers solvent. Governmental restrictions that damage this marketplace should be fully transparent. Perhaps residents of an underserved rural community would like to know why they are still waiting for advanced networks to be built. Given current transparency patterns, they may be able to locate a document in which a company that supplies affordable and much-needed components has been banned from the marketplace because an agency decided the company is a threat to national security, but with no further information available on how that determination was reached or the nature of the threat to national security, much less what that ideal means in the first place.

One researcher who has studied Trump's 2019 executive order for a widespread ban of telecommunications equipment concluded that "[t]he U.S. President alone should not hold so much control over the

---

[205] *See* Julia Angwin, Jeff Larson, Charlie Savage & James Risen, *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, PROPUBLICA (Aug. 25, 2015), https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help.

[206] *See* Michael Chertoff, *NSA Surveillance Vital to Our Safety*, USA TODAY (Sept. 11, 2013, 9:00 AM), https://www.usatoday.com/story/opinion/2013/09/11/nsa-privacy-chertoff-911-column/2793063/.

[207] *See* Jake Maxwell Watts & Adam Pasick, *NSA Surveillance Just Gave China's President the Perfect Come-Back Line*, QUARTZ, (July 21, 2022), https://qz.com/92047/nsa-surveillance-just-gave-chinas-president-the-perfect-come-back-line/.

future shape of the Internet,"[208] and related telecom technologies like 5G. The President's influence arises from the questionable use of executive orders reacting to unarticulated emergencies, and a regulatory structure in which the President's underlings in the Executive Branch must follow suit. Those agencies then face few requirements for the transparency of their ultimate regulatory decisions.

For America to serve the networking needs of its own citizens, and to remain a world leader in telecom research and development, a spirit of cooperation with partner nations is sorely needed. Export/import restrictions, based on poorly defined national security concerns, are blunt solutions for a challenge that requires finesse. If America chooses to remain suspicious of foreign networking components, the European Union's stance on security protocols and multilateral negotiations, rather than bans and restrictions,[209] will bring current trade war tensions back into the mundane but manageable realm of established regulations. Otherwise, back-and-forth bickering between nations will accomplish nothing for underserved communities at home.

[208] *See* Opderbeck, *supra* note 60, at 221.
[209] *See* Hinshaw, *supra* note 160.

VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

U.S. CRYPTOCURRENCY REGULATION: A SLOWLY EVOLVING STATE OF AFFAIRS

Dr. Aaron Poynton

After nearly a decade and a half since the creation of the first cryptocurrency, crypto regulation in the United States ("U.S.") is fragmented, with different measures taken at the federal and state levels and even within and amongst agencies. This sluggish speed is not necessarily a surprise as government regulation has always chased rapid advancements in technology and associated consumer and market behavior changes. However, this is a precarious position for the U.S.—and the world—as the U.S. is a leader in the global financial community, the high concentration of crypto-based wealth, and economies' increasingly interconnected and interdependent nature. This paper examines the history of currency, features of cryptocurrency, especially those features which make it prone to regulation, the U.S.' efforts to regulate cryptocurrency, reviewing current and proposed regulatory efforts, and lastly, concludes with an analysis of the research and provides suggestions to lawmakers and regulators. The central theme of the analysis will opine that cryptocurrencies, and their tangencies, such as the crypto-ecosystem they live within, increasingly pose a systematic risk to global financial markets, and little has been accomplished to protect against this from a regulatory perspective. Therefore, there is an imminent need for regulatory action, clarification, and harmonization. Nevertheless, it is essential to maintain a balance in regulatory measures, ensuring that they do not stifle the nascent crypto markets and the flourishing of financial technology innovation.

U.S. CRYPTOCURRENCY REGULATION:[1] A SLOWLY EVOLVING STATE OF AFFAIRS

*Dr. Aaron Poynton**

INTRODUCTION & BACKGROUND

Since the beginning of man and long before the establishment of the State, there has always been a need to exchange goods and services.[2] Before the concept of currency, it is believed that exchange was conducted through barter.[3] Market participants, often fellow villagers, would directly exchange one good or service for another without a medium of exchange; for example, a farmer may exchange a dozen chickens for a pair of shoes from a shoemaker. However, this process was limiting and inefficient as it required a *double coincidence of wants,*[4] did not provide transferability or divisibility, and had significant search, negotiation, and transaction costs.[5] As a result, new mediums of exchange developed over time. Initially, commercial (non-State) mediums developed using commodities and rarities that could be easily traded—cowrie, shells, salt, gold, iron rings, and brass rods.[6] For over 2,000 years, cities and empires traded this way without using coins or other standardized or government-issued currencies.[7]

Commodity mediums were eventually replaced in mid-600 B.C. with a form of *money*—a mutually accepted representation of value—its

* London School of Economics and Political Science.

[1] In the United States, the term "regulation" is distinct from the term "law." A law is passed by a legislative body where a regulation is an administrative agencies' standards and rules that govern how laws will be enforced. Regulations, while not laws, have the force of law because they are adopted under authority granted by statutes and frequently include penalties for violations. In this paper, the term "regulation" includes both laws and regulations.

[2] *See* generally ADAM SMITH, THE WEALTH OF NATIONS (Bibliomania.com Ltd, 2002).

[3] *See* David Graeber, DEBT: THE FIRST 5,000 YEARS 21 (Melville House Publ'n, 2001).

[4] "Double coincidence of wants": Each party must possess the exact good or be offering the exact service that the other party wants.

[5] Scott A. Wolla, *Money and Inflation: A Functional Relationship*, FED. RSRV. BANK OF ST. LOUIS, PAGE ONE ECON. NEWSL. (March 2013).

[6] *See generally* FELIX MARTIN, MONEY: THE UNAUTHORIZED BIOGRAPHY (NEW YORK, ALFRED A. KNOPF 2014). *See also* Paul Bohannan, *The Migration and Expansion of the Tiv.*, 24 AFR. J. OF THE INT'L AFR. INST. 2–16 (1954).

[7] Ben Alsop, *Money*, London: The British Museum, Room 68.

tangible counterpart, *currency*.[8] One of the earliest forms of currency, metal spade coins, was first used in Guanzhuang, China. Similarly, electrum coins (a naturally occurring mix of silver and gold) originated in Lydia, which now resides in central Turkey.[9] Electrum coins were soon adopted as the State currency by Lydia's King Alyattes, who is often regarded as the originator of coinage.[10] As states developed, there was a need for the government to collect revenue, so they adopted legal tender for citizens to pay taxes, fees, and fines. Currency issued and controlled by the state or central authority advanced, and today government-issued legal tender is the predominant source of currency.

Coins transitioned to paper currency during the Tang dynasty (618–907 AD) in China, eliminating the need to carry heavy strings of metallic coins.[11] Coins and paper currency were the primary means of exchange until the Song dynasty (960–1279 AD) when checks were introduced. This payment method later spread to Europe when trade with the Muslim world increased and Europeans began using checks themselves. Nevertheless, it took several hundred more years for the banking system to mature and checks to become ubiquitous. Checks had become the primary means of exchange in the U.S. by the mid-nineteenth century; by the 1950s, more than 28 million checks were written every day.[12]

While coins, paper money, and checks were the leading currency media over the past few centuries, several technological inventions revolutionized how money was exchanged. In the 1800s, the telegram was invented, which transformed long-distance communication. In 1871, Western Union introduced the electronic fund transfer ("EFT") using the telegraph, marking the beginning of electronic money.[13] Over the next

---

[8] DAVID W. PERKINS, CONG. RSCH. SERV., R45427, CRYPTOCURRENCY: THE ECONOMICS OF MONEY AND SELECTED POLICY ISSUES (2020) [hereinafter PERKINS: CRYPTOCURRENCY]; MARTIN, *supra* note 6.

[9] *Alsop, supra* note 7.

[10] Jona Lendering, *Alyattes of Lydia*, LIVIUS, https://www.livius.org/articles/person/alyattes/ (last updated April 21, 2020); *A Case for the World's Oldest Coin: Lydian Lion*, REID GOLDSBOROUGH, https://rg.ancients.info/lion/article.html (last visited Nov. 3, 2022).

[11] *See generally* John Pickering, *The History of Pape Money in China*, 1 J. AM. ORIENTAL SOC'Y 136, 136-42 (1871); Chelsea Allison, *Checking Out: A Brief History of Checks*, FIN, https://fin.plaid.com/articles/checking-out-a-brief-history-of-checks/ (last visited May 6, 2022).

[12] *Id.*

[13] Cecilia Hendrix, *6 Fascinating Things About Western Union's History*, W. UNION (Oct. 8, 2019), https://www.westernunion.com/blog/en/6-fascinating-things-about-western-unions-history/; Tim Ryan, *A Brief History of Western Union Money Transfer Services*, STREETDIRECTORY, https://www.streetdirectory.com/travel_guide/161051/money_management/a_brief

century, Western Union's "wire" service became the leading means to send money instantly over long distances. Western Union implemented new technologies to improve speed and efficiencies as technology advanced, such as when the microwave radio beam system was introduced in 1964.[14] Western Union's presence grew to a network of hundreds of thousands of locations in over 200 countries, serving many unbanked customers.[15]

In the second half of the twentieth century, a revolutionary development would forever disrupt the financial industry and later change the form of currency—the computer was invented. The computer is arguably the most significant invention—ever—and it marked the beginning of a new technological era. By 1983, *Time Magazine* named the computer its "Person of the Year," stating, "the entire world will never be the same."[16] In that article, Harold Todd, Executive Vice President at First Atlanta Bank, predicted, "[m]anagers who do not have the ability to use a terminal within three to five years may become organizationally dysfunctional. That is to say, useless."[17] Todd was right: the financial industry increasingly went electronic. Computers allowed financial transactions, such as currency exchange, to happen with speed, accuracy, and traceability. For example, the aforementioned 28 million checks processed daily in the 1950s grew to 49.5 *billion* checks processed in 1995 via automated electronic means.[18] Moreover, computer advancements facilitated other innovative means of currency exchange, such as debit and credit cards, which far exceeded checks and automated clearing house ("ACH") payments.[19]

As electronic currency exchange grew, the use of cash declined. In most developed countries, their economies transitioned from all cash to a mix of cash, check, and traditional electronic exchange (debit, credit,

---

_history_of__ western_union_money_transfer_services.html (last visited May 6, 2022).

[14] *Id.*

[15] Cecilia Hendrix, *6 Fascinating Things About Western Union's History,* WESTERNUNION (Oct. 8, 2019) https://www.westernunion.com/blog/en/6-fascinating-things-about-western-unions-history/.

[16] Otto Friedrich, *The Computer Moves In*, TIME (Jan. 3, 1983) https://content.time.com/time/subscriber/article/0,33009,953632-8,00.html.

[17] *Id.*

[18] Allison, *supra* note 11.

[19] In 2015 in the U.S., payments occurred via debit card (69.5 billion transactions worth $2.56 trillion), credit card (33.8 billion transactions worth $3.16 trillion), automated clearing house payment (23.5 billion transactions worth $26.83 trillion), and check payment (17.3 billion payments worth $26.83 trillion). DAVID W. PERKINS, CONG. RSCH. SERV., R45716, LONG LIVE CASH: THE POTENTIAL DECLINE OF CASH USAGE AND RELATED IMPLICATIONS 9 (2019) [hereinafter PERKINS: LONG LIVE CASH].

and ACH). In 2016, cash only accounted for 31 percent of all transactions in the U.S., and traditional electronic transactions accounted for 56 percent of transactions.[20] Although the use of cash has declined, some experts have repeatedly projected cash's obsolescence and disappearance. For example, when the Mondex machine and cards were initially rolled out in a 1995 trial, newspapers headlined, "Cash Died Today."[21] However, despite its initial excitement, the trials ended without a nationwide launch of the service. Likewise, a 2019 report from the U.S. Congressional Research Service, titled "Long Live Cash," acknowledges the decline of cash but cites its robustness and staying power, stating, "[c]ash has a number of advantageous features that has made it a simple and robust payment system throughout most of human history. It is difficult to imagine conditions under which cash would be replaced entirely, and disappear from the economy, at least in the near future."[22]

While currency exchange has evolved from coins to paper to checks to electronic, one feature has remained consistent throughout most of modern history—the currency exchanged has been *legal tender* and controlled by the government.[23] Any form of payment recognized by a government that is used to pay debts or financial obligations is considered legal tender. This includes not only taxes or other government payments, but all parties are generally obligated to accept the legal tender and settle debts.[24] Therefore, legal tender status gives the currency value because anyone who wishes to engage in basic economic activities must have and use this type of money. National currencies, such as the U.S. dollar, and multinational currencies, such as the Euro, are considered legal tender within their respective jurisdictions. Some countries with weak governments, institutions, or financial systems also use another country's currency as their legal tender, such as Panama with the U.S. dollar and South Georgia with the Sterling Pound. However, the government's exclusive control over the tender is more important than simply the recognition of legal tender.

In the U.S., Congress is granted the exclusive power by Article 1, Section 8 of the U.S. Constitution "[t]o coin Money, [and] *regulate the*

---

[20] PERKINS: LONG LIVE CASH, *supra* note 19, at 2.
[21] Alsop, *supra* note 7.
[22] PERKINS: LONG LIVE CASH, *supra* note 19, at 25.
[23] Although private banks did print their own currency before the 1930s, these banks were chartered by the United States Government, backed by U.S. treasury bonds, and were generally accepted to settle debts. Ben S. Bernanke, *A Century of US Central Banking: Goals, Frameworks, Accountability*, 27 J. ECON. PERSPECTIVES 3, 3-16 (2013).
[24] *See* PERKINS: CRYPTOCURRENCY, *supra* note 8 at 4.

Value thereof."[25] The Department of the Treasury creates and distributes coins and dollars to the public through its Bureau of Engraving and Printing. The Federal Reserve acts as the central bank and creates monetary policy. Its primary responsibilities include implementing national monetary policy, supervising and regulating banks, ensuring financial stability, and providing banking services.[26] Likewise, in Great Britain, the money supply is controlled by the Bank of England ("BOE"), and the Monetary Policy Committee ("MPC") makes monetary policy decisions.[27] In essence, the government has a powerful monopoly on money, which was a driving factor leading to the creation of cryptocurrencies. This control became especially important as governments transitioned from commodity-based currencies with an inherent value to currency where value is derived from government decree.

While the first government coins used for currency from China and Lydia had intrinsic value because they were created from a commodity, such as metal or Electrum, this had limited scalability and the concept could not be transferred to paper currency. Instead, governments began to issue currency that was backed by a commodity. For example, the United Kingdom adopted a gold standard for the Sterling in 1717. The gold standard backed the government-issued paper and coins with a promise to pay the currency holder a certain amount of gold on demand, and it established a fixed price for gold at which it buys and sells gold.[28] Master of the Mint, Sir Isaac Newton, established the gold price of £4.25 per fine ounce, which lasted two centuries.[29] This practice of backing a currency with gold spread beyond England to France, Germany, Switzerland, Belgium, and the U.S. during what is known as the "classical gold standard era."[30] In the United States, a bimetallic gold and silver standard existed in its early days, but the U.S. transitioned to an all-gold standard in 1879.[31] The *Gold Standard Act* of

---

[25] U.S. CONST. art. 1, § 8 (emphasis added).
[26] Adam Hayes, *Federal Reserve: What It Is and How It Works*, INVESTOPEDIA (June 7, 2022), https://www.investopedia.com/terms/f/federalreservebank.asp.
[27] *Monetary Policy*, BANK OF ENGLAND, https://www.bankofengland.co.uk/monetary-policy (last visited May 12, 2022).
[28] Chris Parker, *A Short History of the British Pound*, WORLD ECON. F., (June 27, 2016), https://www.weforum.org/agenda/2016/06/a-short-history-of-the-british-pound/.
[29] *Id.*
[30] James Chen, *Gold Standard: Definition, How It Works, and Example*, INVESTOPEDIA (updated August 25, 2022), https://www.investopedia.com/terms/g/goldstandard.asp.
[31] CRAIG K. ELWELL, CONG. RSCH. SERV., R41887, BRIEF HISTORY OF THE GOLD STANDARD IN THE UNITED STATES 6 (2011).

1900 fixed the value of a dollar to the equivalent of $20.67 per troy ounce.[32] Most of this gold was stored at the Fort Knox Bullion Depository, where it held up to 650 million ounces of gold in reserve, which is the equivalent of $1.2 trillion in April 2022.[33]

However, in the early 1930s, a historic shift occurred that unwound millenniums of convention. No longer was a medium of exchange either made from or backed by a commodity—*fiat money* was introduced. The term "fiat" comes from the Latin "fieri," which means an arbitrary act or "a decree, command, order."[34] During the Great Depression, most developed countries that followed the gold standard began to abandon it for a fiat currency. The gold standard was abandoned due to its volatility and the constraints it imposed on governments.[35] Governments were hampered in pursuing expansionary policies during the Depression by maintaining a fixed exchange rate.[36] Japan was the first large economy to make the switch in 1931, followed by much of Europe in the following years. The United States partially followed suit in 1933, eventually abandoning the gold standard in 1973.

Today, the gold standard is not used by any major government—currency does not have an intrinsic value and is not backed by a physical commodity, such as gold or silver. Instead, its value is derived from the "full faith and credit" of the issuing government. The U.S. Congressional Research Service notes, "[t]he currency is neither valued in, backed by, nor officially convertible into gold or silver."[37] The history described above of currency and technology created the perfect conditions for developing cryptocurrencies. Computing power has advanced exponentially since the invention of the computer, facilitating innovation in the financial markets. Additionally, the transition from the gold standard to a fiat currency has left a void for a medium of exchange that an omnipotent government does not control, paving the way for the adoption of cryptocurrencies. Today, despite its novelty, significant

---

[32] *Id.* at 10.
[33] *See generally Fort Knox Bullion Depository*, U.S. MINT, https://www.usmint.gov/about/mint-tours-facilities/fort-knox (last accessed May 9, 2022).
[34] *See generally Fiat,* ETYMYONLINE, https://www.etymonline.com/word/fiat (last visited May 13, 2022).
[35] *See* Barry J. EICHENGREEN, GLOBALIZING CAPITAL: A HISTORY OF THE INTERNATIONAL MONETARY SYSTEM, *1-85,* (Princeton *Univ.* Press *3rd ed.* 2019*), for an overview of the volatility of the gold standard.*
[36] *Id.*
[37] ELWELL*, supra* note 31, at Summary.

risks, and lack of regulation, an estimated 27 million Americans and 2.3 million Britons own cryptocurrency.[38]

The 2008 Global Financial Crisis eroded confidence and trust in banks and financial institutions and was a catalyst for introducing cryptocurrencies.[39] It appears to be more than a mere coincidence that Bitcoin, the inaugural and preeminent cryptocurrency, was introduced in January 2009 at the pinnacle of the Global Financial Crisis. While Bitcoin and other cryptocurrencies continue to advance, government regulators have moved to begin regulating them. However, regulatory efforts have been disjointed and uncoordinated as regulators strive to comprehend the innovative developments in cryptocurrency and its associated implications. Government proponents of cryptocurrency are going even further, exploring the adoption of cryptocurrencies as a central bank product, such as a Central Bank Digital Currency ("CBDC"). While the history of cryptocurrency is yet to be written, in less than a decade, it has accelerated from a little-known, niche technology to a mainstream financial asset that is primed for regulatory intervention before it expands further and poses a systemic financial risk.

Having a thorough understanding of the historical and contextual backdrop of traditional currency that prompted the inception of cryptocurrencies, the following section of this paper will explore the features of cryptocurrency in-depth, especially those features which make it prone to regulation. In the next section, this paper will examine the U.S.'s efforts to regulate cryptocurrency, reviewing current and proposed regulatory efforts. Lastly, this paper will conclude with an analysis of the research and provide suggestions to lawmakers and regulators. The fundamental premise of this analysis is to assert that cryptocurrencies, along with their related components such as the crypto-ecosystem, are progressively posing a systemic risk to global financial markets, and little has been accomplished to protect against this from a regulatory lens. Therefore, there is an imminent need for regulatory action, clarification, and harmonization. Nevertheless, it is essential to maintain a balance in regulatory measures, ensuring that they do not stifle the nascent crypto markets and the flourishing of financial technology innovation. While it is imperative to regulate the

---

[38] *Cryptocurreny Across the World: Global Crypto Adoption*, TRIPLEA, https://triple-a.io/crypto-ownership-data/ (last visited Nov. 11, 2022); Rupert Jones, *About 2.3m Britons Hold Cryptocurrencies Despite Warnings of Risk*, THE GUARDIAN (June 12, 2021, 11:50 EDT), https://www.theguardian.com/technology/2021/jun/17/about-23m-britons-hold-cryptocurrencies-despite-warnings-of-risk.

[39] Timothy C. Earle, *Trust, Confidence, and the 2008 Global Financial Crisis*, 29 RISK ANALYSIS, 6 (2009).

cryptocurrency sector, it must be acknowledged that the benefits of innovation cannot be overlooked.

I. FEATURES OF CRYPTOCURRENCY

Cryptocurrency, sometimes called *virtual currency* or *digital currency*, is "a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority."[40] The key features of a cryptocurrency are 1) digital (i.e., no physical currency), 2) decentralized (i.e., no central authority), 3) secured by cryptography (i.e., encryption algorithm), and 4) managed on a distributed ledger (i.e., peer-to-peer network). Other characteristics of some types of cryptocurrency include a limited supply (i.e., scarcity) and backing or pegging of the cryptocurrency to fiat money or an exchange-traded commodity (e.g., stable coin). These features distinguish a cryptocurrency from the ubiquitous fiat-money electronic cash, which is simply an electronic version of the government's physical currency with its exact features, benefits, and drawbacks.

There are over 18,000 cryptocurrencies in circulation, and the global cryptocurrency market is valued at over $1.28 trillion as of May 16, 2022.[41] Despite the plethora of cryptocurrencies, Bitcoin, the first cryptocurrency, remains the most prominent and dominant crypto in 2022—accounting for about 45% of the market.[42] However, stable coins, a type of cryptocurrency backed or pegged by an external reference, such as a fiat currency, are increasing in popularity and have snagged significant market share from Bitcoin in recent years. Stable coins also represent most of today's trading volume: in May 2022, stable coin trading made up over 89% of the crypto market's volume.[43] The stable coin Tether, which is pegged to the value of a U.S. dollar, made up nearly all of that volume.[44] Nonetheless, because of Bitcoin's history, market dominance, and popularity, it will be used predominantly throughout this paper for examples, references, and illustrations.

---

[40] Rally Point, *Crypto 101: Everything You Need to Know…to Start*, RALLY POINT (May 16, 2022), https://rallypoint.pr/crypto-101-everything-you-need-to-know/; Mary Eltawil, *Why Cryptocurrency?*, AZREIA (Sept. 1, 2022), https://azreia.org/chicago-title-agency/why-cryptocurrency/.
[41] *See generally Today's Cryptocurrency Prices by Market Cap*, COINMARKETCAP, https://coinmarketcap.com/ (last visited Nov. 8, 2022).
[42] *Id.*
[43] *Id.*
[44] *Id.*

Bitcoin was introduced in early 2009 by Satoshi Nakamoto, a pseudonym for an unknown computer programmer or group of programmers.[45] The launch followed Nakamoto's momentous white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, which made a case for creating a new online payment system and described its processes. Blockchain is the core technology at the heart of Bitcoin: a distributed database known as a distributed ledger technology (DLT) that is shared among computer network nodes.[46] The DLT allows digital information to be recorded and distributed but not edited—a feature often described as "immutable."[47] The Bitcoin blockchain went live on January 3, 2009, when the first block—coined the *genesis block*—was mined.[48] Sixteen months later, the first economic transaction occurred when a man paid 10,000 Bitcoin through barter on an internet forum to purchase two pizzas, establishing a then-market price of four Bitcoin per penny.[49] Later that same year, Bitcoin hit multiple exchange platforms, allowing for easier exchange, although its market price was zero dollars at launch.[50] Over the decade, the value and use of Bitcoin accelerated, and in 2021 Bitcoin had an average price of $47,300, and there were about 250,000 confirmed transactions per day.[51]

Bitcoin was created with a finite supply of 21 million coins that are mined using powerful computers solving complex math problems to discover new Bitcoins and confirm the legitimacy and accuracy of previous Bitcoin transactions.[52] Miners are rewarded with new Bitcoin, and the block reward given to Bitcoin miners for processing transactions

---

[45] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* METSDOWD, (Oct. 31, 2008, 12:10 EDT), https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.
[46] Adam Hayes, *What is Blockchain?* INVESTOPEDIA, https://www.investopedia.com/terms/b/blockchain.asp (last visited Mar. 12, 2022).
[47] *Id.*
[48] Paulina Likos and Coryanne Hicks, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS, (Feb. 4, 2020), https://web.archive.org/web/20210127074436/https://money.usnews.com/investing/articles/the-history-of-bitcoin.
[49] *Id.*
[50] Cryptopedia Staff, *The Early Days of Crypto*, CRYPTOPEDIA, (Mar. 17, 2022), https://www.gemini.com/cryptopedia/crypto-exchanges-early-mt-gox-hack#section-more-bitcoin-exchanges-hit-the-scene.
[51] Vildana Hajric, *Bitcoin's Plunge Is Hitting the Little Guy Who Got into Crypto During COVID Worst of All*, FORTUNE (May 10, 2022), https://fortune.com/crypto/2022/05/10/bitcoin-plunge-hitting-small-investor-crypto-during-covid/; *Confirmed Transactions Per Day*, BLOCKCHAIN, https://www.blockchain.com/charts/n-transactions (last visited May 12, 2022).
[52] Likos & Hicks, *supra* note 48.

is cut in half every 210,000 blocks mined, or roughly every four years.[53] The last halving event was on May 11, 2020, and the reward went from 12.5 Bitcoins per block to 6.25 Bitcoins per block, where it will remain until all coins have been mined.[54] Halving allows for controlled, synthetic inflation with a predictable and decreasing inflationary impact over time. All Bitcoins are estimated to be mined around 2140.[55] After that, miners are expected to be paid a fee for their work to validate and confirm new transactions.[56] However, it is unknown whether Bitcoin will remain the dominant cryptocurrency or it will be replaced with another cryptocurrency, such as the emerging stable coins. New crypto coins and tokens are coming into the market at a brisk pace. As of January 2021, there were 5,728 initial coin offerings ("ICOs")—an unregulated method to raise capital for a new cryptocurrency or crypto ventures—valued at more than $27 billion. [57]

The name "Crypto*currency*" is a misnomer because cryptocurrencies are rarely used as currency in the traditional sense. A comprehensive review of all cryptocurrencies found that two-thirds of all cryptocurrency transactions are non-economic transactions.[58] Transactions do not involve a user purchasing something with the currency but rather involve transactions between a single user's own crypto accounts. According to a joint study conducted by finance professors Antoinette Schoar at the MIT Sloan School of Management and Igor Makarov of the London School of Economics, 90% of Bitcoin transactions are "not tied to economically meaningful activities."[59] This is because currency is a medium of exchange representing money—and cryptocurrency is a poor representation of money.

---

[53] Luke Conway, *Bitcoin Halving*, INVESTOPEDIA, https://www.investopedia.com/bitcoin-halving-4843769 (last visited May 13, 2022).
[54] *Id.*
[55] Benedict George, *What Happens When All Bitcoin Are Mined*, COINDESK, https://www.coindesk.com/learn/what-happens-when-all-bitcoin-are-mined/ (last visited May 13, 2022).
[56] Conway, *supra* note 53.
[57] Oksana A.Karpenko, Tatiana K. Blokhina, and Lali V. Chebukhanova, *The Initial Coin Offering (ICO) Process: Regulation and Risks*, J. RISK AND FIN. MGMT. 14: 599 (2021); *Investor Bulletin: Initial Coin Offerings*, SEC (July 25, 2017), https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings [hereinafter Investor Bulletin].
[58] Olga Kharif, *Up to Two-Thirds of Bitcoin Transactions Have No Economic Value*, BLOOMBERG (July 26, 2018, 9:07 EDT), https://www.bloomberg.com/news/articles/2018-07-26/up-to-two-thirds-of-bitcoin-transactions-have-no-economic-value.
[59] Igor Makarov & Antoinette Schoar, *Blockchain Analysis of the Bitcoin Market* (Oct. 13, 2021), https://ssrn.com/abstract=3942181.

Money is a mutually accepted representation of value, and currency is its tangible counterpart. Money should have the three following characteristics: a medium of exchange, a unit of account, and a store of value. A widely accepted expanded definition for each category is:

> [t]o function as a *medium of exchange*, the thing must be tradable and agreed to have value. To function as *unit of account*, the thing must act as a good measurement system. To function as a *store of value*, the thing must be able to purchase approximately the same value of goods and services at some future date as it can purchase now.[60]

The extreme volatility alone disqualifies cryptocurrency as a well-functioning store of value and unit of account. For example, Bitcoin has an annualized volatility of 81%, meaning extreme price swings are common.[61] These swings can be dramatic, like when Bitcoin lost 60% of its value in one month between January and February 2018.[62] Furthermore, cryptocurrency's absence of legal-tender status, lack of ubiquitous acceptance, high transaction costs, and other practical factors make it a dubious medium of exchange.

Despite cryptocurrency's current lack of value as money and its lack of use as currency, crypto still offers several conceivable advantages and possesses future potential. Proponents of crypto refer to its benefits of privacy, security, speed, cost, mobility, accessibility, and immutability. However, the most notable feature of cryptocurrency is its decentralization, meaning there is no central authority, such as a central bank or government that controls the currency. Crypto advocates cite this feature as eventually allowing crypto to be more efficient and secure than current monetary and payment systems.[63] Modern financial institutions operate and maintain sizeable electronic network infrastructure, employ people, and take time to complete transactions, which adds cost and complexity, particularly in international

---

[60] PERKINS: CRYPTOCURRENCY, *supra* note 8, at 2.
[61] Alex Botte & Mike Nigro, *Risk Analysis of Crypto Assets*, TWO SIGMA, https://www.twosigma.com/articles/risk-analysis-of-crypto-assets/ (last visited May 22, 2022).
[62] Ben Popken, *Bitcoin Loses More Than Half Its Value Amid Crypto Crash,* NBC NEWS (Feb. 2, 2018, 4:43 EDT), https://www.nbcnews.com/tech/internet/bitcoin-loses-more-half-its-value-amid-crypto-crash-n844056.
[63] PERKINS: CRYPTOCURRENCY, *supra* note 8, at 2.

transactions.[64] Proponents believe that removing these intermediaries will improve economic efficiency by reducing costs through competition or eliminating them.[65]

Related to crypto's decentralization feature is increasing credibility and trust relative to fiat currency. In the United States, trust in the federal government and financial institutions remains low, with only 39% of Americans trusting the federal government and 33% of Americans trusting financial institutions.[66] According to the most recent Chicago Booth/Kellogg School Financial Trust Index (FTI), the 33% of Americans who trust financial institutions is an "all-time high" since the index was established in 2008 during the Great Financial Crisis (GFC).[67] However, this report was published in 2020 before the after-effects of the COVID-19 stimulus spending were felt. Today, due at least partly to extraordinary government stimulus spending not linked to productivity, America is experiencing high inflation, and consumer confidence is at an 11-year low.[68] The current sentiment likely reflects further government and financial institution trust decline.

Waning confidence in government, its fiat currency, and financial institutions motivate people to acquire and use Bitcoin and other cryptocurrencies to hedge against fiat. In contrast to declining trust in financial institutions, Bitcoin's unique features and staying power have increased cryptocurrency trust. A recent survey reported that 50% of professionals trust cryptocurrency, and 57% currently own some.[69] What's more, financial institution employees had much more trust, with 90% of professionals at JP Morgan Chase and 70% of workers at Goldman Sachs saying they trust cryptocurrency.[70] Another survey found

---

[64] *Id.* at 15.
[65] *Id.* at 15-16.
[66] Megan Brenan, *Americans' Trust in Government Remains Low*, GALLUP, (Sept. 30, 2021), https://news.gallup.com/poll/355124/americans-trust-government-remains-low.aspx; Paolo Sapienza & Luigi Zingales, *Financial Trust Index*, CHI. BOOTH KELLOGG SCHOOL, (last visited May 23, 2022), http://www.financialtrustindex.org/resultswave28.htm.
[67] *Id.*
[68] Megan Henney, *Consumer Confidence Sinks to 11-Year Low in May as Inflation Rages*, FOX BUS., https://www.foxbusiness.com/economy/consumer-confidence-sinks-may-inflation (last visited May 24, 2022).
[69] Benjamin Powers, *Half the Professionals Surveyed in Anonymous Poll 'Trust' Crypto*, COINDESK (Sept. 14, 2021, 8:20 PM), https://www.coindesk.com/markets/2021/03/03/half-the-professionals-surveyed-in-anonymous-poll-trust-crypto/.
[70] *Id.*

that 41% of people globally trust Bitcoin over their local currency.[71] Established cryptocurrencies, such as Bitcoin, are gaining the public's trust despite their turbulent past. The growing trust and popularity of cryptocurrencies have garnered lawmakers' and regulators' attention, who often cite crypto's numerous potential risks and drawbacks.

Many people who question the benefits of cryptocurrency cite the exaggeration of its benefits. Nearly every crypto benefit has practical counterpoints overlooked by proponents who hype cryptocurrency. Take privacy and security as an example—two of the hallmark features that led criminals to flock to cryptocurrency. As it turns out, this is more of an "in theory" feature than a "real-world" one. Two features make this system *theoretically* tamperproof: a cryptographic fingerprint unique to each block and a "consensus protocol," the process by which network nodes agree on a shared history.[72] However, hackers have repeatedly demonstrated vulnerability in the system using sophisticated methods, such as an "eclipse attack" that fools the blockchain network by confirming fake transactions.[73] In 2021 alone, there were over $7.7 billion stolen as a result of crypto hacks.[74] The trend accelerated in 2022 with the infamous March 2022 hack of $600 million that stole from Ronin Network—an NTF gaming blockchain platform.[75] This hack occurred only *one month* after the February 2022 Wormhole attack, where hackers stole 120,000 wETH, a token pegged to Ether, valued at $325 million.[76]

Likewise, cryptocurrency is not as private as many believe. This was demonstrated in 2018 when Mashael Al Sabah, a cybersecurity researcher at the Qatar Computing Research Institute, was able "to trace purchases made on the black-market 'dark web' site Silk Road back to users' real identities simply by culling through the public Bitcoin

---

[71] Eric Vazquez, *Why the Success of Alts Like Dogecoin Is Promising for the Future of Bitcoin*, PREMISE (Nov. 2, 2021), https://www.premise.com/blog/why-the-success-of-alts-like-dogecoin-is-promising-for-the-future-of-bitcoin/.
[72] Mike Orcutt, *How Secure Is Blockchain Really?*, MIT TECH. REV. (Apr. 25, 2018), https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.
[73] *Id.*
[74] Carly Page, *FBI Eyes Ransomware Profits with New Cryptocurrency Crimes Unit,* TECHCRUNCH+ (Feb. 18, 2022, 9:58 AM), https://techcrunch.com/2022/02/18/fbi-ransomware-cryptocurrency-crimes/.
[75] Joe Tidy, *Ronin Network: What's a $600m Hack Says About the State of Crypto*, BBC NEWS (Mar. 30, 2022), https://www.bbc.com/news/technology-60933174.
[76] *Wormhole Cryptocurrency Platform Hacked for $325M After GitHub Bug,* 6PARK.NEWS/USA (Feb. 3, 2022, 5:43 AM), https://6park.news/usa/wormhole-cryptocurrency-platform-hacked-for-325m-after-github-bug.html.

blockchain and social media accounts for matching data."[77] Because cryptocurrency transactions are all publicly recorded, identifying the wallets used by buyers to store their digital currency is simple and it is often a starting point in unraveling anonymity.[78] This is especially the case now since crypto platforms are legally required to know the identities of their customers.[79] The U.S. Department of Justice (DOJ) and other international organizations are increasingly able to track and recover cryptocurrency used in illegal activity. For example, in February 2022, the DOJ announced it seized $3.6 billion of Bitcoin stolen in the 2016 hack of Bitfinex and charged the suspects with conspiracy to commit money laundering and conspiracy to defraud the United States, a crime that carries a sentence up to 25 years in prison.[80]

Other economic and efficiency aspects of touted cryptocurrency benefits are also shaky and exaggerated. Increased speed and reduction or elimination of intermediary infrastructure appear to be two of these questionable features. In 2022, the average Bitcoin transaction took forty minutes,[81] compared to the average Visa credit card chip transaction, which takes less than two seconds.[82] Moreover, one of the key characteristics of crypto is its direct peer-to-peer network and the promise to eliminate middlemen. The original Bitcoin whitepaper by the pseudonym Satoshi Nakamoto states in its first sentence that Bitcoin "would allow online payments to be sent directly from one party to another without going through a financial institution."[83] However, an ecosystem of crypto-asset service providers (CASPs), such as wallets, exchanges, and trading platforms, performs the same functions as

---

[77] MIT Technology Review Insights, *Cryptocurrency Isn't Private—But with Know-How, It Could Be*, MIT TECH. REV., (Oct. 28, 2021), https://www.technologyreview.com/2021/10/28/1027250/cryptocurrency-isnt-private-but-with-know-how-it-could-be/.

[78] Rebecca Heilweil, *The Rise of the Crypto Cop*, VOX, (May 11, 2022, 11:30 AM), https://www.vox.com/recode/2022/5/11/23065956/detectives-crypto-cops-irs-fbi-cyber-bitcoin.

[79] *Id.*

[80] U.S. Dep't of Just., Off. of Pub. Aff., *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency,* U.S. DEP'T JUST. (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[81] *Average Transaction Speed of 66 Cryptocurrencies with the Highest Market Cap as of September 2022*, STATISTA, https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/ (last visited May 28, 2022).

[82] Chris Isidore, *Visa Moves to Speed Up Chip Card Transactions*, CNN MONEY, (Apr. 20, 2016, 7:45 AM), https://money.cnn.com/2016/04/20/pf/visa-chip-card-speed/index.html.

[83] Nakamoto, *supra* note 45.

custodians, stock exchanges, and brokers in traditional financial institutions.[84] Dr. Philipp Paech with the London School of Economics writes, "Structurally, the functions are comparable, and so are the ensuing risks . . . the pure existence of these intermediaries contradicts . . . the promises on which the crypto-space is built."[85]

In summary, the benefits of cryptocurrency were built on features and characteristics that have been oversold and morphed into what increasingly looks like a more traditional finance space, and regulation is no exception. The largely unregulated beginnings that cryptocurrency operated within was a key concern for government officials, and over the past several years, authorities have begun to regulate cryptocurrency, but more work needs to be done. According to the U.S. Security and Exchange Commission (SEC) Chairman, novel financial services never existed long-term outside the regulatory perimeter because financial services required trust.[86] The SEC Chairman noted that much of what currently constitutes the cryptocurrency market would either disappear or enter the regulated space.[87] The following section of this paper will review the U.S.'s current and proposed efforts to bring cryptocurrency into its regulatory sphere.

II. U.S. CRYPTOCURRENCY REGULATORY LANDSCAPE

The U.S. financial regulatory framework is vast, comprehensive, and complex. In the U.S., a constitutional federal republic system of government exists. The U.S. has fifty-one separate and autonomous governments in its simplest form—fifty state governments and one federal government. Federal and state governments have independent and autonomous authority over their respective territories through separate administrative, legislative, and judicial branches. This authority includes broad powers such as assessing, levying, and collecting taxes; passing and enforcing laws; and appointing officials. They also bear many responsibilities, such as providing public services and ensuring people's safety and well-being, including financial regulation. Even though each government is distinct and autonomous, they are not wholly independent of one another. Many of their powers and responsibilities are shared and divided, resulting in interdependence

---

[84] Philipp Paech, "Crypto Assets" (lecture taught at the London School of Economics and Political Science in 2021) (on file with author).
[85] *Id.*
[86] *Id.*
[87] *Id.*

at all levels of government. This shared and divided governance method is woven into the republic's fabric and is at the heart of American federalism.

The federal government's authority is derived from and limited to the powers explicitly granted to it in the U.S. Constitution, including those implied by the Constitution's text and structure. The delegated and enumerated powers are found in Article I, Section 8 and include the authority to *borrow and coin money*, regulate commerce with foreign nations, declare war, raise and support armies, provide and maintain a navy, and call forth the militia to execute the laws of the union, suppress insurrections, and repel invasions.[88] Except for the powers delegated to the federal government, the Constitution reserves all other powers to the states and the people.[89] Despite its limited powers, the federal government is supreme: Article VI, clause 2 of the U.S. Constitution, often referred to as "The Supremacy Clause," states, "the Laws of the United States … shall be the supreme Law of the land."[90] This means that no state can pass a law that conflicts with the supreme laws of the federal government. Regardless of the type of government, one of the most fundamental responsibilities of any government is to protect its citizens—and financial regulation aims to do this.

Financial regulation is a tool for the government to protect its people through transparency, fairness, and honesty and protect the government's interests in maintaining the financial system's integrity, stability, and efficiency to facilitate growth. The American system of federalism means that states and the federal government may each pass their own laws and enact regulations to oversee financial markets and companies. In practice, federalism leads to a complex patchwork of overlapping regulatory agencies and efforts. In addition to the fifty state legislatures and U.S. Congress, there are multiple regulatory bodies, including the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), Commodity Futures Trading Commission (CFTC), Financial Industry Regulation Authority (FINRA), State Bank and Insurance Regulators, and the Securities and Exchange

---

[88] U.S. CONST. art. I, § 8*; see also* Aaron S. Poynton, The Duel Over Duality: Effects of Federalism on the United States National Guard's Emergency Response Mission (2010) (unpublished Ph.D. dissertation, University of Baltimore) (on file with University of Baltimore).

[89] Poynton, *supra* note 88.

[90] U.S. CONST. art. VI, cl. 2.

Commission (SEC).[91] This regulatory framework serves as the foundation for the current efforts to regulate cryptocurrency.

There are two primary approaches to cryptocurrency regulation that are taking place concurrently. First, government officials are regulating cryptocurrencies through existing laws and authorities. However, many are concerned whether existing laws and regulations adequately and efficiently address the risks posed by cryptocurrency. For example, SEC Chairman Jay Clayton stated in testimony to Congress in 2018 that "[t]he recent proliferation and subsequent popularity of cryptocurrency markets creates a question for market regulators as to whether our historic approach to the regulation of sovereign currency transactions is appropriate for these new markets."[92] Second, legislators are looking for new laws and regulations to govern cryptocurrencies and their ecosystems, some of which is happening at the state level. However, there are renewed efforts to take a more comprehensive, federal approach following several incidences, such as the crash of TerraUSD, a stablecoin whose value plummeted 98% in May 2022, and the November 2022 collapse of FTX, which lost $8.9 billion in deposits.[93]

Each approach will be discussed further below. Regardless of the path, there are three general government responses to cryptocurrencies: 1) encouraging the use and development of cryptocurrencies within the jurisdiction; 2) prohibiting or restricting the use of cryptocurrencies within the jurisdiction; and 3) regulating the use of cryptocurrencies to reduce potential risks while encouraging financial innovation.[94] Because cryptocurrencies are still relatively new, government approaches are still evolving in all cases. [95]

With Bitcoin millionaires appearing overnight, the first aspect of cryptocurrency that the government addressed was how to tax cryptocurrency. The Internal Revenue Service (IRS) issued Notice 2014-

---

[91] Michael Schmidt, *Financial Regulators: Who They Are and What They Do*, INVESTOPEDIA (Dec. 6, 2021), https://www.investopedia.com/articles/economics/09/financial-regulatory-body.asp#toc-state-securities-regulators.

[92] Jay Clayton, *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CTTC*, U.S. SEC. & EXCH. COMM'N. (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission.

[93] *TerraUSD*, COINDESK, https://www.coindesk.com/price/terrausd/ (last visited May 28, 2022); Alexander Saeedy, *FTX Says $8.9 Billion in Customer Funds Are Missing*, WSJ (Mar. 2, 2023), https://www.wsj.com/articles/ftx-says-8-9-billion-in-customer-funds-are-missing-c232f684.

[94] REBECCA NELSON, CONG. RSCH. SERV., R45440, INTERNATIONAL APPROACHES TO DIGITAL CURRENCIES 1 (2018).

[95] *Id.*

21 in March 2014, stating that cryptocurrency would be classified as property rather than currency for federal income tax purposes.[96] States commonly follow the federal treatment, although due to its novelty and lack of harmonization, states currently differ in their treatment of cryptocurrency for tax purposes.[97] Cryptocurrency is calculated as a capital gain or loss and is generally taxed at a lower rate than ordinary income, with a top federal tax bracket of 20% versus 37%, as long as the asset is held for at least one year.[98] Those who trade cryptocurrency frequently and hold less than one year are generally taxed at ordinary income rates. Suspecting many sellers of cryptocurrencies were not paying taxes on their gains, in July 2019, the IRS began sending letters to cryptocurrency owners whose information they received from crypto exchanges as part of their know-your-customer (KYC) requirements.[99] The letters advised owners to file amended tax returns and pay back taxes based on the IRS's suspicions that many were not properly paying taxes on their gains.[100]

Crypto exchanges are required to collect KYC and other due diligence information, but they are not required to report transactions to the IRS automatically. In contrast, broker-dealer firms and banks must report all securities and cash transactions over $10,000 to the IRS.[101] As a result, the IRS requests "John Doe" summons court orders to gain information about possible tax-evaders, which is a court order allowing them to gather information from third parties, such as banks or other financial institutions, even if they don't have the names of the individuals involved. In 2021, the IRS stated it would increase the use of these

---

[96] U.S. INTERNAL REVENUE SERV., NOTICE 2014-21 (2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

[97] Scott Schiefelbein & Tyler Greaves, *Uncharted Territory: The State Income Tax Implications of Blockchain Technology and Cryptocurrency*, DELOITTE TAX LLP 1 (2020), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Tax/us-uncharted-territory-state-income-tax.pdf.

[98] *IRS Provides Tax Inflation Adjustments for Tax Year 2022*, U.S. INTERNAL REVENUE SERV. (Nov. 10, 2021), https://www.irs.gov/newsroom/irs-provides-tax-inflation-adjustments-for-tax-year-2022.

[99] *IRS Has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency's Larger Efforts*, U.S. INTERNAL REVENUE SERV. (July 26, 2019), https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts.

[100] Susan Tompor, *Crypto Taxes: Not as Easy to Hide from as You'd Imagine*, DETROIT FREE PRESS (Mar. 25, 2022, 6:01 AM), https://www.freep.com/story/money/personal-finance/susan-tompor/2022/03/25/taxes-bitcoin-digital-currency-crypto/6972094001/.

[101] *Understand How to Report Large Cash Transactions*, U.S. INTERNAL REVENUE SERV. 1 (Feb. 2021), https://www.irs.gov/newsroom/understand-how-to-report-large-cash-transactions.

summonses and launched Operation Hidden Treasure, a new tax enforcement initiative for cryptocurrency-related tax evasion.[102] However, many exchanges already reported this information to the IRS voluntarily and notified account holders via forms 1099K, 1099-MISC or 1099B.[103] Reporting has become a legal requirement beginning in 2023 as the Infrastructure Investment and Jobs Act (IIJA) mandates that exchanges generate 1099-Bs and report to the IRS. In addition to the revenue generated by the government, the collection of transaction information serves as a baseline tool to counter illegal activity—a key concern for regulators.

Most financial laws and regulations were drafted prior to the invention and subsequent growth of cryptocurrencies, raising concerns about whether existing laws and regulations adequately and efficiently address the risks posed by cryptocurrency.[104] Nevertheless, some of the first regulatory efforts have adopted current regulations, akin to the metaphor "fitting a square peg into a round hole." As noted above, the American system of federalism constructs a fragmented and overlapping dual federal-state regulatory system. Moreover, the regulatory regime has evolved mainly due to major historical financial crises.[105] These characteristics form an imperfect set of conditions to regulate cryptocurrency, and one must wonder if regulation is always chasing the last crisis. For example, following the Great Financial Crisis of 2008, the Dodd-Frank Wall Street Reform and Consumer Protection Act created the Financial Stability Oversight Council (FSOC) to address the regulatory system's fragmentation, and prevent systemic failure.[106] The FSOC is only now beginning to address the risks of cryptocurrencies.

The FSOC provides the U.S. financial industry's first comprehensive monitoring system to identify risks, promote market discipline, and respond to emerging risks.[107] In 2021, the FSOC recommended in its annual report that "state and federal regulators review available regulations and tools that could be applied to digital

---

[102] Philip J. Bezanson, Anne M. Termine & Brittney E. Justice, *The IRS Is Mining for Crypto Account Holders*, 172 NAT'L L. REV. (June 21, 2022), https://www.natlawreview.com/article/irs-mining-crypto-account-holders.
[103] Andrew Perlin, *Everything You Need to Know About Crypto 1099s in 2023*, TOKENTAX (Apr. 12, 2023), https://tokentax.co/blog/form-1099-crypto-exchange; *See also* I.R.S. Form 1099-b, https://www.irs.gov/forms-pubs/about-form-1099-b.
[104] PERKINS: CRYPTOCURRENCY, *supra* note 8, at 15.
[105] MARC LABONTE, CONG. RSCH. SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 1 (2020).
[106] *Id.*
[107] *Financial Stability Oversight Council*, U.S. DEP'T OF TREAS. (last visited May 28, 2022), https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc.

assets." Particularly, it focused on stablecoins, stating, "[a] run on stablecoins during strained market conditions may have the potential to amplify a shock to the economy and the financial system."[108] The recommendation followed the President's Working Group on Financial Markets Report on Stablecoins that echoed similar concerns and warned that stablecoins are "not subject to a consistent set of prudential regulatory standards."[109] It cites a loss of value risk associated with a run on stablecoins; payment system risks, "including credit risk, liquidity risk, operational risk, risks arising from improper or ineffective system governance, . . . settlement risk" risk of scale, systemic risk, and concentration of power.[110] In essence, these reports sounded the alarm for the first time that a cryptocurrency posed a systemic risk to the financial system—an eerie reminder of 2008. The President's report recommends legislative action to close the regulatory gaps by having legislation provide consolidated supervision, prudential standards, and a federal safety net.[111] Following this report, the stablecoin TerraUSD crashed, and legislative initiatives have been moved to the forefront of Congress' agenda, where they have already introduced a record thirty-five bills in 2021 focused on cryptocurrencies and blockchain.[112]

In addition to the FSOC, which is vigilant against systemic risk, several other existing laws, regulations, and regulatory bodies apply to cryptocurrency. The first and most significant application of current legislation to cryptocurrency is the Banking Secrecy Act (BSA), the principal federal anti-money laundering statute enforced by the Financial Crimes Enforcement Network (FinCEN).[113] In 2013, FinCEN released guidelines clarifying the BSA's application to the financial industry related to cryptocurrency.[114] The guidance clarified that a virtual currency *administrator* or *exchanger* is a Money Services Business (MSB) and, therefore, subject to registration, reporting, and

---

[108] *Id.*
[109] President's Working Group on Financial Markets, et al., *Report of STABLECOINS*, U.S. DEP'T OF TREAS. (Nov. 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.
[110] *See generally id.*
[111] *Id.* at 16.
[112] Jason Brett, *In 2021, Congress Has Introduced 35 Bills Focused on U.S. Crypto Policy,* FORBES (Dec. 27, 2021), https://www.forbes.com/sites/jasonbrett/2021/12/27/in-2021-congress-has-introduced-35-bills-focused-on-us-crypto-policy/?sh=47b77d2dc9e8.
[113] Office of the Comptroller of the Currency, *Bank Secrecy Act*, U.S. DEP'T OF TREAS., https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.
[114] U.S. DEP'T OF TREAS., FINANCIAL CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013).

recordkeeping regulations. The guidance further clarified that a *user* of cryptocurrency is not an MSB, and therefore not subject to the BSA.[115] This means that crypto exchanges must follow a comprehensive compliance program—including verifying customer identity—establishing due diligence systems and monitoring programs; screening against controlled government lists; monitoring and reporting suspicious activity; and creating risk-based anti-money laundering programs.[116]

In 2021, FinCEN proposed a new rule to expand the BSA to "unhosted wallets or wallets hosted in a jurisdiction identified by FinCEN," citing it was a "loophole-closing measure to prevent illicit transactions …. [that] would otherwise be subject to familiar and long-established reporting requirements if they were in cash."[117] If FinCEN chooses to finalize the rule, it will likely occur in February 2024.[118] The application of the BSA to crypto exchanges and potentially wallets is a regulatory measure meant to curb money laundering and illegal activities, such as terrorist financing, tax and sanction evasion, and drug and human trafficking. Although, many opponents of the expanded regulation cite the erosion of cryptocurrency's privacy—one of its hallmark features that attracted many cryptocurrency users. Balancing regulation against the benefits of cryptocurrency must be considered holistically so that regulation does not diminish crypto's positive attributes or hamper financial innovation generally.

As noted above, current regulatory efforts fall within the existing authority and the regulatory enforcement agencies. While a myriad of regulatory agencies and departments exist, the most prominent is the Securities and Exchange Commission. The SEC was established in 1934 by the Securities Exchange Act to aid in the restoration of investor confidence following the 1929 stock market crash.[119] Its mission was to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.[120] The SEC's jurisdiction extends to companies that offer securities for public sale, as well as those who sell

---

[115] *Id.*
[116] 31 U.S.C. §§ 5311-5330.
[117] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 7352 (proposed Jan. 28, 2021) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022).
[118] *View Rule*, EXEC. OFFICE OF THE PRESIDENT, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=1506-AB41 (last visited Apr. 18, 2023).
[119] *The Role of the SEC,* U.S. SEC. & EXCH. COMM'N, https://www.investor.gov/introduction-investing/investing-basics/role-sec (last visited June 2, 2022).
[120] *Id.*

and trade securities—such as brokers, dealers, and exchanges. The SEC has regulatory jurisdiction over some types of cryptocurrencies and related activities, but not over digital assets—which it differentiates as a commodity, not a security. The SEC regulates securities, which are defined as: "(1) an investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profit, (4) to be derived from the efforts of others."[121] Some cryptocurrency activities, such as many ICOs, fit this description, but Bitcoin does not, as a profit-seeking business does not issue it.[122]

Adding to the ambiguity of crypto regulatory jurisdiction, SEC Chair Gary Gensler said to the U.S. Congress House Appropriations Financial Services Subcommittee on May 18, 2022, that his agency has jurisdiction "over probably a vast number" of cryptocurrencies, but Bitcoin was "maybe" not under its purview.[123] These statements certainly did not give the impression of definitiveness or confidence. Around the same time as Gensler's testimony, SEC Commissioner Hester Peirce stated that the agency "dropped the regulatory ball" by not acting sooner and there would be "long-term consequences of that failure."[124] Both statements were made during a time of public scrutiny as crypto markets were melting down. Peirce went on to redirect the issue back to Congress, stating, "[i]t would be helpful if Congress came in and said, 'SEC, here's the role we think you should be playing. CFTC, here's the role for you."[125]

Commissioner Peirce was referring to the other federal securities regulatory body with jurisdiction over cryptocurrencies, the Commodity Futures Trading Commission. The CFTC was established in 1974 to regulate commodity futures and options markets, which historically included agricultural commodities but grew to include financial variables contracts, such as interest rates and stock indexes.[126] The CFTC was given exclusive jurisdiction over any contact "in the character of" future contacts, and its jurisdiction was later expanded to over-the-counter derivatives.[127] Its mission is to "*protect market users and the public from*

---

[121] Jay B. Sykes, *Securities Regulation and Initial Coin Offerings: A Legal* Primer, CONG. RSCH. SERV. 1, 5 (last updated Aug. 31, 2018).
[122] EVA SU, CONG. RSCH. SERV., R45221, CAPITAL MARKETS, SECURITIES OFFERINGS, AND RELATED POLICY ISSUES 37 (2018).
[123] MacKenzie Sigalos, *SEC's Hester Peirce Says the U.S. Has Dropped the Ball on Crypto Regulation*, CNBC (May 25, 2022), https://www.cnbc.com/2022/05/25/secs-hester-peirce-us-dropped-the-ball-on-crypto-regulation.html.
[124] *Id.*
[125] *Id.*
[126] RENA S. MILLER, CONG. RSCH. SERV., IF10117, INTRODUCTION TO FINANCIAL SERVICES: DERIVATIVES 1, (2019).
[127] MARC LABONTE, CONG. RSCH. SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 19 (2020).

fraud, manipulation, and abusive practices related to the sale of commodity futures, options and swaps, and to foster open, competitive, and financially sound commodity futures, options and swaps markets."[128] Even though many of the aforementioned federal government agencies play a significant role in cryptocurrency regulation, in 2014, the CFTC declared cryptocurrency a commodity subject to oversight under its authority.[129] It went on to take several regulatory actions, such as suing the unregistered bitcoin futures exchange BitFinex. [130] In May 2022, in response to various bills circulating in Congress related to the regulation of cryptocurrency, CFTC Chairman Rostin Behnam reiterated that his agency believes Bitcoin and ether are commodities.[131]

While officials are using existing authority to regulate cryptocurrency, and regulatory jurisdiction is evolving, the federal government is considering new laws and regulations to organize regulatory efforts better and more effectively achieve the regulation's goals. On March 9, 2022, President Joseph Biden signed an Executive Order (EO) to ensure the responsible development of digital assets, which was claimed to be the first whole-of-government strategy to protect consumers, financial stability, national security, and address climate change.[132] The EO called for measures to protect consumers, investors and businesses, protect financial stability and mitigate systemic risk, promote leadership in technology and economic competitiveness and reinforce leadership in the global financial system, promote equitable access to safe and affordable financial services, support technological advanced and ensure responsible development and use of digital assets and explore a CBDC.[133] Many critics of the EO describe it as lackluster as it does not prescribe any regulatory framework, issue any

---

[128] *Summary of CFTC Mission Statement, Strategic Goals & Outcomes*, COMMODITY FUTURES TRADING COMM'N https://www.cftc.gov/sites/default/files/reports/presbudget/2012/2012presidentsbudget0405.html (last visited Nov. 4, 2022).

[129] Timothy Massad, Testimony of CFTC Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition and Forestry (Dec. 10, 2014).

[130] In re BXFNA Inc., CFTC Docket. No. 16-19 (June 2, 2016),

[131] Kevin Helmes, *CFTC Chairman Confirms Bitcoin, Ether Are* Commodities, BITCOIN.COM (May 22, 2022), https://news.bitcoin.com/cftc-chairman-confirms-bitcoin-ether-are-commodities/.

[132] Exec. Order No. 14067, 87 Fed. Reg. 40881 (July 8, 2022); *see also Executive Order on Ensuring Responsible Development of Digital Assets*, THE WHITE HOUSE, (March 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[133] Exec. Order No. 14067, 87 Fed. Reg. 40881.

new rules or provide any further guidance.[134] The EO simply gives the various departments and agencies about 180 days to submit reports on the assigned topics.[135] Furthermore, some of the EO's requirements have already been addressed; for example, at the time of the EO's announcement, the Federal Reserve had recently published two reports on CBDC, which likely satisfy the EO's request.[136] As a result, the executive order was criticized by many as insufficient to address the regulatory challenges in the cryptocurrency space.

Regardless of the EO's issuance, new laws related to crypto should ultimately come from Congress. The 116th Congress (2019-2021) introduced thirty-five bills related to cryptocurrency, and the 117th Congress (2021-2023) introduced fifty bills covering the crypto regulatory landscape—a significant uptick from previous sessions. The bills are broken into six categories: taxation, CBDC, regulatory treatment, national security, and limitations on elected officials.[137] The most comprehensive bill introduced to date that would have provided regulatory guidance and clarity, H.R.6154 - Crypto-Currency Act of 2020, was never passed.[138] The bill provided clear and distinct classifications and definitions for digital assets, made the CFTC the primary regulator of crypto-currencies and the SEC the primary regulator of crypto-securities, and assigned the primary regulators various additional oversight responsibilities and required "those agencies to notify the public of any Federal licenses, certifications, or registrations required to create or trade in such assets, and for other purposes."[139] To date, the only federal legislation passed related to crypto-regulation was in the aforementioned IIJA, which merely expanded reporting requirements.

Lastly, because of the lack of federal action, many new laws and regulations are being enacted at the state level. There are about thirty-

---

[134] Sean Anderson, et al, *U.S. Crypto Regulation: Biden Signs Executive Order on Strategy to Regulate Crypto*, JDSUPRA (Mar. 16, 2022), https://www.jdsupra.com/legalnews/u-s-crypto-regulation-biden-signs-5184693/
[135] Exec. Order No. 14067, 87 Fed. Reg. 40881.
[136] Aaron Klein, *How Biden's Executive Order on Cryptocurrency May Impact the Fate of Digital Currency and Assets*, BROOKINGS (Mar. 17, 2022) https://www.brookings.edu/blog/techtank/2022/03/17/how-bidens-executive-order-on-cryptocurrency-may-impact-the-fate-of-digital-currency-and-assets/.
[137] Jason Brett, *Congress Has Introduced 50 Digital Asset Bills Impacting Regulation, Blockchain, and CBDC Policy*, FORBES (May 19, 2022), https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=708ddbcf4e3f.
[138] Crypto-Currency Act of 2020, H.R. 6154, 116th Cong. (2020).
[139] Scott H. Kimpel, *The Crypto-Currency Act of 2020*, HUNTON ANDREWS KURTH (Mar. 17, 2020), https://www.blockchainlegalresource.com/2020/03/the-crypto-currency-act-of-2020/; H.R. 6154.

three states with active legislation and seventeen states with enacted legislation as of 2021.[140] While the particulars of state legislation are beyond this paper's scope, it is noteworthy that New York and California have been the most active in implementing cryptocurrency regulation, primarily due to the number of cryptocurrency businesses in these states and the pro-regulation political environment.[141] Conversely, Arizona, Texas, and Wyoming have become the most progressive states. For example, Arizona considered a bill that would have established Bitcoin as legal tender;[142] likewise, Texas has taken legislative steps to make Bitcoin its legal tender.[143] Although, the constitutional legality of these initiatives is doubtful, and they may not survive a legal challenge.[144]

The most important aspect of these laws is allowing states to experiment. The U.S. federal system of government permits states to implement novel laws to determine their impact and effectiveness before scaling to other states or the federal government. Associate Supreme Court Justice Louis Brandeis was the first to popularize the phrase "states are laboratories of democracy."[145] In his dissenting opinion of *New State Ice Co v. Liebmann* in 1932, he stated: "a state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country." [146] Yet, while these state efforts may be a good stopgap and allow experimentation in an emerging market, harmonization of the laws and regulations at the federal level is desperately needed to coalesce the haphazard, fragmented, and patchwork evolution of regulation this path is producing.

---

[140] Heather Morton, *Cryptocurrency 2021 Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 16, 2021), https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx.

[141] Rakesh Sharma, *More US States May Roll Out Cryptocurrency Regulations*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/news/majority-us-states-are-still-acknowledge-cryptocurrencies/

[142] Ben Schreckinger, *A Crypto Breakthrough? Western States Consider Taking Digital Currency*, POLITICO (Feb. 1, 2021, 4:30 AM), https://www.politico.com/news/2022/01/31/crypto-wyoming-arizona-tax-payments-00003910.

[143] Rachel Wolfson, *More Than a Law: Texas Takes Steps to Amend Bitcoin into State Constitution*, COINTELEGRAPH (Sept. 10, 2021), https://cointelegraph.com/news/more-than-a-law-texas-takes-steps-to-amend-bitcoin-into-state-constitution.

[144] Schreckinger, *supra* note 142.

[145] Bradley A. Blakeman, *States Are the Laboratories of Democracy*, THE HILL (May 7, 2020), https://thehill.com/opinion/judiciary/496524-states-are-the-laboratories-of-democracy/.

[146] New State Ice Co. v. Liebmann, 285 U.S. 262, 387 (1932).

CONCLUSION

The United States has the most robust economy and greatest capital markets in the world. The free enterprise systems of capitalism and democracy have been forces for good, lifting people out of poverty, creating economic wealth, and promoting cultural freedom. But, then, why regulate? Because guardrails are needed to keep the system working optimally. Regulation has always been a means to provide a check and balance against the ever-lurking darkness of freedom and capitalism. It strives to protect consumer interests, promote market efficiency, and mitigate risk.[147] Nevertheless, the regulation's consumer protection and risk mitigation efforts must be designed and implemented with great finesse so as not to strangle the productivity and innovation created by the imaginative entrepreneurs that seek their efforts' social and economic rewards. This is the "art" of regulation.

However, this paper demonstrates that the U.S. is far from the subtle art of implementation; the crude foundation is still evolving. After nearly a decade and a half since the creation of the first cryptocurrency, crypto regulation in the United States is fragmented, with different measures taken at the federal and state levels, and even within and among agencies. For example, the SEC has indicated that initial coin offerings may qualify as "securities"; the CFTC categorized many cryptocurrencies as "commodities"; the IRS regards crypto as "property"; states oversee virtual currencies through state money transfer laws; and FinCEN treats crypto as a currency for anti-money-laundering purposes.[148] Despite all of this, the only thing that is certain, as recently put by SEC Chairman Gary Gensler: "there are no customer protections right now in the crypto market."[149]

This sluggish speed is not necessarily a surprise as government regulation has always chased rapid advancements in technology and associated consumer and market behavior changes.[150] And while the differences in pace are a product of their organizational design and culture, these differences produce a beneficial outcome—to a point. It is

---

[147] Phillipp Paech, "Introductory Slides Class 1 LLM407E" (lecture taught at the London School of Economics and Political Science in 2021) (on file with author).
[148] SU, *supra* note 122, at 41.
[149] Kevin Helms, *CFTC Chairman Confirms Bitcoin, Ether Are Commodities – Regulation Bitcoin News*, PUB. NEWS TIMES (May 22, 2022), https://publicnewstime.com/news/cftc-chairman-confirms-bitcoin-ether-are-commodities-regulation-bitcoin-news/.
[150] *Regulation and Legislation Lag Behind Constantly Evolving Technology*, BLOOMBERG L. (Sept. 27, 2019), https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology/.

impracticable to regulate every aspect of market development. The delay in regulatory action allows the marketplace to work out the "kinks" in the early days associated with new ideas, concepts, and business models. As new ideas develop, they will improve, comply with existing regulations, self-regulate, or fade altogether. Moreover, it allows the government to direct its limited resources to those regulatory issues that have the most significant potential impact on society and the economy. Nevertheless, we are now well beyond the "view from afar and wait-and-see" approach. Cryptocurrency has proliferated from niche to mainstream, and little has been done to regulate it.

As suggested above, the U.S. financial system has evolved mainly due to major historical financial crises, and the government lacks the imagination to foresee a crisis and the determination to take proactive measures. The financial regulatory system's evolution, rather than being purpose-built, leads to the hazards of path dependence. This is a precarious position for the U.S. and the world as the U.S. is a leader in the global financial community, the high concentration of crypto-based wealth, and economies' increasingly interconnected and interdependent nature. If the U.S. falls, the world follows.

While crypto regulation is multifaceted (e.g., consumer protection, reduction of illicit activities), I believe the risk of systemic failure is the most significant risk needing regulatory attention. The chances of the next financial crisis emerging from cryptocurrency or related fintech platformization have risen from low to moderate in recent years and are increasing each day significantly. About 7% of the world's money is in cryptocurrency,[151] and according to the CNBC Millionaire Survey, about half of millennial millionaires have at least 25% of their *wealth* in *cryptocurrencies*.[152] As cryptocurrencies gain greater adoption and acceptance, these numbers will rise, and as they grow, so will the risk of systemic financial system failure.

Moreover, because of the network effect's exponential growth and massive scale associated with crypto—such as gamification and platformization—the risk may grow exponentially rather than linearly. If the crypto market hits a certain tipping point, systemic failure may happen quickly with unimaginable ramifications and rippling effects through the traditional financial markets. With the last financial crisis,

---

[151] Nathan Reiff, *How Much of All Money Is in Bitcoin?*, INVESTOPEDIA (Nov. 26, 2021), https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/.

[152] Robert Frank, *Millennial Millionaires Have a Large Share of Their Wealth in Crypto, CNBC Survey Says*, CNBC: WEALTH (June 10, 2021, 10:23 AM), https://www.cnbc.com/2021/06/10/millennial-millionaires-have-large-share-of-wealth-in-crypto-cnbc-survey-.html.

regulators could not prevent a risk that built up under slower conditions with months of warning in traditional, regulated markets. So, they are certainly not prepared to prevent a rapid meltdown in the crypto markets.

The 118th Congress (2023-2025) should pass comprehensive and bipartisan cryptocurrency regulations to mitigate the risk of systemic failure. What is needed most is clarity on regulatory jurisdiction, harmonization among efforts at various levels of government, international harmonization and treaties, more enforcement resources, and consumer education and disclosure requirements. Furthermore, the government should deprioritize or eliminate the rosy exploration of a CBDC—it adds little benefit to the existing fiat digital currency for a country with a strong currency and financial system, such as the case in the U.S. It is also a distraction from much-needed prioritization of regulation and runs antithetical to the core concepts of crypto (e.g., decentralization).

Providing the proper cryptocurrency regulatory framework and tools will remain a significant challenge throughout the next decade. It is imperative because cryptocurrencies, and their tangencies, such as the crypto-ecosystem they live within, increasingly pose a systematic risk to U.S. and global financial markets. Nevertheless, any regulation should not be stronghanded and must be balanced not to smother emerging crypto markets and financial technology innovation. U.S. cryptocurrency regulation has been a slowly evolving state of affairs, and regulators must get to work on the art of their practice before it is too late.

VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

NFT ART HEISTS: ANALYZING NFTS UNDER U.S. LAW AND INTERNATIONAL CONVENTIONS ON ART THEFT

Kevin D. Brum

NFT ART HEISTS: ANALYZING NFTS UNDER U.S. LAW AND INTERNATIONAL CONVENTIONS ON ART THEFT

Kevin D. Brum[*]

INTRODUCTION

The non-fungible token ("NFT") is a type of digital asset with a unique identifier that is usually associated with an image. An NFT cannot be copied or reproduced, and records of NFT transactions are stored on the blockchain.[1] NFTs are a recent innovation and have swept the world by storm.[2] NFT sales tripled from 2019 to 2020 and DappRadar—the premier platform for hosting decentralized NFT portfolio management applications[3]—estimates that NFT sales hit twenty-five billion dollars in 2021.[4] Many NFTs appear to be artistic works and, either individually or in a collection, can be given away for free, sold for a few dollars, or sold for millions.

Not long after the NFT craze began, various individuals and organizations created NFTs to either gain internet popularity or to raise

---

[*] Candidate for Juris Doctor, Notre Dame Law School, 2023; Bachelor of the Arts in Political Science and History, University of California at Irvine, 2019. A heartfelt thank you to my colleagues on the *Journal of Emerging Technologies* for their diligent effort in editing and providing feedback on this piece. I would also like to express exceptional gratitude to my friends and family, especially my parents and grandparents, for their continued support, as well as Jerry Mowbray and the Mowbray & Hammes families. Special thanks as well to the Institute of Advanced Legal Studies at the University of London for providing me with access to their collection while I was studying abroad as part of the University of Notre Dame's London Law Program, without which, this note would not have been possible. A thank you as well to Professor Stephen Yelderman at Notre Dame Law School for suggesting this topic.

[1] Rakesh Sharma, *Non-Fungible Token (NFT): What It Means and How It Works*, INVESTOPEDIA (June 22, 2022), https://www.investopedia.com/non-fungible-tokens-nft-5115211.

[2] Sam Dean, *$69 Million for Digital Art? The NFT Craze Explained*, L.A. TIMES (Mar. 11, 2021, 10:34 AM), https://www.latimes.com/business/technology/story/2021-03-11/nft-explainer-crypto-trading-collectible.

[3] DAPPRADAR, *About Us,* https://dappradar.com/about-us (last visited Oct. 23, 2022).

[4] Elizabeth Howcroft, *NFT Sales Hit $25 Billion in 2021, but Growth Shows Signs of Slowing*, REUTERS (Jan. 11, 2022, 3:50 PM), https://www.reuters.com/markets/europe/nft-sales-hit-25-billion-2021-growth-shows-signs-slowing-2022-01-10/. Ryan Duffy, *The NFT Market Tripled Last Year, and It's Gaining Even More Momentum in 2021*, EMERGING TECH BREW (Feb. 22, 2021), https://www.morningbrew.com/emerging-tech/stories/2021/02/22/nft-market-tripled-last-year-gaining-even-momentum-2021.

money.[5] The success of NFTs also drew the attention of some unscrupulous individuals and scammers—such as the adult actress Lana Rhoades who made headlines after raising $1.5 million in Ethereum for a series of planned NFTs and subsequently disappearing from the project,[6] in what has been termed a "rug pull" scam.[7] While federal authorities have begun cracking down on these kinds of activities,[8] there has also been a rise in NFT "heists."[9] In one case, thieves used social engineering to attain users' login credentials on OpenSea—a popular NFT trading platform—and stole NFTs collectively worth over $1.7 million.[10]

Given NFTs have visual representations, these high-profile thefts have left many wondering how, if at all, American art theft law applies to the theft of NFTs. In addition, due to the international nature of the internet, some have wondered whether international law governing stolen and illegally exported artwork could apply to NFT theft. These legal questions are the subject of this note.

Part I will cover the unique properties of NFTs and how they interact with modern notions of property law and severability. Part II will discuss art theft, NFT theft, different legal regimes governing restitution

---

[5] These ranged from video game companies like Electronic Arts and Ubisoft to the National Basketball Association (NBA). Andrew King, *Where Game Companies Stand on NFTs*, GAMESPOT (Feb. 4, 2022, 8:47 AM), https://www.gamespot.com/articles/where-game-companies-stand-on-nfts/1100-6500331/.
Jeff John Roberts, *Want to Own Kawhi's Jump Shot? NBA and CryptoKitties Maker Launch Digital Collectibles*, FORTUNE (July 31, 2019, 2:00 PM), https://fortune.com/2019/07/31/nba-top-shots-blockchain-collectibles/.

[6] Jeffery Gogo, *Porn Star Lana Rhoades Makes Off with $1.5M in Apparent NFT Scam*, BEINCRYPTO (Feb. 24, 2022, 5:30 PM), https://beincrypto.com/porn-star-lana-rhoades-makes-off-with-1-5m-in-apparent-nft-scam/. After disappearing from the internet for several weeks, Rhoades made her return to the NFT project a mere 12 hours after the FBI made headlines by arresting two other NFT rug pullers. @l337m45732, *Lana Rhoades' NFT Scam is Back from the Dead*, LEOFINANCE https://leofinance.io/@l337m45732/lana-rhoades-nft-scam-is-back-from-the-dead (last visited Oct. 27, 2022).

[7] Amiah Taylor, *Watch Out for the 'Rug Pull' Crypto Scam That's Tricking Investors Out of Millions*, FORTUNE (Mar. 3, 2022, 12:36 AM), https://fortune.com/2022/03/02/crypto-scam-rug-pull-what-is-it/. ("Rug pulls are a lucrative scam in which a crypto developer promotes a new project—usually a new token—to investors, and then disappears with tens of millions or even hundreds of millions of dollars. This particular type of fraud accounted for $2.8 billion in lost money for victims, or 37% of all cryptocurrency scam revenue in 2021.").

[8] Adi Robertson, *Two Men Arrested for $1.1 Million NFT 'Rug Pull' Scam*, VERGE (Mar. 24, 2022), https://www.theverge.com/2022/3/24/22995107/us-arrest-charges-crypto-nft-rug-pull-frosties-ethan-nguyen-andre-llacuna.

[9] *Infra* note 10.

[10] Russell Brandom, *$1.7 Million in NFTs Stolen in Apparent Phishing Attack on OpenSea Users*, VERGE (Feb. 20, 2022, 9:37 AM), https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft.

of stolen property, including the patchwork of international and domestic laws governing the theft of art. Part III will examine the different categories of art classification in U.S. and International Law. Part IV will analyze how NFTs might fit within different legal definitions of art. Lastly, Part V will theorize how NFTs interact with laws governing theft and restitution.

I. BACKGROUND

A. The Non-Fungible Token

NFT stands for "non-fungible token," and, as the name suggests, an NFT is a digital asset (a "token") with unique information (metadata) that is incapable of being copied on the same blockchain.[11] The blockchain is a decentralized network that uses the power of multiple connected computers to track and verify transactions. There are different blockchains for different cryptocurrencies, but most NFTs are tracked using the Ethereum cryptocurrency blockchain.[12] NFTs can be represented by anything: a tweet, an animated GIF, a comic book, etc.[13] While the token can be represented by anything, sometimes purchasing an NFT conveys *no* rights to the visual depiction associated with it.

NFTs can be best analogized to trading cards. For example: a Michael Jordan basketball card bears both Jordan's picture and a unique serial number. Two Michael Jordan basketball cards look identical but have different serial numbers. While a Michael Jordan *baseball* card might have an identical serial number to Jordan's *basketball* card, they are distinct because they are from different sports. Applying NFTs to this analogy: the physical card is the token, the picture is the token's visual representation (hereinafter "visrep"), and each sport is a blockchain. The owner of the card has a right to the card itself: they are free to sell, trade, give away, destroy, or display the card. However, purchasing a Michael

---

[11] Dean, *supra* note 2. Identical NFTs can be "minted" on more than one blockchain. Multiple NFTs can be minted that, while unique, can use the same visual representation.

[12] Mitchell Clark, *NFTs, Explained*, VERGE (June 6, 2022, 8:30 AM), https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq.

[13] Taylor Locke, *Jack Dorsey Sells His First Tweet Ever as an NFT for over $2.9 Million*, CNBC (Mar. 24, 2021, 2:10 PM), https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html. Grace Kay, *'Nyan Cat' flying Pop-Tart Meme Sells for Nearly $600,000 as One-of-a-Kind Crypto Art*, BUS. INSIDER (Feb. 23, 2021, 1:51 PM), https://www.businessinsider.com/ethereum-nft-meme-art-nyan-cat-sells-for-300-eth-2021-2?r=US&IR=T. Emily Zogbi, *Xenoglyphs to Become the First NFT Collectible Comic*, CBR (Mar. 20, 2021), https://www.cbr.com/xenoglyphs-nft-comic/.

Jordan trading card conveys no right to the picture of Michael Jordan. The card's owner cannot license or reproduce the image.

A key difference between trading cards and NFTs lies in their respective fungibility. Fungibility is the idea that a particular object is interchangeable with another, similar object. For example, two identical trading cards in identical condition are interchangeable and, therefore, fungible, even if they have a unique serial number. This is not true for NFTs. An NFT may be *perceived* as more or less valuable based on its visrep. However—unlike a trading card—a token's uniqueness doesn't come from its appearance, but from its metadata. Even two, apparently identical NFTs are not interchangeable, thus, they are non-fungible. Because NFTs are non-fungible, each NFT is individually subject to market forces of supply and demand.[14] As the token itself is as unattractive as the serial number on a blank trading card, market forces usually respond to perceived value around the visrep and the NFT's creator. NBA "Top Shot Moments" offer a concrete example for some of these abstract ideas.

The National Basketball Association (NBA) has the right to broadcast and record NBA basketball games. After the NFT boom began, the NBA took clips of the "game[s'] epic highlights from the most incredible basketball stars," and called them "NBA Top Shot Moments," or "Moments" for short.[15] NBA Top Shot minted NFTs with these short video clips and included information about the player making the "top shot," and the game associated with it. Essentially, Moments are digital trading cards which have a video as their visrep instead of a still image.[16] The NBA Top Shot Terms of Use describe the value attached to these Moments as follows:

> The value of each Moment is inherently subjective, in the same way the value of other collectibles is inherently subjective. Moments have no inherent or intrinsic value. Some collectors might prefer to have a Moment featuring a certain NBA player, while another might prefer an equivalent Moment featuring a different NBA player. Each NBA player can have more than one Moment associated

[14] As some NFTs are part of collections from the same creator, perceived value of the collection and the creator can inflate or deflate the market value of an NFT.

[15] *What Are Moment™ NFTs?*, NBA TOP SHOT, https://support.nbatopshot.com/hc/en-us/articles/4404116274451-What-are-Moment-NFTs-. (last visited Jan. 7, 2023).

[16] This is an analogy that NBA Top Shot seems to embrace as they use card packs and other terms and imagery that are generally associated with the trading card world. *See id.*

> with them, and those Moments will each have different characteristics.[17]

Buying an NBA "Top Shot Moment" NFT does not confer unfettered rights to the "Top Shot Moment" upon the buyer.[18] While the owner can "swap [the] Moment, sell it, burn it, exchange it, upgrade it or give it away to the extent that such uses are made available in the [application]"[19] NBA Top Shot retains all the hallmarks of property ownership.[20] A Moment owner cannot license, modify, commercialize, or use the Moment in any form except for one's sole personal non-commercial use.[21]

While it may initially seem odd that one could or would want to own an object without being able to exploit it, this is common in trading cards and in the art world at large. There are entire markets and industries centered solely on usage rights.[22] This is particularly true in the digital world. Traditionally, digital art was seen as inherently fungible because it can be copied flawlessly with a few clicks. Thus, much of the law surrounding digital artwork relates to intellectual property. The non-fungibility of NFTs complicates things because they challenge the traditional view that all digital assets are inherently fungible.

Given the unique nature of NFTs and the law surrounding them, it is tempting to view the token as separate from its visrep. Legally, this would offer a simple solution to questions of whether NFTs are art and whether art theft law could apply to NFTs; that answer would be "no" to both. As a token is no more artistic than a serial number, the token is highly unlikely to be considered art. Not only would that answer end the discussion of this topic here, but such an answer also misunderstands how a token and its visrep are inseparably tied.[23] Much like a trading card, it would be effectively impossible to remove the image of Michael Jordan off the trading card without damaging the card. Likewise, in the realm of the internet, the only way to separate a visrep from an NFT is to

---

[17] *Terms of Use: Sec. 2(iii)*, NBA TOP SHOT, Sec. 2(iii) (Aug. 31, 2022), https://nbatopshot.com/terms ("Subjectivity of Moments").
[18] *See id.* at Sec. 4(iv), 4(vi) ("Restrictions on Ownership").
[19] *Id.* at Sec. 4(i) ("Ownership of the Moment").
[20] They retain the right to use the moment continually. *See id.* at Sec. 4. ("Ownership, License, and Ownership Restrictions").
[21] *Id.*
[22] Prime examples of these kinds of markets include photographs, digital artwork, and fonts—all of which can, and many do, distinguish between personal and commercial use.
[23] *Can You Edit an NFT After It Has Been Minted?*, ASSETMANTLE (May 9, 2022), https://blog.assetmantle.one/2022/05/09/can-you-edit-an-nft-after-it-has-been-minted/.

"burn" the NFT—in other words, destroy it entirely.[24] While a buyer's rights to a token's visrep might change depending on the transaction, a token and its visrep are as inseparable as a U.S. quarter is from George Washington's portrait—the only way to separate the two is to melt the quarter. Therefore, this note will proceed on the theoretical understanding that a token and its visrep, while different, are inseparable components of a single object.

B. Severability & the Blackstone-Hohfeld Spectrum of Property

When conceptualizing property, two major frameworks come to the forefront: Blackstone's and Hohfeld & Honoré's. Blackstone believed that property entailed the right to exclusive use, whereas Hohfeld & Honoré argued that property could be conceived of as a "bundle" of rights that can be modified to fit one's needs. Hohfeld and Honoré won the debate in modern property law, and, as a result, bundle theory has prevailed. Consequentially, art law is intertwined with Hohfeld and Honoré's Bundle Theory.

In the art context, the most common severable rights are title, possession, and exploitation.[25] Often, a private individual will agree to have artwork from their collection exhibited at a museum. They may also choose to grant the museum exclusive rights to take photographs and to produce merchandise based on the exhibited piece. The owner is vested with title, while the museum is vested with possession and exploitation, albeit temporarily. In legal disputes between titleholders and possessors, titleholders come out victorious as they are often considered the original owners.[26] Though it is important to note that the unique nature of art law has also led to the creation of other rights that do not exist for other personal property, including the "right to display."[27]

Using basic ideas surrounding property rights, one can conceive of NFTs on a spectrum (hereinafter "Blackstone-Hohfeld Spectrum"). On the "Blackstonian" side of the Spectrum, an NFT can convey full title and

---

[24] *Id.* Obviously, it is possible to screenshot or record a token's visrep without destroying the NFT. However this is duplication of the visrep, rather than removal of the visrep from the token.

[25] Title can best be described as ownership. Possession is self-explanatory. Exploitation encapsulates *inter alia* use, derivative use, and intellectual property rights.

[26] *Clarke, Hunt Cook and Newsquare v. The Association for the Creation of the Vincent Van Gogh Foundation – Arles* (2010). NORMAN PALMER, ART, ADVENTURE AND ADVOCACY 77 (2015) (A painting by Francis Bacon was loaned to the Van Gogh Foundation, when the owner attempted to secure the return of the painting, the Foundation attempted to block the return on the basis that, *inter alia*, it had the right to display the painting. This argument failed to persuade the French court.).

[27] PALMER, *supra* note 26, at 77.

exclusive use to the token's visrep (hereinafter "Blackstone NFTs").[28] On the "Hohfeldian" side of the Spectrum, an NFT conveys almost no rights to the token's visrep (hereinafter "Hohfeld NFTs").[29] Most NFTs exist somewhere in the middle of the Spectrum. NFTs on either side of the Spectrum pose theoretical difficulties in interacting with art and property law and the internet.[30]

A Blackstone NFT purchase is a straightforward transaction: the buyer receives the NFT and exclusive rights to its visrep. Yet, Blackstone NFTs buck our notions of digital ownership. Due to the nature of the internet, while a token cannot be copied, its visrep can. Enforcing copyright over any visual medium on the internet poses feasibility challenges. While Blackstone NFTs convey exclusive use, there is nothing stopping another NFT creator from copying or screenshotting a Blackstone NFT's visrep and creating a new NFT with that same visrep. There's no clear answer on what recourse, if any, a copyright holder has when an NFT creator makes and sells a new NFT using a copyrighted visrep. Even if they pose enforcement challenges, Blackstone NFTs are easier to conceive of than Hohfeld NFTs because they grant full ownership of the token with exclusive rights to its visrep.

Unfortunately, Hohfeld NFTs are more difficult to grasp, because they lack one of the primary hallmarks of property ownership: exclusive use, and thus, the right to exploit. Consider the following hypothetical: in a bid to raise funds for the national parks, the federal government auctioned off illusory "deeds" to the national parks. The "deedholders" are allowed to display or transfer the "deed" but they do not receive any special privileges or additional rights to the national park. While the "deedholder" technically now "owns" the national park, they are prevented from exercising any authority over the land. Many would question what, if any, value is to be gained by owning land that one cannot exploit. However, if the government actually auctioned off illusory "deeds" to famous national parks—such as Yellowstone, Yosemite, or Joshua Tree—it is easy to believe that some people would buy them, purely to say that they "own" a national park. In this analogy, the "deed" is the Hohfeld token, the national park is the visrep, and the federal government is the creator of the NFT.

---

[28] Named after Sir William Blackstone and his formulation of property rights: the right to exclusive use.

[29] Named after Wesley Hohfeld and A.M. Honoré for their formulation of property rights: a bundle of rights.

[30] How copyright works with non-fungibility and digital ownership is a worthy topic of study, but beyond the scope of this note.

For some individuals, the allure of owning something—a star,[31] an acre on the moon,[32] a lordship[33]—even without the ability to use it, is a novelty worth paying for. Clearly, there is some idiosyncratic value that certain individuals place on these certificates of ownership alone. When thinking of Hohfeld NFTs in this frame of mind, purchasing one seems more reasonable. One could imagine a future where NFTs may be displayed in someone's online, virtual reality gallery that others can enter and appreciate. In such a future, the limited "right to display" an NFT's visrep—especially one worth millions of dollars—is a status symbol; not too different from some art today, particularly modern art,[34] regardless of whether someone can screenshot or otherwise copy the visrep.

To summarize, on one side of the Blackstone-Hohfeld Spectrum, Blackstone NFTs convey all three property rights (title, possession, and exploitation) to the token's visrep,[35] while on the other side of the Spectrum, Hohfeld NFTs leave out all but the "right to display" the token's visrep.[36] Regardless of which end of the spectrum an NFT is at, the purchase of an NFT always grants the buyer full rights to the *token*.

II. THEFT

Though art theft has advanced and adapted to the modern era, art theft is nothing new; it stretches back into antiquity.[37] High-profile heists

---

[31] *Buy a Star in the Sky*, COSMONOVA, https://cosmonova.org/ (last visited Oct. 23, 2022).

[32] *Buy Land on the Moon*, LUNAREMBASSY, https://lunarembassy.com/product/buy-land-on-the-moon/ (last visited Oct. 23, 2022).

[33] *Become a Lord, Lady, Baron, or Baroness*, SEALAND, https://sealandgov.org/shop/become-a-lord-lady-baron-or-baroness/ (last visited Oct. 23, 2022).

[34] Modern art is a particularly apt comparison as certain people crave uniqueness compared to effectively fungible "ordinary" luxury goods (such as sports cars, mansions, etc.). Lorenzo Pereira, *New Status Symbols: Big Art*, WIDEWALLS (Apr. 28, 2015), https://www.widewalls.ch/magazine/new-status-symbols-big-art ("[B]illionaires are looking for possessing something unique, something that will be a topic of gossips or discussions. They want unique, expensive things that no one else could have - not because of its price, but because of its uniqueness.").

[35] While an NFT cannot be replicated, in the sense that no two NFTs are perfectly identical given the Blockchain, this paper presumes that the owner of a Blackstone NFT can create subsequent NFTs using the same image. Ultimately this is a creature of copyright, which is beyond the scope of this note.

[36] Exploring what it means to "possess" something digitally is difficult when the object one "possesses" can be replicated by a third party with even temporary access to the data. One could conceive of this as having a right of "non-exclusive" possession; meaning one is in a *group* of individuals allowed to possess an image.

[37] Annabelle Steffes-Halmer, *Looted Art, from Antiquity to Present-Day*, DEUTSCHE WELLE (May 21, 2021), https://p.dw.com/p/3tiWa; *See also* Petrus C. van Duyne, Lena Louwe, and Melvin Soudijn, *Money, Art, and Laundering: Coming to Grips with the Risks, in* CULTURAL PROPERTY CRIME: AN ANALYSIS OF CONTEMPORARY PERSPECTIVES AND TRENDS 79 (Joris D. Kila & Marc Balcells eds. 2014) ("[S]ince time

have captured the attention of authorities and the public, such as the infamous Isabella Stewart Gardner Museum theft in 1990, where thirteen pieces, including Rembrandt's famous *The Storm on the Sea of Galilee*, were stolen.[38] What often goes unnoticed is the approximately 52 percent of art thefts from private homes,[39] perhaps most analogous to the theft of NFTs from personal digital wallets.

When thieves steal an art piece or object of cultural heritage,[40] they face a serious problem: converting it to money. Thieves may be in possession of artwork worth millions of dollars, but finding a buyer and selling it without getting caught[41] (or ransoming the piece back to the original owners—often dubbed "artnapping"), is arguably as difficult as the heist itself.[42]

There is little controversy at law when a thief takes possession of an object they do not have title to and ransoms it back to the original owner. Problems arise when the thief succeeds in offloading the artwork to another individual (bona fide buyer), especially when the transactions occur internationally.

A. NFT Theft

One might think it's easy to track down an NFT thief due to the nature of blockchain technology. However, the reality is that, while the Ethereum Blockchain is publicly available to browse, it is not as easy to analyze. Even when one is just looking to track down a specific transaction from one wallet to another, browsing the transaction history of a singular wallet can be difficult. If the stolen NFT is worth millions of

---

immemorial, objects of art have been stolen by individuals as well as by states.") (citing CHARNEY ET AL., THE JOURNAL OF ART CRIME: SPRING (2009)).

[38] *The Theft*, ISABELLA STEWART GARDNER MUSEUM, https://www.gardnermuseum.org/about/theft-story (last visited Apr. 4, 2022). The FBI ranks the Isabella Steward Gardner Museum theft second in a list of top ten art crimes. *Art Crime*, FBI, https://www.fbi.gov/investigate/violent-crime/art-theft (last visited Nov. 3, 2022).

[39] *Theft and Forgery in the World of Art*, PRINTERINKS https://www.printerinks.com/theft-and-forgery-in-the-world-of-art.html (last visited Apr. 4, 2022).

[40] There are different laws governing objects of cultural heritage that, if discussed would go beyond the scope of this paper, thus, going forward, this paper shall focus solely on art.

[41] Duncan Chappell & Kenneth Polk, *The Peculiar Problem of Art Theft*, *in* CONTEMPORARY PERSPECTIVES ON THE DETECTION, INVESTIGATION AND PROSECUTION OF ART CRIME 38, 40-43 (Duncan Chappell & Saskia Hufnagel, eds., 2014) [hereinafter Chappell & Polk: The Peculiar Problem].

[42] Henri Neuendorf, *Mysterious Thief Surfaces and Demands Ransom for Klimt Painting Stolen in 1997*, ARTNET NEWS (Nov. 5, 2015) https://news.artnet.com/art-world/ransom-stolen-klimt-painting-356045.

dollars, an owner probably wouldn't hesitate to put in the effort and resources to track it down.

To combat the blockchain's ability to track them down, thieves have adapted. Some NFT and crypto thieves use services designed to effectively anonymize transactions. These criminals currently use two popular methods to throw off authorities. One method, called "mixing," works by creating a whirlwind of transactions between a source wallet and destination wallet.[43] By "mixing," there are so many transactions between wallets in randomized sequences and at random times that the stolen assets become incredibly difficult, if not impossible, to track down. The most infamous service that does this is Samourai's Whirlpool.[44]

Another service thieves have used is Tornado Cash.[45] Tornado Cash is an online service that launders cryptocurrency.[46] In fact, Tornado Cash was recently used to try and launder approximately $600 million in cryptocurrency related to NFT gaming.[47] Tornado Cash works similar to how early banks operated;[48] users "deposit" an amount into the service and receive a receipt with a unique key.[49] The user wait as long as they like and then, when they are ready to receive the funds in a clean wallet, the user enters the unique key and the funds are transferred, minus a fee.[50]

As the tainted wallet and clean wallet never come into direct contact with each other, the transactions cannot be effectively traced. Thus, the only real way to trace the transaction is by looking at the amount of crypto transferred to find patterns and similarities linking the funds to a recent theft. Yet, a Tornado Cash user can split the crypto into multiple transactions, mitigating the effectiveness of some of these methods. Tornado Cash's process has the effect of "washing" the crypto. While this may seem less applicable to NFT theft because Tornado Cash

---

[43] JP Buntix, *3 Reasons to Pay Attention to Samourai Wallet's Whirlpool for Bitcoin Privacy*, CRYPTOMODE (June 28, 2021), https://cryptomode.com/3-reasons-to-pay-attention-to-samourai-wallets-whirlpool-for-bitcoin-privacy/.

[44] *Id.*

[45] *See, e.g.*, Robertson, *supra* note 8.

[46] *Id.*

[47] David Gealogo, *How over $600+ Million Worth of NFT Got Stolen in Axie Infinity Hack*, CRYPTO GAMING (Mar. 31, 2022), https://www.esports.net/news/axie-infinity-hacked-over-600-million-worth-of-nft-stolen/.

[48] Both the Knights Templar and the Tang Dynasty used similar methods that would allow people to deposit money in one place, carry a letter of credit or key with them, and withdraw it in another place or at another time. Tim Harford, *The Warrior Monks Who Invented Banking*, BBC NEWS (Jan. 30, 2017), https://www.bbc.co.uk/news/business-38499883.

[49] *How Tornado Cash Works,* TORNADO CASH, https://tornado.cash/ (last visited May 2, 2022).

[50] *Id.*

relies on the fungibility of cryptocurrencies,[51] it is easy to envision criminals using both services in conjunction. While Tornado Cash has been made unavailable in the United States, it is still available in other countries, and therefore, until the service is permanently discontinued, it remains an asset for criminals.[52]

B. Nemo Dat Versus Good Faith Buyer

Theft has existed in every culture since time immemorial. It is unsurprising that different legal systems came to different conclusions on who should hold title when a thief succeeds in selling stolen property to a bona fide buyer who was unaware of the theft. Though rules vary from state to state, in Western European jurisprudence, two different systems emerged to settle these disputes—largely based on whether a country followed the civil or common law. Civil law countries favor the circulation of property and thus, over time, have adopted a regime that provides greater protection to bona fide buyers.[53] In these jurisdictions, original owners have no legal right to the return of their stolen property if a bona fide buyer purchased the stolen property in good faith and exercised due diligence to ensure that it was not stolen (hereinafter "Good Faith Buyer Rule/Jurisdiction"). In contrast, common law countries such as the United States and the U.K., adhere to the rule of *nemo dat quod habet* (hereinafter "*Nemo Dat* Rule/Jurisdiction"). Translated from Latin, *nemo dat quod habet* literally means "no one

---

[51] If a unique token can be tracked between wallets, it effectively would provide the same service as Samourai's Whirlpool, thus defeating the extra layer of anonymity.

[52] In August of 2022, the U.S. Treasury Department Office of Foreign Asset Control officially sanctioned Tornado Cash. Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), U.S. DEPT. OF TREASURY, U.S. TREASURY SANCTIONS NOTORIOUS VIRTUAL CURRENCY MIXER TORNADO CASH, (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916. The Office of Foreign Asset Control referenced a $60 million civil penalty issued in 2020 by the Financial Crimes Enforcement Network for similar misconduct. *Id.* FINANCIAL CRIMES ENFORCEMENT NETWORK, U.S. DEP'T. OF TREASURY, NUMBER 2020-2, ASSESSMENT OF CIVIL PENALTY IN THE MATTER OF LARRY DEAN HARMON (2020), https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf (assessment of civil penalty). In an announcement on its website, the Treasury Department stated that Tornado Cash had been used to launder approximately $7 billion in virtual currency since its founding in 2019, including laundering $455 million stolen by North Korea's state-sponsored hacking group, known as the Lazarus Group. U.S. DEP'T. OF TREASURY, *supra* note 52 (press release).

[53] *See, e.g.*, Guido Carducci, *The Growing Complexity of International Art Law: Conflict of Laws, Uniform Law, Mandatory Rules, UNSC Resolutions and EU Regulations*, *in* ART AND CULTURAL HERITAGE: LAW, POLICY, AND PRACTICE, 68, 90 (Barbara T. Hoffman ed., 2006).

gives what he does not have."[54] Under the *Nemo Dat* Rule, because a thief cannot take title to an object from its original owner, the thief is incapable of transferring title to a bona fide buyer, regardless of the circumstances.[55]

To illustrate the differences between these systems, consider the following hypothetical: a burglar steals a ring from someone's home in the middle of the night. After making his getaway, the thief trips and injures his ankle. In the morning, the thief puts on an ankle brace and goes to a pawn shop to sell the ring. The merchant asks how the thief came by the ring and asks why he wants to sell it. The thief claims the ring belonged to his late grandfather and, while it holds great sentimental value, he needs to sell it to pay for his medical expenses. The merchant notices the thief's injured ankle and does not see anything inherently suspicious about him. The ring is a plain gold wedding band with no uniquely identifiable features, making it virtually impossible to run the ring through a stolen property registry. Ultimately, the merchant purchases the ring. The next day, the original owner of the ring arrives at the pawn shop and presents conclusive evidence showing that he is the owner and provides incontrovertible proof that the ring was stolen.

If the events described above occurred in France (a Good Faith Buyer Jurisdiction) the merchant purchased the ring in good faith and did their due diligence, therefore, the merchant legally owns the ring and the original owner has no right to its return. Neither does the original owner have a right to be compensated by the merchant; this is because it was the thief, not the merchant, who wronged the original owner.

However, if these events occurred in the U.K. (a *Nemo Dat* Jurisdiction), the circumstances of the sale—the merchant's good faith and due diligence—are irrelevant. The thief possessed the ring, but he never owned it and thus, he was legally incapable of transferring ownership to someone else. Consequently, the original owner has legal ownership and the ring must be returned. The merchant has no right to be compensated by the ring's owner because it was the thief, not the ring's owner, who wronged the merchant.

As one can infer from the issues presented by the hypothetical, in Good Faith Buyer Jurisdictions litigation over stolen objects revolves around the bona fide buyer's due diligence and good faith or lack thereof. However, who bears the burden of proving or refuting good faith and due

---

[54] *Legal Maxims*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("*Nemo dat quod habet*. No one gives what he does not have; no one transfers (a right) that he does not possess. According to this maxim, no one gives a better title to property than he himself possesses. A variation of this maxim is *Nemo dat qui non habet* (no one gives who does not have).").

[55] *See, e.g.*, Carducci, *supra* note 53, at 76.

diligence varies depending on the state.[56] In *Nemo Dat* Jurisdictions, transferring title to a stolen object is a legal impossibility; thus, litigation hinges on whether the object was stolen or not. If the object was stolen, the bona fide buyer is strictly liable.

While strict liability is the general rule in *Nemo Dat* Jurisdictions, there are some affirmative defenses that a bona fide buyer can raise to acquire title to stolen property: the statute of repose,[57] if one exists and has tolled,[58] or the equitable doctrine of laches.[59] However, for a bona fide buyer to assert either of these defenses not only must they show that laches or the statute of repose applies, additionally, the bona fide buyer must also prove that they purchased the stolen object in good faith *and* exercised due diligence to determine that the object was not stolen.[60] While this may sound similar to the Good Faith Buyer Rule, the burden of proof is inverted. In Good Faith Buyer Jurisdictions the original owner bears the burden of proving that the bona fide buyer did *not* purchase in good faith or did *not* exercise due diligence. When asserting an affirmative defense in a *Nemo Dat* Jurisdiction, the bona fide buyer bears the burden of proving that the affirmative defense applies, that they exercised due diligence, *and* that they purchased in good faith.[61]

While one would hope, due to its cultural value, that art would be treated differently from other forms of personal property, prior to the nineteenth and twentieth centuries, most countries did not consider art to be legally unique. Therefore, rules governing the transfer and return

---

[56] PALMER, *supra* note 26, at 11.

[57] Kenneth Polk & Duncan Chappell, *Art Theft and Time Limits for Recovery: Do the Facts of the Crime Fit the Limits of the Law?*, *in* CULTURAL PROPERTY CRIME: AN OVERVIEW OF ANALYSIS OF CONTEMPORARY PERSPECTIVES AND TRENDS 3 (Joris D. Kila, Marc Balcells eds. 2014) (The doctrine of *nemo dat* has been around since 1623 and still applies in art law.) [hereinafter Polk & Chappell: Art Theft].
(The statute of repose in the United States is generally six years, however, when the statute of repose tolls varies by state.).

[58] "[T]he states (especially New York and California ["where most of the actions regarding art recover in the United States are lodged"] have '. . . developed limitation of action principles which strongly favor original owners and property rights.' In these two states in particular . . .. the legal statutes provide that the time limitation clock does not start to run until the 'dispossessed owner' either comes into possession of knowledge about the whereabouts of the previously stolen object (as in California) or takes some action regarding these objects (as in New York)." *Id.* at 11.

[59] Barbara T. Hoffman, *International Art Transactions and the Resolution of Art and Cultural Property Disputes: A United States Perspective*, *in* ART AND CULTURAL HERITAGE: LAW, POLICY, AND PRACTICE (Saskia Hufnagel, Duncan Chappell eds., 2014) 169, 172. (The doctrine of laches holds that, even in cases of international art theft, if an entity did not exercise due diligence to try and return the items, they may forfeit title). Greek Orthodox Patriarchate of Jerusalem v. Christie's Inc., No. 98 Civ. 7664 (S.D.N.Y. 1999) (granting summary judgement to Christie's because the Patriarchate did not take action soon enough, the fact that they were a monastery with infrequent access to the internet was irrelevant).

[60] Polk & Chappell: Art Theft, *supra* note 57, at 10.

[61] *Id.*

of stolen objects also applied to art.[62] There has been movement in the last two centuries to provide exceptions to traditional property law for art, however many states continue to rely upon these foundational concepts of property ownership when issues of stolen art arise. As the world has become more interconnected, and recognition of art's unique value has increased, there have been several attempts to create a specialized framework for the transfer of stolen art on the national and international level with limited success.

C. The UNESCO & UNIDROIT Conventions

The United Nations Educational, Scientific and Cultural Organization ("UNESCO") recognized the need for a unified standard to deal with the international transport of stolen art and artifacts. Thus, in 1970, UNESCO published the UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (hereinafter "UNESCO Convention").[63] The bulk of the UNESCO Convention concerns state requests for the return of cultural heritage items, particularly art of prominence.

The Convention laid out three variations on the illegitimate movement of art: illegal export (smuggling "national treasure[s]" out of the country of origin); illicit excavation (removing objects from places that a country regards as national property—such as tombs or other archaeological sites);[64] and "simple theft,"[65] (the kind of art thievery behind the disappearance of *The Storm on the Sea of Galilee*). The UNESCO Convention provided no distinction between illegal export, illicit excavation and simple theft; rather, the Convention used the umbrella term "illicit" to cover all three practices. As the topic of this note surrounds digital artwork, discussion of international law shall be confined to discussing the illegal export/import and "simple theft" of artwork.

The importance of the UNESCO Convention in prompting special legal designations for art cannot be overstated. As mentioned earlier, many countries did not exempt artwork from their legal regimes governing the transfer of stolen property. While the UNESCO

---

[62] Polk & Chappell: Art Theft, *supra* note 57, at 3.
[63] UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, Nov. 14, 1970, 823 U.N.T.S 231 [hereinafter UNESCO Convention].
[64] Several countries, Mexico being a prime example, consider all tombs and pre-Columbian artifacts as belonging to the state, thus even undiscovered works are considered state property and removing them from the country is considered theft. *See, e.g.*, United States v. McClain, 551 F.2d 52 (5th Cir. 1977); United States v. Hollinshead, 495 F.2d 1154 (9th Cir. 1974).
[65]Hoffman, *supra* note 59, at 90.

Convention has gained widespread acceptance,[66] the Convention also had some major issues. For one, it recognized art traffic as illicit *only* if the trafficked artwork had been officially designated by a signatory state as "cultural property" *and* if the art fit within certain categories—albeit, quite broad and extensive categories.[67]

The United States and the United Kingdom, unlike some other large western countries, do not have a system of artwork classification, meaning any artwork illegally exported from the United States or the United Kingdom automatically fails one of the required elements for protection under the UNESCO Convention.[68] Another major issue with the UNESCO Convention is the lack of rights for individual owners of stolen artwork. Under the Convention, individuals who are victims of art theft are essentially at the mercy of their government's willingness to consider their stolen art as worthy of protection.

The UNESCO Convention's issues became glaringly obvious after several important court cases. These cases had the same theme: when determining who holds title to stolen artwork, *Nemo Dat* Jurisdictions apply *lex situs*—the law of the country where the art was sold by the thief to a bona fide buyer.[69]

In one infamous British case, *Winkworth v. Christie Manson and Woods Ltd* (1980), a collection of Japanese artwork called *netsuke* were stolen from Winkworth's home in England.[70] The *netsuke* were transported to Italy where they were sold to the Marchese Paolo Da Pozzo (the bona fide buyer).[71] Da Pozzo put the items on auction through Christie's (a popular auctioneer) and Winkworth sued, seeking an injunction and restitution.[72] The English court, applying conflict of law principles, found that because the sale took place in Italy, Italian law applied.[73] Crucially, Italy was a Good Faith Buyer Jurisdiction.[74] Consequently, the English court found that Da Pozzo purchased in good faith and exercised due diligence under Italian law; thus, Christie's won the lawsuit and Winkworth was left with nothing.

---

[66] As of the writing of this note, the UNESCO Convention has been ratified by 141 countries. *See* UNESCO Convention, *supra* note 63.
[67] UNESCO Convention *supra* note 63, at Art. I.
[68] The United States does have a growing body of law recognizing American Indian artifacts and artwork as cultural pieces, however this appears to remain almost exclusive to American Indian artifacts. FBI *infra* note 128.
[69] PALMER, *supra* note 26, at 12.
[70] *Case Summary: Winkworth v. Christie Manson and Woods Ltd.*, INT'L FOUNDATION FOR ART & RESEARCH, https://www.ifar.org/case_summary.php?docid=1192827443 (last visited Oct. 23, 2022). Winkworth v Christie Manson and Woods Ltd. (1980) 1 Ch 496, (QB).
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*

Another seminal case in international art theft litigation was *Autocephalous Greek-Orthodox Church v. Goldberg & Feldman Fine Arts, Inc.*[75] The case operated under similar conflict of law principles as *Winkworth*. In *Goldberg* several mosaics stolen from the Greek Church in Cyprus were sold to art dealers based in Indiana, but the sale itself was performed at a "freeport" in Switzerland.[76] Similar to their English counterparts, the American court used conflict of law principles and found that *lex situs* applied.[77] Switzerland is a Good Faith Buyer Jurisdiction.[78] However, the court found that the freeport was a mere fleeting transport area, therefore, the law of the bona fide buyer's home—the State of Indiana—applied.[79] As Indiana is a *Nemo Dat* Jurisdiction, the mosaics were ordered to be returned.[80]

The events of *Autocephalous Greek-Orthodox Church* occurred after the United States implemented several individual articles of the UNESCO Convention in 1983.[81] While it may seem that the UNESCO Convention would have made the litigation conclusive without reaching for *lex situs*, the Government of Cyprus—where the mosaics had been stolen—never requested the mosaics be returned. As a result, Autocephalous Greek Orthodox Church was forced to pursue the mosaics through pre-UNESCO litigation in the United States.

After several years, it was clear that having no set international standard for questions of restitution left *individuals* vulnerable and also failed to take into account that some of the largest art markets (the United States and the U.K.) had no official system of art classification. Consequently, in 1983 UNESCO held a specialist meeting to determine the impact of the UNESCO Convention.[82] This expert panel concluded that the International Institute for the Unification of Private Law (UNIDROIT) should coordinate to unify national laws, partially because criminals were exploiting different legal regimes (Good Faith versus *Nemo Dat*) to successfully offload stolen art.[83] In fact, there were several

---

[75] Autocephalous Greek-Orthodox Church v. Goldberg & Feldman Fine Arts, Inc., 917 F.2d 278 (7th Cir. 1990).
[76] *Id.*
[77] *Id.*
[78] *Swiss to Crack Down on Stolen Art*, FORBES (July 30, 2002, 12:01 AM) https://www.forbes.com/2002/07/30/0730hot.html?sh=67fd75b4ac30.
[79] *Id.*
[80] *Id.*
[81] Which, it should be noted, only partially implemented the UNESCO Convention; specifically Articles 7 and 9 "on a piecemeal bilateral basis." PALMER, *supra* note 26, at 12.
[82] Lyndel V. Prott, *UNESCO's Influence on the Development of International Criminal Law, in* CONTEMPORARY PERSPECTIVES ON THE DETECTION, INVESTIGATION AND PROSECUTION OF ART CRIME: AUSTRALASIAN, EUROPEAN AND NORTH AMERICAN PERSPECTIVES 143 (Saskia Hufnagel, Duncan Chappell, eds. 2014).
[83] *Id.*

prominent civil law lawyers—such as the legal counsel for the French Museums, Professor Jean Catelain—who pointed out that the Good Faith Buyer Rule aided art thieves.[84] Professor Catelain even suggested that the Good Faith Buyer Rule was inappropriate for determining the ownership of art and other objects of cultural heritage.[85]

Thus, in the 1990's, UNIDROIT convened in Rome to attempt to remedy the UNESCO Convention's issues. The product of these efforts was the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects (hereinafter "UNIDROIT Convention").[86] The UNIDROIT Convention recognized a legal difference between illegally exported and stolen artwork.[87] The UNIDROIT Convention also harmonized Good Faith Buyer and *Nemo Dat* rules by requiring that all signatories adopt *Nemo Dat* rules when it came to questions of ownership,[88] but required fair compensation for good faith bona fide buyers that exercised due diligence before purchasing.[89] Furthermore, the UNIDROIT Convention stated that a party is entitled to restitution of their stolen artwork if they make a claim within three years of finding the location of a stolen object.[90] However, claims were subject to a fifty year statute of repose, and signatories had the option of imposing an *absolute* statute of repose of seventy-five years.[91]

Additionally, the UNIDROIT Convention provided better guidance to courts on which factors they should consider when determining whether a bona fide buyer exercised good faith and due diligence. Some of these factors were: the behavior of the transacting parties, the price paid, whether the seller consulted registries of stolen

---

[84] Professor Catelain wrote "genuinely effective protection of the property concerned is impossible without total abolition of protection for purchasers . . . . If the legitimate owner is to be obliged to pay back the purchase price, recovery will often be impossible. Again, this would constitute indirect protection only of the final purchaser but also of all those through whose hands the object has passed." LYNDEL V. PROTT, COMMENTARY ON THE UNIDROIT CONVENTION 30 (1997). He was not the only civil law lawyer to see these problems; criticisms of the Good Faith Buyer Rule from civil lawyers began as far back as 1904. *Id.*

[85] *Id.*

[86] UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects, June 24, 1995, U.N.I.D.R.O.I.T.

[87] *Id.* Even though it made this distinction it left the definitional section on stolen art broader the sections on illegally exported art. This was done out of a fear that states would be over inclusive in what they deemed to be illegally exported art, thus leading to an outsized response from the host country.

[88] *Id.* at Art. 3(1) ("The possessor of a cultural object which has been stolen shall return it").

[89] Prott, *supra* note 82, at 143.

[90] UNIDROIT Convention, *supra* note 86, at Ch. II, Art. 3, Sec. 3–5.

[91] *Id.*

items, and any other relevant information and documentation that a buyer could reasonably have obtained.[92]

However, the great strides made by the UNIDROIT Convention came at a cost: many countries were unwilling to conform to the UNIDROIT Convention's sweeping changes. As a result, the UNIDROIT Convention has far fewer signatories than the UNESCO Convention (at the time of this note, the UNIDROIT Convention has 52 signatories compared to the UNESCO Convention's 141). Worse still, several major art market countries—including the United States and the United Kingdom—have refused to sign the UNIDROIT Convention.

While the lack of participation from the U.S. and the U.K. poses difficulties for some owners seeking restitution, there are a few mitigating factors that should be mentioned. First, both the U.S. and the U.K. are *Nemo Dat* jurisdictions. Thus, one of the most significant aspects of the UNIDROIT Convention—adopting a *Nemo Dat* standard for ownership—is not as crucial. Though, without the UNIDROIT Convention, ordinary conflict of law principles still apply, meaning courts will continue using *lex situs* to settle questions of ownership. While this poses an obstacle, one would hope that courts applying *lex situs* would take into account whether a country was a signatory of the UNIDROIT Convention. Unfortunately, common law jurisdictions *exclusively* apply the *domestic* law of the *lex situs* country, not that country's private international law, meaning courts applying *lex situs* do not consider whether a country is a signatory of the UNIDROIT Convention.[93] Even though Italy is currently a signatory of the UNIDROIT Convention, if the events in *Winkworth* occurred today, common law courts would reach the same conclusion: the Good Faith Buyer Rule applies. It is possible that this loophole could be resolved by signatories passing UNIDROIT Convention implementation legislation and incorporating it into that country's domestic law,[94] but it is unclear

---

[92] *Id.*

[93] "The English High Court[,] having accepted that France was lex situs, held that it was to French domestic law, and not to French private international law, that the court should look [at] to determine the effect of the law of France on original title." PALMER, *supra* note 26, at 14 (citing Government of the Islamic Republic of Iran v. Berend (2007) (QBD)). This is referred to as the doctrine of *renvoi*. It should be noted that *renvoi* doctrine differs in the United States, In Re Schneider's Estate, 96 N.Y.S.2d 652 (1950), thus, it is possible that U.S. courts would apply different rules for UNIDROIT countries.

[94] It is interesting to note that, if *Winkworth* were litigated today, English Courts would still apply Italian law, but because Italy implemented the UNIDROIT Convention into its domestic law in 2000, the English Court would apply the *Nemo Dat* rule as required by UNIDROIT. *Practical Operation of the 1995 UNIDROIT Convention: Italy*, UNIDROIT, https://www.unidroit.org/english/conventions/1995culturalproperty/1meet-120619/answquest-ef/italy.pdf (last visited Mar. 6, 2023).

whether common law courts would consider implementation legislation to be private international law or domestic law.

The second mitigating factor is that the UNIDROIT Convention does not require reciprocity to apply. This means that citizens in the United States or the United Kingdom can independently seek restitution under the UNIDROIT Convention from a signatory state, even though their home countries are not signatories. This is particularly important as both the United States and the United Kingdom have a large art market, and as *Nemo Dat* jurisdictions, they are susceptible to having their art stolen and exported to Good Faith Buyer Jurisdictions.

Neither the UNESCO Convention nor the UNIDROIT Convention are ideal solutions to the growing problem of international art theft. While the UNESCO Convention was a good start, its reliance on state-backed claims and designations excluded key countries and precluded individual claims. The UNESCO Convention also failed to harmonize the *Nemo Dat* and Good Faith Buyer rules. While the UNIDROIT Convention remedied many of these issues, its lack of adoption poses serious issues for enforcement—particularly in countries which apply *lex situs* to settle ownership disputes.

D. Implications for International Criminal Law

Both the UNESCO and UNIDROIT Conventions, despite largely dealing with restitution and procedural measures to recover art, also had a significant impact on the criminal law.[95] Especially in art law, civil and criminal law intertwine to form what many would describe as a seamless web.[96]

While UNESCO has little enforcement power on its own, signatory states have passed legislation that conforms to the UNESCO Convention's principles and creates penalties for engaging in the illicit trade of art.[97] However, the wide latitude which allowed the UNESCO Convention to become so broadly adopted has caused subsequent issues. Different interpretations of the UNESCO Convention among signatories has led to inconsistent enforcement.[98] Some nations, for example, while implementing the UNESCO Convention, failed to adopt criminal sanctions for breach of the Convention's principles.[99]

However, some international bodies have picked up the slack. Despite UNESCO's lack of punitive power,[100] organizations with criminal

---

[95] Prott, *supra* note 82, at 135.
[96] *Id.*
[97] *Id.*
[98] *See id.*
[99] *Id.*
[100] *Id.* at 136.

jurisdiction, such as the International Criminal Court, have begun punishing criminals who engage in illicit trade of art under the UNESCO Convention.[101] Furthermore, other treaties have incorporated the Convention's standards—including treaties of mutual legal assistance—which go hand-in-hand with improved extradition and enforcement.[102]

While significant international criminal sanctions in art law do not kick in until armed conflict,[103] the UNESCO Convention established civil sanctions that, while not directly targeting criminal activity, certainly had a significant impact on it.[104] For example, the UNESCO Convention requires signatories subject art dealers to penal or administrative sanctions if they fail to maintain a registry recording each item's origin, name, supplier information, description, and price.[105] The record-keeping requirement not only aids law enforcement in tracking theft, it also gives authorities the power to go after unscrupulous art dealers who fail to keep accurate records.[106]

UNESCO also takes an active role in attempting to deter the illicit art trade through educational resources.[107] UNESCO actively collaborates with Interpol and works with the International Council of Museums (ICOM) to publish lists of stolen and endangered art.[108] UNESCO has pursued regional workshops in partnership with Interpol and ICOM to educate dealers and push for greater enforcement.[109]

Turning to a concrete example of the criminal consequences of the UNIDROIT Convention, its examination of due diligence for buyers has led to several prosecutions in the art world. In one case, the prosecution of an art merchant named Giacomo Medici brought down an international web of stolen art and artifacts, and Medici himself was convicted and sentenced to ten years in prison.[110] Generally speaking though, international criminal sanctions are rare.

E. U.S. Art Theft

As mentioned prior, the United States is not a signatory of the UNIDROIT Convention. The United States, while currently a signatory of the UNESCO Convention, did not pass implementation legislation until 1983; even then, it only assented to Article 7(b) (prohibiting the

---

[101] Prott, *supra* note 82, at 135.
[102] *Id.* at 136.
[103] *See id.* at 136–41.
[104] *Id.* at 143.
[105] UNESCO Convention, *supra* note 63, at Art. 10(a).
[106] Prott, *supra* note 82, at 141.
[107] *Id.* at 146.
[108] *Id.* at 147.
[109] *Id.* at 147.
[110] *Id.* at 143, n.20.

import of stolen cultural property) and Article 9 (agreeing to take on a concerted effort to prevent pillaging and looting of archaeological sites).[111] Instead, the U.S. relies on a patchwork of state laws and federal statutes that draw no distinction between property and works of art. the U.S.'s current system is characteristic of the pre-nineteenth century understanding of art: that artwork was indistinguishable from other kinds of property.[112]

The primary mode of federal prosecution in art theft cases was, and still is, the National Stolen Property Act.[113] Passed by Congress in 1934, The National Stolen Property Act (hereinafter "NSPA") established a broad offense for transport and sale of stolen "goods" worth more than $5,000,[114] $100,000 when adjusted for inflation.[115] The senatorial debate was motivated and dominated by concerns over the growth of organized crime.[116] Though art, particularly stolen art, has been used as a money-laundering mechanism,[117] it appears that this was either unknown to the senators debating the bill, or the senators felt it was unnecessary to address. Regardless, there was no mention of artwork on the Senate floor.[118]

The first federal prosecution for stolen art under the NSPA came nearly thirty years later in *United States v. Hurley*.[119] In *Hurley*, the

---

[111] *Id.* at 143, n. 20. PALMER, *supra* note 26, at 12. UNESCO Convention, *supra* note 63, at Art. 7(b), Art. 9.

[112] The United States passed the Antiquities Act in 1906, 16 U.S.C.A. §§ 431-33 (West 1993), which made it a crime to export antiquities without a license, however, this was later ruled unconstitutional. LEONARD D. DUBOFF & CHRISTIE O. KING, ART LAW IN A NUTSHELL, 21-22 (3d ed. 2000).

[113] National Stolen Property Act, 18 U.S.C. § 2314 (1934).

[114] *Id.* § 2314(1).

[115] *CPI Inflation Calculator*, U.S. BUREAU OF LAB. STATS., https://www.bls.gov/data/inflation_calculator.htm (last visited May 2, 2022) (selecting May 1934 as the initial date, inputting $5,000, and selecting the date of the month of this paper's creation, April 2022, then pressing calculate).

[116] The law was passed as a way to extend the National Stolen Motor Vehicles Act as it was observed organized crime had begun trafficking in other stolen goods. 78 CONG. REC. 448 (1934) (statement of Sen. Royal S. Copeland), https://www.govinfo.gov/content/pkg/GPO-CRECB-1934-pt1-v78/pdf/GPO-CRECB-1934-pt1-v78-7-1.pdf.

[117] Duyne et al., *supra* note 37, at 80-81 ("A new relationship between art, crime, and money has come into being with criminalization of money laundering . . . . According to Nelson (2009), examples of art used for laundering abound . . . . In this regard they are put in line with other traders of valuable objects such as jewellers[sic] and car dealers . . . . In the literature on organized crime and money laundering, art hardly plays a role.").

[118] *Id.*

[119] United States v. Hurley, 281 F. Supp. 443 (D. Conn. 1968). As property is largely state law, there were likely many cases prosecuting art theft as property theft on the state level, however when it comes to the context of the internet, federal law applies—especially in cases of international transit.

Defendants burglarized a private home and stole several paintings.[120] They moved the paintings from Massachusetts to Connecticut.[121] Unable to offload the famous paintings, the Defendants placed them in the homes of relatives.[122] Under U.S. law at the time, it didn't matter whether the thieves stole *The Storm on the Sea of Galilee* or a large number of objects collectively worth over $5,000, the NSPA applied in either case. The NSPA has been amended to expand the broad term of stolen "goods" to include money, securities, and other assets, but again, no specific designation for artwork exists.

Before implementing parts of the UNESCO Convention, the U.S. had no statute explicitly prohibiting the import and export of stolen art. Still, the U.S. has no statute explicitly prohibiting the *export* of illegally stolen art.[123] Rather, the U.S. relies upon the broad applicability of the NSPA. Under the NSPA, art that is illegally exported from another country but legally imported into the U.S. is still considered "stolen," even if the art had not *actually* been stolen.[124] The United States also has provisions in some bilateral treaties with foreign countries, such as Mexico, that allow extradition for crimes against cultural property—including theft.[125]

In a landmark case applying this standard, *United States v. Hollinshead*,[126] an art dealer in Guatemala acquired pre-Columbian artifacts and exported them to the United States under suspicious circumstances. Guatemala, like Mexico, had designated all cultural artifacts, even undiscovered ones, as state property.[127] It is illegal to export these artifacts without a license.[128] The court found that the NSPA applied because the cultural objects were considered stolen under Guatemalan law and transported across international borders illicitly.[129]

Several other laws have been applied to art theft,[130] though only two sections of the U.S. Code explicitly prohibit theft and illegal trafficking in art and cultural artifacts: Theft of Major Artwork, and

---

[120] *Id.* at 445.
[121] *Id.*
[122] *Id.*
[123] Convention on Cultural Property Implementation Act, 19 U.S.C. §§ 2601–2613 (1983).
[124] United States v. McClain (McClain I), 551 F.2d 52, (5th Cir. 1977).
[125] DUBOFF & KING, *supra* note 112, at 17.
[126] United States v. Hollinshead, 495 F.2d 1154 (9th Cir. 1974).
[127] *Id.* It should be noted that it was lack of recognition of these kinds of laws that was a major motivator behind the UNESCO Convention.
[128] *Id.*
[129] *Id.* at 1155–56.
[130] *Art Theft*, FBI, https://www.fbi.gov/investigate/violent-crime/art-theft (archival link: https://web.archive.org/web/20220425165519/https://www.fbi.gov/investigate/violent-crime/art-theft) (last visited May 2, 2022).

Illegal Trafficking in Native American Human Remains and Cultural Items.[131] Therefore, only the NSPA and Theft of Major Artwork apply to non-American-Indian cultural items.

The Theft of Major Artwork (hereinafter "ToMA"), as the title suggests, attempts to distinguish *major* works of art from "standard" art classified as stolen under the NSPA. ToMA retains the $5,000 threshold established in the NSPA, but *only* for objects that are over one hundred years old.[132] However, there is no age requirement for art and cultural items that are worth over $100,000.[133]

There are, however, additional requirements for ToMA to apply. One of the elements requires that the artwork be stolen from a museum. The U.S. Code defines a museum as:

> [An] organized and permanent institution the activities of which affect interstate or foreign commerce . . . situated in the United States . . . established for an essentially educational or aesthetic purpose; has a professional staff; and owns, utilizes, and cares for tangible objects that are exhibited to the public on a regular schedule.[134]

By such a definition, a person's private collection would not qualify as a museum. Even if a thief steals "major artwork" (as defined by ToMA) from someone's home, ToMA does not apply. Additionally, by definition, ToMA only covers museums situated in the U.S. Thus, a thief who steals the *Mona Lisa* and exports it to the United States is not prosecutable under ToMA.

III. DEFINING ART

Having explained the various laws governing the theft of art both internationally and in the United States, this note now turns to what constitutes art.

A. U.S. Definitions

Courts and lawmakers have grappled with the question of what qualifies as artistic work for centuries. Different courts and different areas of the law have come to different conclusions on what art is, and

---

[131] 18 U.S.C. § 668 (1996).
[132] 18 U.S.C. § 668(a)(2) (1996).
[133] *Id.*
[134] 18 U.S.C. § 668(a)(1) (1996).

some of these conclusions have changed over time to become more inclusive.

One definition for art comes from U.S. customs law.[135] In disputes over tariff exemptions, "[c]ourts have focused on the appearance of the object" when questioning whether an item is art.[136] Reflecting the evolution of property ideas around artwork, early U.S. cases from the late nineteenth century restricted the term "art" solely to the fine arts.[137] The fine arts were distinguished from mechanical or industrial pieces; pieces that many would categorize as artwork today.[138] For example, in *United States v. Perry*,[139] the U.S. Supreme Court held that stained glass windows with images of saints could not enter duty-free as art.[140] While the Court acknowledged the beauty of the pieces, it drew a line between (fine) art and "decorative" elements for industrial and mechanical purposes.[141] The Court defined art as being "intended solely for ornamental purposes . . . including painting in oil and water, upon canvas, plaster, or other material, and original statuary of marble, stone, or bronze."[142] The definition excluded, inter alia, "[m]inor objects of art, intended also for ornamental purposes, [which] are susceptible [to] an indefinite reproduction of the original."[143]

It was not until the innovation of abstract art that things changed, culminating in Congress amending the tariff laws in 1958.[144] These 1958 amendments expanded the definition of art to include work "in other media," beyond the media listed in the customs definition.[145] This directive evolved with the adoption of the Harmonized Schedule in 1988. "The Harmonized Schedule incorporate[d] international established product definitions to which all major U.S. trading partners subscribe."[146] This definition still excluded some forms of what may be considered art though, such as "articles made by stenciling, photocopying, or other mechanical processes, or . . . painted or decorated manufactured articles, such as vases, cups, plates, screens, cases, trays, chests, etc."[147] Furthermore, the definition excluded castings and art

---

[135] DUBOFF & KING, *supra* note 112, at 1–7.
[136] *Id.* at 1.
[137] *Id.* at 1–2.
[138] *Id.*
[139] United States v. Perry, 146 U.S. 71 (1892).
[140] DUBOFF & KING, *supra* note 112, at 2 (citing United States v. Perry, 146 U.S. 71 (1892)).
[141] *Id.* (citing United States v. Perry, 146 U.S. 71 (1892)).
[142] *Id.* (citing United States v. Perry, 146 U.S. 71 (1892)).
[143] *Id.*
[144] *Id.* at 2–3.
[145] *Id.*
[146] *Id.*
[147] *Id.* at 4.

prints, only including prints that were made by hand.[148] The new definition allowed duty-free entry for commercial lines of limited edition sculptures as art, but only for the first ten pieces.[149]

As odd as it may sound, the creator of the artwork is also crucial in determining whether something is art or not in U.S. customs law.[150] Artwork can only be considered art if it was created by an "artist," not merely an "artisan."[151] The elements that show the difference between an artist and an artisan vary, but generally, it is said that an artist works from their own inspiration and skill, whereas the artisan—such as an artist's assistant—recreates or mimics an artist's work and therefore, is not working from their own inspiration.[152] This distinction appears to not apply to original paintings by hand; original paintings enjoy special treatment,[153] possibly because paintings by hand have been grandfathered in as "fine art."[154]

The final requirement for an object to be considered art is a lack of utility; whatever the piece is, it *cannot* be an item of utility nor made for commercial use. Most courts have taken a conservative stance on this point, holding that an object with *any* functional elements, cannot be art.[155] This is why objects like vases and cups, despite being artistic works, are excluded—they are utilitarian in nature—unless their size and dimension make it clear they're meant purely for ornamental purposes.[156]

In summary, when looking at U.S. Customs law, art is defined as: (1) an original object, (2) created by hand, (3) by an artist, (4) through his or her own inspiration and skill, (5) which cannot be used for utilitarian or commercial purposes. This definition (hereinafter "Customs Definition") has several flaws. Even though certain objects of utilitarian value are not considered art by the Customs Definition, intellectual property protects art, regardless of utility or commercial use.

To illustrate the discontinuity between these two areas of the law, consider gift wrapping paper. Wrapping paper can include some unique designs. These designs are protected by copyright and/or trademark. Yet, when wrapping paper arrives at a U.S. port, it is not considered "art" due to its utilitarian and commercial nature. This was a similar line of reasoning behind the U.S. Supreme Court's decision in *Bleistein v.*

---

[148] *Id.*
[149] The Harmonized Schedule expanded this to twelve. *Id.*
[150] *Id.*
[151] *Id.*
[152] *Id.* at 5.
[153] *Id.*
[154] *Id.* at 2.
[155] *Id.* at 5-6.
[156] *Id.*

Donaldson Lithographing Co.[157] In *Bleistein* the Supreme Court ruled that advertising illustrations, despite their commercial nature, are still protected by copyright as art.[158]

While the Customs Definition is flawed and underinclusive, it is the closest U.S. law gets to a definition of art. When looking at other areas of the law there is no litmus test: "[t]hings have been categorized as art if: (1) they sell; (2) creators (or others) offer them for sale as art; or (3) paradoxically, they are designated as art."[159] Thus judicial decisions attempting to create a formula have been scarce, with courts opting for a "know it when they see it" approach.[160] However, this has only really been used to draw a line between legitimate artistic expression and obscenity;[161] thus, it may not be instructive as to how a court would define artwork. Likewise, copyright litigation yields equally vague definitions. Courts have found that "[a]n object is art 'if it appears to be within the historical and ordinary conception of the term art.'"[162] Yet, courts have generally rejected attempts at standardless subjective definitions.[163] There is no clear definition of what art is or what art can be beyond the idea that there must be a limit or standard somewhere.

B. International Definitions

As explained earlier, there are two major conventions governing the illicit movement of artwork: the UNESCO Convention[164] and the UNIDROIT Convention.[165] Both have definitions and standards for what can be considered art.

While the UNESCO Convention restricts its applicability to items designated as art by signatory states, it does offer definitional elements to explain what it may consider to be "property of artistic interest;" these include:

> pictures, paintings and drawings produced entirely by hand on any support and in any material (excluding industrial designs and manufactured articles decorated by

---

[157] Bleistein v. Donaldson Lithographing Co., 188 U.S. 239 (1903).
[158] *Id.*
[159] ALEXANDRA DARRABY, 1 DARRABY ON ART LAW § 1:7 (2021).
[160] *Id.* at § 1:8 (citing Jacobellis v. State of Ohio, 378 U.S. 184 (1964) (Stewart, J. concurring)).
[161] *Id.*
[162] *Id.* (citing Rosenthal v. Stein, 205 F.2d 633, 635 (9th Cir. 1953)).
[163] *Id.* (citing Skyywalker Records, Inc. v. Navarro, 739 F. Supp. 578 (S.D. Fla. 1990), *rev'd,* 960 F.2d 134 (11th Cir. 1992)).
[164] UNESCO Convention *supra* note 63.
[165] UNIDROIT Convention *supra* note 86. For ease of reading, this note shall focus solely on art and omit the provisions and areas of the Convention that concern cultural artifacts.

> hand . . . original works of statuary art and sculpture in any material; . . . original engravings, prints and lithographs; . . . original artistic assemblages and montages in any material.[166]

This list (hereinafter "UNESCO List") gives broad definitions for art. These definitions can afford to be broad because art requires state designation to be protected. This assuages concerns that the definition is over-inclusive.

The UNIDROIT Convention lists: "cultural objects are those which . . . are of importance for . . . art . . . and belong to one of the categories listed in the Annex to this Convention."[167] The UNIDROIT Annex restates the UNESCO List verbatim.[168] While the UNIDROIT Convention does not have state designation of artwork as a limiting principle, it does have a "limiting" principle: for an object to be protected it must be "of importance for . . . art."[169] One can speculate that this would be interpreted to mean that the artwork must be of importance to the field of art—perhaps some kind of seminal work that began an art movement or a magnum opus by some great artist. Currently, there are no clear answers one way or the other.

While this hardly seems to be limiting at all, it may be a tacit acknowledgement that any attempt to define art will be underinclusive in some way. Having established national and international definitions for art, this note now turns to the question of how NFTs may be considered art.

IV. CLASSIFYING NFTS

There are different definitions for art in both U.S. and International law. It is easy to imagine that NFTs could fit into a broad, vague category of art because an NFT can be represented by anything visual. The question is how NFTs might fit into the definitions of art explained in Part III.

A. NFTs Under U.S. Customs

For an object to be artwork according to the U.S. Customs Definition, it must be (1) an original object; (2) created by hand; (3) by

---

[166] UNESCO Convention, *supra* note 63, at Art. 1(g)(i-iv).
[167] UNIDROIT Convention, *supra* note 86, at Art. 2.
[168] *See id.* UNESCO Convention, *supra* note 63, at Art. 1.
[169] UNIDROIT Convention, *supra* note 86, at Art. 1.

an artist; (4) through his or her own inspiration and skill; (5) which cannot be used for utilitarian or commercial purposes.

Regarding originality, Hohfeld NFTs would almost certainly fail. Just as a trading card is not an original piece of art, neither is a Hohfeld NFT. Many Blackstone NFTs also seem to fail the originality element too. Many NFTs are in collections that are procedurally generated or are variations of the same exact design (NFT "bored apes" are a prime example of this).[170] There are, however, some original Blackstone NFT visreps that aren't variations of the same exact design. Those NFTs would pass the originality element.

Assuming that a Blackstone NFT is an original piece, it might fail the second element—being made by hand. As all NFTs require a computer for their creation, the question becomes whether or not being made by someone on a computer qualifies as being made by hand. The Harmonized Schedule was passed only five years after the invention of the modern internet and two years before the world wide web,[171] it did not anticipate the proliferation of the internet or the use of computers to create unique artwork. One of the categories excluded from being considered art are objects made by a mechanical device.[172] Currently, there is no case law on the question of whether computers are mechanical devices. It is difficult to believe, given the inherent differences between mechanical devices and digital devices, that computers would be categorized as mechanical devices. It is possible that NFTs created by an individual—as opposed to being procedural or AI-generated—would likely pass the "handmade" element. For similar reasons, it is possible that many original NFTs, created by an individual, would pass the fourth element of the customs definition: something made through his or her own inspiration and skill.

Even if an NFT satisfies the elements above, the "made by an artist" element would likely prove fatal. Given the strict definition of "artist," it is doubtful whether most NFTs would qualify as being made "by an artist" rather than an "artisan" or an "amateur;"[173] this would certainly exclude any procedural or AI-generated NFTs as well.

---

[170] As an aside, the Bored Ape Yacht Club was hacked recently, resulting in the theft of many NFTs. Rich Stanton, *NFT Bored Ape marketplace gets hacked, people lose 'millions' in ape pictures*, PC GAMERS (Apr. 26, 2022) https://www.pcgamer.com/nft-bored-ape-marketplace-gets-hacked-people-lose-millions-in-ape-pictures/.

[171] While the internet was invented in the 1960s, the TCP/IP (IP address) wasn't invented until 1983, while the Harmonized Schedule was passed in 1988. *A Brief History of the Internet*, ONLINE LIBR. LEARNING CTR., https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml (last visited Mar. 6, 2023). The world wide web wasn't invented until two years after the Harmonized Schedule. *Id.*

[172] DUBOFF & KING, *supra* note 112, at 4.

[173] This is assuming that there is some framework to define what an NFT artist is and how to differentiate them from a digital artist.

Assuming an NFT passed the artist creation requirement, the fifth and final element—that the objects cannot be used for utilitarian or commercial purposes—may pose issues. While NFTs could probably get passed the utility exclusion, the noncommercial requirement may be problematic. Many NFTs are created to be sold, some in large collections, this might qualify as commercial activity.

In summary, while the U.S. Customs Definition would be fatal to the vast majority of NFTs—including all Hohfeld NFTs—it is possible to imagine that some Blackstone NFTs may pass muster under the Customs Definition.

B. Visrep Classification

Moving away from the Customs Definition, there is an alternative, simpler classification that could answer the question of whether NFTs are art or not. In Part I, this note analogized NFTs to trading cards. Asking whether NFTs are art is similar to asking whether trading cards are art. There are two primary reasons why this question is difficult: first, the token and its visrep are inseparable parts of one object; second, visreps range drastically in format—comic books, GIFs, tweets, etc. Given the variety of different visreps, it seems simplest to adopt a system of categorization based purely on whether the visrep is art (hereinafter "Visrep Classification"). To use the trading card analogy: if the photo of Michael Jordan on his trading card is art, then the whole trading card is, likewise, art. Just as a comic book is considered art, an NFT that uses a comic book as its visrep is also art. Inversely, because Jack Dorsey's first tweet is not art, the NFT of Jack Dorsey's tweet is also not art.

Superficially, Visrep Classification seems like a panacea, but there are serious issues with this system. First and foremost, Visrep Classification equates the token with its visrep. As explained in Part I, a token and its visrep are not the same, they are inseparable elements of one object. Each token is unique, visreps are not necessarily unique and they can be duplicated and placed on a new token. Second, Visrep Classification punts the issue of whether an NFT is art back down to whether the visrep is art; a question that, as demonstrated by legal attempts to define art, is vague.

Despite its flaws, if courts adopt Visrep Classification as the primary mode of NFT classification, it is certainly possible that NFTs could be categorized as art under U.S. copyright law. As stated earlier, under U.S. copyright law, "[a]n object is art 'if it appears to be within the historical and ordinary conception of the term art.'"[174] Determining

---

[174] DARRABY, *supra* note 159, at § 1:8.[175] *Id.* at § 1:7.[176] The UNESCO and UNIDROIT Conventions focus on who is the rightful owner of the artwork after it has been stolen

whether a particular NFT is art would be an ordinary case of art litigation. It is even more likely that NFTs could be categorized as art when one looks to the broader definitions for artwork. To reiterate, courts have found objects to be artistic works if "(1) they sell; (2) creators (or others) offer them for sale as art; or (3) paradoxically, they are designated as art."[175]

Yet, this does not end an NFT art analysis. As elaborated earlier, the unique nature of NFTs and the complex relationship between a token and its visrep means that an NFT art inquiry would involve two steps. First, one would ask whether an NFT was a Blackstone or a Hohfeld NFT. If the NFT is sufficiently "Blackstonian" then courts would proceed to step two of the analysis: whether the visrep is art or not. However, if the NFT is sufficiently "Hohfeldian" courts may be tempted to default to traditional notions of digital property ownership; that is to say, courts might decide that regardless of whether the token is non-fungible, because the visrep is fungible, it is not "original art" but a mere reproduction. Courts may conclude that because a Hohfeld NFT conveys no rights to the visrep beyond the right to display, a Hohfeld NFT is no more artwork than a single copy of a Michael Jordan trading card; or, as stated earlier, courts may default to traditional notions of digital ownership and decide that these NFTs, like most digital assets are inherently fungible.

In summary, if courts were to adopt Visrep Classification, despite its flaws, Blackstone NFTs may be considered artistic works while Hohfeld NFTs face larger obstacles. However, if courts rejected Visrep Classification, NFTs would face an uphill battle for recognition as art.

C. NFTs under International Definitions of Art

The internet is largely international; NFTs and NFT theft are, likewise, international. Whether NFTs can be protected under conventions governing stolen artwork depends on whether NFTs can fit into international definitions of art. Similar to U.S. Law, Blackstone NFTs seem to have a far better chance at recognition than Hohfeld NFTs. International law recognizes the right to title of an original artwork.[176]

---

and resold. While the UNIDROIT Convention provides some monetary restitution for a good faith bona fide buyer of a stolen piece, it does not officially recognize a right of possession.

[175] *Id.* at § 1:7.[176] The UNESCO and UNIDROIT Conventions focus on who is the rightful owner of the artwork after it has been stolen and resold. While the UNIDROIT Convention provides some monetary restitution for a good faith bona fide buyer of a stolen piece, it does not officially recognize a right of possession.

[176] The UNESCO and UNIDROIT Conventions focus on who is the rightful owner of the artwork after it has been stolen and resold. While the UNIDROIT Convention

Hohfeld NFTs do not convey title to their visrep, and therefore, are likely unprotected by international art theft law. Thus, only NFTs on the Blackstone side of the spectrum would be in the running for art law protection.

The UNESCO Convention does not offer a solution. Currently, no country has designated an NFT as part of their cultural heritage. Hypothetically, even if a country were to designate an NFT as part of their cultural heritage, it is unclear whether the UNESCO List would encompass *digital* artwork. As odd as this may sound, there is nothing that would explicitly prohibit a country from recognizing something digital as protected artwork. This is a case where Visrep Classification, for all its flaws, would aid in protecting Blackstone NFTs.

The UNESCO Convention provides protections for "pictures, paintings and drawings produced entirely by hand on any support and in any material (excluding . . . manufactured articles decorated by hand)."[177] For original NFTs, one could argue that the language "produced entirely by hand on any support and in any material" could cover using computers (as a "support") to create digital (the medium/"material") artwork.[178] Albeit, this may be stretching the definition too far. This definition would probably exclude procedurally generated collections, such as "bored apes," as it could be argued that the means of generating highly similar images only to be differentiated with handcrafted details, would qualify under the "manufactured articles decorated by hand" exception.

Yet, even these collections might be salvageable under the UNESCO List. The UNESCO List protects "original artistic assemblages and montages in any material."[179] While the originality element is up for debate, one could argue that, because these NFTs are part of a collection, it is a kind of montage or assemblage.

Additionally, there are other ways NFTs might be classified that protect them under the UNESCO Convention even if they aren't considered art. For example, the UNESCO Convention also covers "rare manuscripts and incunabula, old books, documents and publications of special interest (historical, artistic, scientific, literary, etc.) singly or in collections."[180] This could form the protection for NFT comic books and NFT documents.

While this ends the analysis of NFTs under the Conventions as artwork, it would be remiss to not discuss how NFTs could fall under the other subcategories of cultural artifacts; a classification that would not

---

provides some monetary restitution for a good faith bona fide buyer of a stolen piece, it does not officially recognize a right of possession.

[177] UNESCO Convention, *supra* note 63, at Art. 1(g)(i).

[178] *Id.*

[179] *Id.* at Art. 1(g)(iv).

[180] *Id.* at Art. 1(h).

even require resorting to a token's visrep. The UNESCO Convention permits protection for "property relating to history, including the history of science and technology and military and social history, to the life of national leaders, thinkers, scientists and artist and to events of national importance."[181] While it's not exactly clear from the drafting how important a thinker, scientist, or artist would have to be; theoretically, it could offer protection to both Hohfeld and Blackstone NFTs as their relevance could relate more to the token itself or the token's creator rather than its visrep. The UNESCO Convention also allows protection for "archives, including sound, photographic and cinematographic archives."[182] One could make the argument that the way NFTs are traded and tracked effectively on the blockchain creates an "archive" of ownership, though admittedly, this is less persuasive as really it is the blockchain that keeps track, not the NFT itself.

As the UNIDROIT Convention uses the same list as the UNESCO Convention,[183] the points made above could easily apply to the UNIDROIT Convention. As discussed earlier, though, the UNIDROIT Convention does not limit its applicability to artwork and objects designated by states, rather it limits its applicability to objects that "are of importance for archaeology, prehistory, history, literature, art or science and belong to one of the categories listed [in the UNESCO List]."[184] One may argue that certain NFTs are of importance to history, art, and/or (computer) science, but it is doubtful that they would all be significant.

Therefore, while NFTs can be protected as objects of cultural importance, whether NFTs can be classified as art comes down to how one conceptualizes NFTs: a token with a severable visual representation, or the token tied inexorably to its visual representation. The former categorization seems far more legally persuasive, given nothing would stop someone from minting two NFTs and assigning them identical visual representations—even though the tokens themselves are different. However, the latter conceptualization—that the token and visrep are inexorably tied—is more technically persuasive, as there is no way to strip an NFT of its visrep, and might be protected under art theft law. On the other hand, if one adopts the position that the token and its visrep are separate objects, then it seems simple to dismiss arguments that art theft law should apply. For the sake of analysis, this note shall now presume that NFTs are considered art.

---

[181] *Id.* at Art. 1(a).
[182] *Id.* at Art. 1(j).
[183] UNIDROIT Convention, *supra* note 86, at Annex *compare with* UNESCO Convention, *supra* note 63, at Art. 1.
[184] UNIDROIT Convention, *supra* note 86, at Art. 2.

V. THEFT & RESTITUTION

Presuming that NFTs are categorized as art, the next question is how this would impact the criminal law and the laws governing restitution.

A. Theft

Due to the interstate and international nature of the internet, federal and international law applies whenever an NFT is stolen. The NSPA, as pointed out earlier, has been amended to prohibit the transfer of stolen securities, money, goods, etc.[185] Under U.S. law, (regardless of whether NFTs are art or not) NFT theft is prosecutable under the NSPA.

The only specific art crime statute that the United States has is the ToMA. It is difficult to picture an NFT theft being prosecuted under ToMA. Similar to the very first conviction for art theft under the NSPA,[186] thieves have stolen NFTs from both private individuals and websites, but none from museums. ToMA requires that a museum be the target of the theft, and it defines exactly what a museum is—categories that are virtually impossible for anyone who is not extraordinarily wealthy to satisfy. However, it is possible that NFT theft could qualify for prosecution under ToMA in one narrow circumstance: if thieves stole an NFT from a museum. Given NFTs' increase in popularity, it is reasonable to assume that at some point a U.S. museum would acquire an NFT. If a thief stole that NFT, then that might satisfy the prima facie case for ToMA, with only one foreseeable issue: tangibility. Recall the definition of a museum in the U.S. Code:

> [An] organized and permanent institution the activities of which affect interstate or foreign commerce . . . established for an essentially educational or aesthetic purpose; has a professional staff; and owns, utilizes, and cares for *tangible objects* that are exhibited to the public on a regular schedule.[187]

While this might initially seem to pose some difficulty for NFTs, the definition doesn't specify that the *stolen* object be tangible, only that the establishment owns, utilizes, and care for tangible objects. In other words, an establishment must own, utilize, and care for tangible objects to be considered a museum, but the stolen artwork does not have to be

---

[185] 18 U.S.C. §§ 2314 et seq.
[186] United States v. Hurley, 281 F. Supp. 443 (D. Conn. 1968)..
[187] 18 U.S.C § 668(a)(1).

among those tangible objects. By this logic, it is possible that an NFT stolen from a U.S. museum might fall under ToMA.

When it comes to international law, NFTs would only be recognized as stolen under the UNESCO Convention if a state designates them as art or an object of cultural heritage. The United States, as mentioned beforehand, does not have a system of classification nearly as robust as other countries—even then, most of that classification revolves around American Indian artifacts.[188] Thus, it is highly unlikely there would be a movement in the United States to designate stolen NFTs as objects of cultural heritage. Regardless, it is disputable whether NFTs would qualify as an object of cultural heritage. Similar reasoning would apply when trying to apply the UNIDROIT Convention to NFTs.

Ultimately, whether NFTs are actually art, the international conventions would only aid in the prosecution of criminals if dealers, in buying NFTs, considered them artwork and adhered to the same international requirements that recently led to the conviction of Medici and the downfall of the web of international art theft in Italy. Otherwise, without state designation, there is little hope that NFTs on either side of the Blackstone-Hohfeld Spectrum can be protected.

B. Restitution

While the question of whether NFTs are art does not have much of an effect on criminal prosecution in the United States, it has wide-reaching implications when it comes to international restitution. Ultimately, similar to traditional art theft, the only way for thieves to make money is either by "artnapping" or offloading the NFT to a bona fide buyer.[189]

If NFTs are not art, then, regardless of international conventions on the illicit movement of art, straightforward conflict of law principles apply. This poses difficulties when applying these treaties to NFTs, especially if thieves use services such as Samurai's Whirlpool. If an NFT can bounce between digital wallets in multiple countries, the question is how courts can accurately determine *lex situs*. Countries may have different ways to resolve this under conflict of law principles, but it would be neither easy nor pleasant to navigate the various jurisdictions the NFT touched on its way to a bona fide buyer.

A cleaner answer to this question appears if one looks to *Autocephalous Greek-Orthodox Church*.[190] One could categorize wherever an NFT transaction takes place as a "fleeting transport area,"

---

[188] FBI, *supra* note 130.
[189] Chappell & Polk: The Peculiar Problem, *supra* note 41; Neuendorf, *supra* note 42.
[190] Autocephalous Greek-Orthodox Church, 917 F.2d 278 (7th Cir. 1990).

similar to the Swiss freeport where the Defendants in *Autocephalous* bought the stolen mosaics.[191] Thus, a court applying conflict of law principles could ignore the various jurisdictions the stolen NFT passed through and just use the bona fide buyer's home jurisdiction. Unfortunately, this approach would also leave NFT owners open to the same pitfalls as *Winkworth*; if the bona fide buyer exercised due diligence, purchased in good faith, and is in a Good Faith Buyer jurisdiction, then the original owner has no recourse. The only way to avoid application of *lex situs* in a common law country is to sue the bona fide buyer in the buyer's own country—but only if the buyer's country is a signatory of the UNIDROIT Convention. Assuming the original owner is successful, they'll still need to compensate the bona fide buyer. If an NFT is worth millions of dollars, the cost of that compensation may be prohibitive.

Given the nature of NFTs, questions arise about what constitutes good faith and due diligence. In traditional art transactions, bona fide buyers exercised due diligence by checking stolen art registries and other available resources. While lists of famous stolen NFTs are available online,[192] there are currently no widely retained registries of all stolen NFTs—given how easy it is to create NFTs, it may be impossible to ever have a registry of all stolen NFTs—still, it is one step a bona fide buyer could take. As many NFTs have a single image as their visrep, one can imagine performing a reverse image search[193] to scan registries of stolen NFTs. Due to the simplicity of these steps, courts could construe them as the bare minimum for due diligence.

If a bona fide buyer finds no record of the stolen NFT on those registries or through a reverse image search, the buyer can turn to the blockchain. Unlike traditional art, where provenance is not always clear and where art does not have a unique serial number, NFTs do. The entire transaction history for an NFT is on the blockchain. While services like Samurai's Whirlpool may "mix" the NFT, throwing off the original owner's efforts to track it down, a buyer might look at the number and frequency of transactions and immediately be tipped off that something was wrong. While there may be no concrete way to guarantee that an NFT is not stolen—barring an extensive search through the blockchain—there

---

[191] *Id.* at 282.

[192] Rebecca Moody, *Worldwide NFT Heists Tracker*, COMPARITECH (Nov. 1, 2022), https://www.comparitech.com/blog/vpn-privacy/nft-heists/.

[193] A reverse image search is a process by which a search engine can take an image and search the web for similar looking images. Matt Golowczynski, *Google Reverse Image Search: Everything You Need to Know*, SMARTFRAME (Nov. 13, 2020), https://smartframe.io/blog/google-reverse-image-search-everything-you-need-to-know/. There are limitations to this technology, for example, reverse image searches—as the name suggests—only work on images and only images that are sufficiently similar.

are certain steps a buyer can take to try and ensure an NFT wasn't stolen. Additionally, stolen NFTs bear certain hallmarks—such as being transferred between many different wallets—that can give buyers an idea of whether an NFT was stolen.

While courts may be tempted to impose a full transaction history search on any prospective NFT purchase as the bare minimum for due diligence, there are two issues with such an approach. The first issue is precisely how far back a bona fide buyer must go to satisfy due diligence. While performing this task might be easier today because NFTs are a new innovation, it will become far more difficult as the blockchain's size balloons and NFTs continue to proliferate. The second issue is whether performing a blockchain search might be too much to ask for non-sophisticated parties especially, as stated previously, because the size of the blockchain grows and the number of NFTs increase.

Continuing with the presumption that NFTs are art, the UNIDROIT Convention not only provides a safety net to original owners but also provides guidance on the factors courts should examine when determining whether a bona fide buyer did their due diligence. Those factors included: the behavior of the transacting parties, the price paid, whether the seller consulted registries of stolen items, and any other relevant information and documentation that a buyer could reasonably have obtained.[194] The last factor—information that a buyer could reasonably have obtained—at least offers some limiting principle the blockchain search. The question shifts from whether a buyer must search the blockchain at all, to how reasonably far the buyer must go in searching the blockchain.

Courts would look at the totality of the circumstances and, hopefully, understanding the complexity of the blockchain, would not expect a bona fide buyer to perform a full forensics work-up before purchasing an NFT, but to do at least some research into where the NFT originated from. On the other hand, perhaps courts would view due diligence differently depending on the cost of the NFT and the sophistication or resources available to the bona fide buyer.

So far, this section has concerned the duties of the bona fide buyer, yet, even in *Nemo Dat* Jurisdictions, the original owner also has duties and responsibilities if they seek to retain ownership. The question of a blockchain search and sophistication of parties is perhaps equally true to original owners when faced with the doctrine of laches and statutes of repose. The owner of a stolen NFT can track down the stolen art full stop, though it is made far more difficult if the NFT is mixed through a service like Samurai's Whirlpool. Original owners have a duty to try and track down their property and to seek restitution. Much like adverse

---

[194] *Id.*

possession,[195] failure to assert one's rights is a sure way to lose them. In the context of original owners, courts have found that lack of sophistication is insufficient to defeat a laches defense. In *Greek Orthodox Patriarchate of Jerusalem v. Christie's Inc.*,[196] the court found *inter alia* it was irrelevant to the doctrine of laches that the plaintiff was a monastery with very limited resources to conduct research. Thus, it would seem that a laches defense could hold against an NFT owner who claimed lack of sophistication and resources is what prevented them from tracking their NFT on the blockchain.

Statutes of Repose would also likely cut against an NFT owner. An NFT can easily be lost in the blockchain until the Statue of Repose expires, though admittedly, this could take many years. A patient enough thief however, may take their chances and perpetually mix the NFT until the statute of repose has expired, then sell it to a bona fide buyer. However, there is some hope that these strategies might be futile depending on when exactly the statute of repose tolls and expires.

If it is possible for an original owner to connect the digital wallet address of a bona fide buyer with a specific country or physical location, then the UNIDROIT Convention would aid the original owner in restitution. However, if the country in question is not a signatory of the UNESCO Convention or if the originating country is a common law country applying *lex situs* to a Good Faith Buyer jurisdiction, the original owner would face additional difficulties in recovering their NFTs. Furthermore, due to the digital nature of the artwork, there is nothing stopping a thief from "exporting" the artwork to a wallet address based in a different country to avoid having to return it.

CONCLUSION

It is only recently that NFT theft has raised the question of how to tackle non-fungible goods in a digital world. Indeed, the idea that anything digital could be truly non-fungible is groundbreaking. With the rise of non-fungibile digital assets, it appears that there may be a spot open in the legal lexicon for *digital* art theft, yet the art world—still struggling to adapt to the growing illicit international trade in *physical* art—seems a poor place to look for protection. Not only do attempts to categorize NFTs as art pose theoretical difficulties in art classification that would preclude most NFTs, but their ability to be fluidly transported across borders poses issues for any legal regime that ties legal rights to the NFT's presence in any particular jurisdiction.

---

[195] *Adverse Possession*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[196] Greek Orthodox Patriarchate of Jerusalem v. Christie's Inc., 1999 U.S. Dist. LEXIS 13257, 30-34 (S.D.N.Y. 1999).

Whatever the future may hold, NFTs, if they do fit within the scope of art law, do so uncomfortably. As a new technology, it appears that NFTs must either rely on the centuries-old laws of stolen property ownership or the emerging laws governing digital assets. Consequently, NFT owners are at the mercy of the same courts that decided *Winkworth* and the same civil law jurisdictions that favor circulation of property over the original owner's right to title. Until there is some legislative or international initiative to create special laws governing NFTs—which seems unlikely given how long and controversial efforts to create special rules governing traditional art and cultural artifacts—NFTs will continue being treated like any other stolen asset but, as the length of this note demonstrates, NFTs appear to be in a league of their own. While current U.S. law and international conventions struggle to comport with this vision of the future, given the high value of NFTs, it would be worth implementing specific legislation that addresses ownership, theft, and restitution of non-fungible digital assets in both the domestic and international context.

VOLUME 4 April 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

NOTES

ARTISTIC RELEVANCE IN ARTIFICIAL INTELLIGENCE? "*ROGER*" THAT!

*Kelly Heilman**

In an era of technological revolution, artificial intelligence is shocking the legal field with its increasing popularity, power, and potential.[1] The limits of property, personhood, and creativity are in question by both the public and the courts, leaving significant ambiguities in the law.[2] Legal standards regarding the regulation of advanced technologies have raised unique and critical substantive questions for intellectual property rights, particularly that of trademarks, where the traditional purpose is source identification between consumers and goods.

Since the 1989 holding in Rogers v. Grimaldi, the use of trademarks for creative purposes, as a matter of First Amendment jurisprudence, has resulted in a near-perfect track record as an infringement defense.[3] Questions have abounded as to who actually owns the property rights to an artificial intelligence generated work,

* Juris Doctor Candidate, Notre Dame Law School, 2023. Many thanks to Professor Gerard Bradley for his passionate guidance and encouragement as my advisor for this Note. I also want to express my sincere love and appreciation to God, my friends, and my family, especially Laines, for unending support in my journey through law school.

[1] *See generally* WORLD INTELL. PROP. ORG., INTELLIGENT TRADEMARKS: IS ARTIFICIAL INTELLIGENCE COLLIDES WITH THE TRADEMARK LAW? 2, https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ind_revella.pdf (last visited Sep. 18, 2022) (explaining the new approach to humans being replaced by AI technology as a "tectonic shift").

[2] *See generally* INT'L BUREAU OF W.I.P.O., MEETING OF INTELLECTUAL PROPERTY OFFICES (IPOS) ON ICT STRATEGIES AND ARTIFICIAL INTELLIGENCE (AI) FOR IP, WORLD INTELL. PROP. ORG. (2018), https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_itai_ge_18/wipo_ip_itai_ge_18_1.pdf.

[3] *See, e.g.*, Gordon v. Drape Creative, Inc., 909 F.3d 257, 261 (9th Cir. 2018). *See also* Stouffer v. Nat'l Geographic Partners, L.L.C., 460 F. Supp. 3d 1133, 1142 (D. Colo. 2020).

and who gets to claim it as his own artful invention.[4] *This Note advances the position that, due to the ongoing circuit split regarding the infamous Rogers test, the law needs to establish clear boundaries as to ownership in artificial intelligence and once-and-for-all define what it means for a work to be "artistically relevant."*[5]

It goes without saying that artificial intelligence will continue to transform the "trademark ecosystem" and that the law will need to innovate alongside it to keep up with market trends.[6] *Consumers must be able to identify artificial intelligence as its own "being" with its proper creators and sources—the source identifying purpose of a trademark—or intellectual property protection may begin to break down and face disincentives for registration in the first place.*

---

[4] Rogers v. Grimaldi, 875 F.2d 994 (2d Cir. 1989).
[5] *See* Stouffer v. Nat'l Geographic Partners, L.L.C., 460 F. Supp. 3d 1133, 1143 (D. Colo. 2020) (describing the *Rogers* test as "'needlessly rigid and [failing] to account for the realities of each situation").
[6] Sonia K. Katyal & Aniket Kesari, *Trademark Search, Artificial Intelligence, and the Role of the Private Sector*, 35 BERKELEY TECH. L.J. 501, 504 (2020).

ARTISTIC RELEVANCE IN ARTIFICIAL INTELLIGENCE? "*ROGER*" THAT!

Kelly Heilman

INTRODUCTION

From the *Rogers* case came the *Rogers* test ("the Test"), as did a circuit split, which is the subject of this Note.[7] The Test, described in detail below, is a defense to trademark infringement, with trademark law being regulated by the Lanham Act of 1946. If a trademark is used in a manner that is claimed to be "artistically relevant," defendants very likely will not face liability, based on the existing case law. The Test has two prongs. Using and portraying an already-registered trademark (not one's own) is protected unless (1) it has "no artistic relevance" to the underlying work, or (2) it explicitly misleads as to the source or content of the work.[8]

There appears to be two ways forward: either the property laws surrounding artificial intelligence become tighter and more transparent to the public, or the *Rogers* test will need to be, once and for all, addressed by the Supreme Court to define the limits—if any—of what it means for something to be "artistically relevant."[9]

For purposes of this Note, "artificial intelligence" is defined as "the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[10] Artificial intelligence is often used as a type of automatic utility to make product selections (possessing capabilities such as maintaining artificial neural networks and hosting expert systems and robotics) rather than doing so via mere human cognition, which confuses the way a traditional trademark functions.[11]

---

[7] Rogers, 875 F.2d at 999.
[8] *Id.*
[9] As stated in *Rogers v. Grimaldi*, 695 F. Supp. 112, 120 (S.D.N.Y. 1988), "[a]s the late Andy Warhol is reported to have stated, '[b]eing good in business is the most fascinating kind of art.'" By this quote, "art" is interpreted to have an incredibly broad meaning, intermingling business as an art in itself.
[10] Ida Arlene Joiner, *Artificial Intelligence*, SCI. DIRECT (2018), https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence#:~:text=Artificial%20intelligence%20is%20the%20theory,making%2C%20and%20translation%20between%20languages.
[11] WORLD INTELL. PROP. ORG., *supra* note 1, at 7.

However, artificial intelligence is not limited to science fiction-style robots, and such technology has snuck into the everyday lives of consumers.[12] This makes for an inquisitive study into who (or what) intellectual property rights belong to, and if secondary use of a trademark through artful creation is considered infringement under the *Rogers* test in commonplace technologies.

A. Where It All Began

The *Rogers* test is a product of *Rogers v. Grimaldi*.[13] In that case, Ginger Rogers and Fred Astaire were considered two of the most famous entertainment industry couples, enjoying the limelight and public recognition, grouped together as "Ginger and Fred." The Appellee-defendants produced and distributed a movie, also by the name of "Ginger and Fred," but with nominal relation to the couple.[14] The question at hand was how to balance the protection of the international recognition for the couple and the right of others to express themselves.[15] Rogers filed suit, seeking permanent injunctive relief and damages for other parties profiting off of *his* name.[16] As stated in the complaint, Rogers claimed the movie title:

> (1) violated section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a) (1982), by creating the false impression that the film was about her or that she sponsored, endorsed, or was otherwise involved in the film, (2) violated her common law right of publicity, and (3) defamed her and violated her right to privacy by depicting her in a false light.[17]

In trademark law, the main way to assess if a trademark has created a distinct commercial impression on the public is by the use of surveys, and such surveys are usually factored in quite heavily to a court's analysis as a primary source of evidence for consumer confusion.[18] Here, however, the risk of misunderstanding by the general consuming

---

[12] *Id.* at 6.
[13] Rogers v. Grimaldi, 875 F.2d 994 (2d Cir. 1989).
[14] *Id.* at 996
[15] *Id.* at 999.
[16] Rogers v. Grimaldi, 695 F. Supp. 112, 115 (S.D.N.Y. 1988).
[17] Rogers v. Grimaldi, 875 F.2d 994, 997 (2d Cir. 1989). *See also* Keller v. Elec. Arts Inc., 724 F.3d 1268, 1279 (9th Cir. 2013) (holding that the Rogers test should not apply "wholesale for right-of-publicity claims").
[18] *See* U.S. PAT. & TRADEMARK OFF., TRADEMARK MANUAL OF EXAMINING PROCEDURE § 1212.06(d) (July 2022).

public—in that the survey in this case found that members of the public *would* draw the incorrect inference that Rogers had some involvement with the movie at issue—was outweighed by First Amendment interests. The Second Circuit found it more dangerous to limit freedom of expression instead of following its typical jurisprudence, which would otherwise have, more likely than not, found the survey evidence to weigh in favor of the couple seeking to protect their name recognition.[19] If the point is to not mislead the consuming public, it appears that freedom of expression has surpassed that goal in terms of importance.

Initially, the District Court granted summary judgment to the defendants, explaining that the use of the name in the production title "failed" what is now called the *Rogers* test—as it was considered to be an "artistic expression."[20] Under the Lanham Act, the law does not bar a minimally relevant use of a celebrity's name in the title of an artistic work where the title does not explicitly denote authorship, sponsorship, or endorsement by the celebrity or explicitly mislead as to content.[21] Defendants argued, however, that the use of Rogers' first name *was* an exercise of their artistic freedom of expression under the First Amendment.[22] With such a claim, the plaintiffs had to meet the heavy burden of establishing that the speech at issue was intended, strictly, to mislead and misuse their rights and recognition, and thus, did not fit under the broad category of freedom of speech protection.[23] On appeal, the Second Circuit held that the sponsorship and endorsement of Rogers' claim raised no genuine issue of material fact since the title did not occupy *any* explicitly misleading endorsement. Therefore, it did not fit under the First Amendment category of commercial speech because the title was found to not be serving a commercial purpose, but rather, a First Amendment one since it was more than an "ordinary commercial product."[24] The speech also did not meet the requirements for the commercial speech analysis, which would otherwise fall under the categories of "trade or advertising" or an "advertisement in disguise" for a "collateral commercial product."[25] Ultimately, again, commercial speech as a potential analytical category for artistic expression and

---

[19] Rogers v. Grimaldi, 875 F.2d 994, 1005 (2d Cir. 1989).
[20] Rogers v. Grimaldi, 695 F. Supp. 112, 124 (S.D.N.Y. 1988).
[21] 15 U.S.C. § 1125(a).
[22] Rogers, 875 F.2d at 998.
[23] *See* Rogers, 695 F. Supp at 112, 124.
[24] Rogers, 875 F.2d at 1006. *See, e.g.*, Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N. Y., 447 U.S. 557 (1980) (explaining the main framework under which the commercial speech analysis arose).
[25] *Id.*

creation in trademark suits proved to not fit appropriately to the existing law, and plaintiffs could not meet the heavy burden of the sweeping protection for artistic relevance under the original *Rogers* test.

B. Inconsistencies with the Foundations of Trademark Law

Traditionally, trademark law has been based in economic theory and preventing unfair competition. With its roots in Article 1, Section 8, Clause 8 of the United States Constitution, intellectual property protections have historically been an essential right as part of a flourishing marketplace.[26] At the most fundamental level, trademark law is meant to protect what Mark McKenna, a renowned trademark scholar, has described as the goal of modern marketing and branding—to rescue producers from having to compete on price or quality.[27] The use of a mark on behalf of the consumer is "an emotionally-driven choice as well as an economic one."[28] Though protecting commercial fairness, business, and innovation is a special priority for the courts, particularly to further the hallmark of this practice area, courts still struggle with whether to prioritize these principles first, or to prioritize placing such commercial activities under First Amendment jurisprudence, typically the *Central Hudson* analysis.[29]

With artificial intelligence, that struggle intensifies as the law around such technology is so new and still developing, without a clear way to avoid a likelihood of consumer confusion. One could argue artificial intelligence fits more properly, first, under market-based legal analyses since it is strongly grounded in innovating the economic sphere. However, an equally enticing argument might suggest that artificial intelligence, as creations or pieces of technological art and skill, should fall under commercial activities as regulated by the First Amendment. The courts are still considering this issue. Nevertheless, by its efficacy and obvious manufacturing of human ingenuity, thus far, artificial intelligence as an art form finds its legal implications as falling within First Amendment jurisprudence as a sort of artistic "creation," leaving trademark law behind.

---

[26] U.S. Const. art. I, § 8, cl. 8.
[27] Mark P. McKenna, *Consumer Decision-Making Theory of Trademark Law*, 98 VA. L. REV. 67, 115 (2012).
[28] Katyal & Kesari, *supra* note 6, at 515.
[29] *See* 2 ANNE GILSON LALONDE & JEROME GILSON, GILSON ON TRADEMARKS § 7.02(1)(6)(C), MATTHEW BENDER & CO. LEXISNEXIS (database updated Sep. 2022); Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N. Y., 447 U.S. 557 (1980).

Because trademark law revolves around the "consumer,"[30] the first step in figuring out where artificial intelligence might legally fall is to understand how, over time, consumers associate the services offered by artificial intelligence with their sources. By looking at the *Abercrombie* case—which provides a spectrum as to how recognizable a mark is within the public mind—trademark examiners will assess the degree to which a particular trademark falls.[31] Outside of that spectrum, a mark might acquire what is known as secondary meaning (also referred to as acquired distinctiveness), meaning a mark becomes so commonplace and recognizable that regardless of where a mark falls on the spectrum, the public still recognizes the mark as indicating a certain source.[32] Thus, to receive protection, a mark must either: (1) fall into the appropriate category of the *Abercrombie* spectrum, or (2) acquire secondary meaning.[33]

In one of the most famous trademark law cases, *Qualitex Co. v. Jacobson Prods. Co.*, the Supreme Court described that:

> [T]rademark law, by preventing others from copying a source-identifying mark, 'reduces the customer's costs of shopping and making purchasing decisions,' . . . for it quickly and easily assures a potential customer that *this* item—the item with this mark—is made by the same producer as other similarly marked items that he or she liked (or disliked) in the past.[34]

---

[30] For a discussion of the "consumer" as the basis of trademark law, *see* U.S. PAT. & TRADEMARK OFF., *supra* note 18, at § 1215.02..

[31] Abercrombie & Fitch Co. v. Hunting World, 537 F.2d 4, 9–11 (2d Cir. 1976).

[32] There are four categories of trademarks: 1. Generic: defines an everyday or general term which everyone has the right to use. Generic marks are not protectable. 2. Descriptive: a mark which describes the goods or services and will be allowed protection if the owner can show secondary meaning. 3. Suggestive: a mark which suggests the quality or attributes of a good or service. Suggestive trademarks are different from descriptive marks in which they don't describe the product, but instead, suggest a feature that requires some thought or perception on the consumer's part. 4. Arbitrary or Fanciful: a fanciful trademark is one that is completely made up, such as Kodak. Fanciful marks are afforded the most protection. An arbitrary trademark is one with common meaning, but the meaning doesn't relate to the goods or services offered. An example is the name Apple for a computer. A computer has no connection to fruit so the mark is therefore arbitrary. *See generally* U.S. PAT. AND TRADEMARK OFF., PROTECTING YOUR TRADEMARK, https://www.uspto.gov/sites/default/files/documents/BasicFacts.pdf (last visited Sep. 23, 2022) (explaining trademark basics and procedures).

[33] U.S. PAT. & TRADEMARK OFF., *supra* note 18, at § 1212.

[34] Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 164–65 (1995) (internal citations omitted).

Until *Qualitex*, conventional mechanisms of source-identification were rather straightforward. Artificial intelligence, however, provides some new challenges because the source of the artificial intelligence itself has invented the concept that itself as a "smart" being is a product or a good, which automatically offers its own services. This confuses what, or who, is the source versus the service under the existing law.

Because trademark law is grounded in principles of competition, and because artificial intelligence is now another source of innovation, all of trademark jurisprudence is facing a never-before-seen challenge and must innovate to keep up with market trends. Over time, such a unique—and confusing—change in source identification will make it quicker for consumers to connect products to their sources via technology. The programming of such technology might be considered an art or software created by its inventor or its artist, or a source identifying entity itself.[35]

C. Passing the Rogers Test with Flying Colors

Under the *Rogers* test for artistic use,

> "the use of a third-party mark in an expressive work does not violate the Lanham Act 'unless the title has no artistic relevance to the underlying work whatsoever, or, if it has some artistic relevance, unless the title explicitly misleads as to the source or the content of the work.'"[36]

With a lack of unanimity as to the interpretation of the words of the Test, courts have taken such ambiguity to mean there is leeway for expressive use in a broad sense. As elaborated in *Gordon v. Drape Creative,* under *Rogers*, the defendant is required to show that the alleged infringing use is technically part of his freedom of expression under the protection of the First Amendment.[37] If the defendant is successful, then the plaintiff faces a heightened burden of proof. The plaintiff must satisfy both the likelihood of confusion analysis and at least one of the two *Rogers* test prongs, which the *Gordon* court restated as:

---

[35] Elizabeth Rocha*, Sophia: Exploring the Ways AI May Change Intellectual Property Protections*, 28 DEPAUL J. ART TECH. & INTELL. PROP. L. 126, 145–46 (2018).
[36] Scott Hervey, *The Rogers Test Gets a Remake in Colorado*, JD SUPRA (Apr. 23, 2021), https://www.jdsupra.com/legalnews/the-rogers-test-gets-a-remake-in-7700800/; *see also* Rogers v. Grimaldi, 875 F.2d 994, 999 (2d Cir. 1989).
[37] Gordon v. Drape Creative, Inc., 909 F.3d 257, 264–65 (9th Cir. 2018) (also stating that the use of the *Rogers* Test defense had never failed before).

> When the defendant demonstrates that First Amendment interests are at stake, the plaintiff claiming infringement must show (1) that it has a valid, protectable trademark, and (2) that the mark is either not artistically relevant to the underlying work *or* explicitly misleading as to the source or content of the work.[38]

The above-described *Rogers* test has been recognized in a handful of cases as being dangerously overbroad. In *Gordon*, the court stated that the use of the *Rogers* test defense *never* failed before *Gordon* was decided.[39] Claims for artistic relevance, with such a low bar to support one's claim, pose a threat to the historically sound nature of decades of trademark jurisprudence.[40] "[B]asically, if the level of artistic relevance is more than zero, this is satisfactory."[41]

To prepare for an influx of the inevitably ensuing artificial intelligence over the coming years, trademark law becomes more important than ever, as protecting the rights of innovators is what keeps them innovating. To keep them innovating, the *Rogers* test must be narrowed, and the term "artistic relevance" properly defined in scope.

I. THE CONTROVERSY IN CONTEXT

The *Rogers* test is facially concerning because of its sweeping language for the protection of artistically relevant trademarks. Moreover, it is concerning for the field of artificial intelligence because it poses greater potential for infringement, such as secondary liability issues.[42] *Rogers* applies to more than mere titles of a work or parodies; it carries over to an expansive breadth of creations, productions, and

---

[38] *See id.*; *see also* Louis Vuitton Malletier S.A. v. Warner Bros. Ent. Inc., 868 F. Supp. 2d 172, 178–79, 184 (S.D.N.Y. 2012) (holding that the speech at issue was clearly artistically relevant with no matter being explicitly misleading; the court was willing to use the *Rogers* test even at the motion to dismiss phase).

[39] *See* Gordon v. Drape Creative, Inc., 909 F.3d at 261. *See also* Stouffer v. Nat'l Geographic Partners, L.L.C., 460 F. Supp. 3d 1133, 1142 (D. Colo. 2020) (explaining that *Gordon* is "analytically messy").

[40] "Artistic relevance" applies to more than just titles in trademark law. It can be expanded to cover claims of copyright infringement as well, meaning it has a dangerous scope in that can be considered overbroad. *See* Christian v. Mattel, Inc., 286 F.3d 1118, 1128–29 (9th Cir. 2002).

[41] Hervey, *supra* note 36.

[42] *Secondary Trademark Infringement Liability in the E-Commerce Setting*, USPTO (Aug. 2021), https://www.uspto.gov/sites/default/files/documents/Secondary-TM-Infringement-Liability-Response.pdf.

compositions, which, when not under the umbrella of copyright law, are under the umbrella of trademark law, thus, being subject to traditional trademark rules and practices. When artificial intelligence takes on formerly human tasks such as buyer, searcher, consumer, etc., it has the potential to be considered as using someone else's already-registered mark, otherwise known as secondary infringement. In fact, Kevin Casey helps communicate this dilemma by posing the following question: "[W]hen your Amazon Echo suggests and buys a product for you that infringes a registered trademark or is a counterfeit, does Amazon become a secondary infringer?"[43]

By claiming that artificial intelligence is one's product of artistic expression, however, plaintiffs who have been the victims of infringement may face a higher bar to seek the same remedies in infringement suits. While various intellectual property concerns about this have come before the World Intellectual Property Organization (WIPO), the Secretariat of WIPO uniquely excluded addressing trademarks.[44] What this illustrates is that we are missing sufficient research and scholarship into what the impacts of artificial intelligence are and who will address them. Though most remain optimistic for this circuit split to ultimately be resolved in favor of justice for intellectual property owners, many remain skeptical. "These changes may 'significantly improve the trademarking process' in the future. So far, however, the implementation has been 'suboptimal.'"[45]

A. The First Amendment in Trademarks: Historical Overview

Both intellectual property and First Amendment law have been "inextricably intertwined"[46] for quite some time, but routinely, the Supreme Court has favored First Amendment freedoms over intellectual property exceptions. "Artistic relevance" as a category of creative freedom of expression has a longstanding historical foundation throughout American legal history. Expressive works are subject to special treatment in the law for two primary reasons: "(1) they implicate the First Amendment right of free speech, which must be balanced against the public interest in avoiding consumer confusion; and (2) consumers are less likely to mistake the use of someone else's mark in an

---

[43] Kevin R. Casey, *Artificial Intelligence in the Trademark World IP Appeal, Fall 2020*, STRADLEY RONON (Oct. 6, 2020), https://www.stradley.com/insights/publications/2020/10/ip-appeal-fall-2020.
[44] Katyal & Kesari, *supra* note 6, at 504.
[45] Casey, *supra* note 43, at 3.
[46] Rogers v. Grimaldi, 875 F.2d 994, 998 (2d Cir. 1989).

expressive work for a sign of association, authorship, or endorsement."[47] Courts have been habitually skeptical in declaring what is and is not regarded as freedom of speech in trademark cases, as it is onerous to present an argument that seeks higher preference than the very foundation of the Constitution's *First* Amendment.[48] As of now, there is little, if any, precedent on artificial intelligence being fitted within the boundaries of the First Amendment category, which this Note suggests signifies the need for further study to provide sound judgment and guidance when these types of infringement cases inevitably come up in the near future.

1. The Hallmark Cases

One need not look further for a synopsis on where the Court currently stands on these issues than landmark cases *Matal v. Tam*[49] and *Iancu v. Brunetti*.[50]

In *Matal*, decided in 2017, the USPTO denied the trademark application for an Asian band, "The Slants," arguing that it was disparaging under section 2(a) of the Lanham Act's disparagement bar, which, at the time, prohibited registration of marks that may "'disparage . . . or bring . . . into contemp[t] or disrepute' any 'persons, living or dead.'"[51] The Band successfully argued that it was using the term at issue to "reclaim" its negative connotation from popular culture and "'take ownership' of stereotypes about people of Asian ethnicity."[52]

In the tradition of protecting free speech, the Supreme Court held the disparagement bar facially unconstitutional because the clause engaged in viewpoint-based discrimination, and was "not an anti-discrimination clause, [but] a happy-talk clause."[53] Some argued that *Matal* should fall under the First Amendment's commercial speech analytical framework, but Justice Kennedy held this as irrelevant because viewpoint-based discrimination necessarily invokes heightened scrutiny, whether or not commercial speech is targeted.[54] Since the broad clause was held unconstitutional, refusing trademark registration to The Slants was not a plausible outcome. Ultimately, the law now holds that whether

---

[47] Hervey, *supra* note 36.
[48] U.S. Const. amend. I.
[49] Matal v. Tam, 137 U.S. 1744 (2017).
[50] Iancu v. Brunetti, 139 U.S. 2294 (2019).
[51] *Matal*, 137 U.S. at 1751; 15 U.S.C. § 1052(a).
[52] *Matal*, 137 U.S. at 1754 (citing *In re Tam*, 808 F.3d 1321, 1331 (CA Fed. 2015)).
[53] *Id.* at 1765.
[54] *Id.* at 1750.

a trademark is disparaging to a subsection of the consuming public has no relation to the purpose of trademark law or registration, which is to facilitate source identification amongst consumers as a component of private speech.[55] Thus, the Slants trademark registered.[56]

Then, two years later in *Iancu*, the Supreme Court held that trademark law allows broad protection of *all* speech, universally covering immoral or scandalous material, a landmark holding for the intellectual property field.[57] In that case, a trademark with the letters "F U C T" was rejected by the USPTO on the grounds that it contained "immoral, deceptive, or scandalous matter" under section 2(a) of the Lanham Act, previously held two years prior to have unconstitutionally disfavored certain ideas.[58] The Court, again, in the tradition of protecting free speech, reasoned that to reject this trademark would be viewpoint-based discrimination. Rather, then, the Court suggested a narrowing of the statute, which could be "reasonably read to bar the registration of only those marks that are obscene, vulgar, or profane,"[59] or those whose "mode of expression" (independent of viewpoint) is particularly offensive. Here too, then, the trademark registered.

In both of these landmark cases, the Court protected First Amendment prerogatives, despite existing trademark regulations which were already in place for many, many years. Thus, throughout this Note, it is important to keep in mind that overcoming a freedom of expression argument is, evidently, incredibly difficult.

B. Sophisticated Consumers as a Setback

Further, the concept of "sophisticated consumers" is a relevant component, for sake of the *Rogers* test application, of the federal *DuPont* factor analysis for likelihood of confusion.[60] A typical "sophisticated consumer" would have prior knowledge in selecting a good or service, and thus have a higher degree of "sophistication" in identifying a product with its source. Machine learning through artificial intelligence can thus blend this factor with new meaning from what it entails for a "sophisticated" consumer to automatically have knowledge of marks and

---

[55] *Id.* at 1768.
[56] "The Slants," Registration No. 5332283 (Nov. 2017), https://tmsearch.uspto.gov/bin/showfield?f=doc&state=4807:119h4t.2.6.
[57] Iancu v. Brunetti, 139 U.S. 2294, 2301 (2019).
[58] *Id.* at 2298.
[59] *Id.* at 2317.
[60] U.S. PAT. & TRADEMARK OFF., *supra* note 18, at § 1207..01.;*In re* E. I. du Pont deNemours & Co., 476 F.2d 1357, 1361 (C.C.P.A. 1973).

their sources. According to the European Court of Justice, it is assumed that the average consumer is defined as "reasonably well informed and reasonably observant and circumspect."[61] However, now, we are looking at the source itself—the technology—as being sophisticated, easing the effort on behalf of the average consumer. Since the major motivations behind creating artificial intelligence included customer experience, optimizing decision-making, new revenue, efficiency, and cost reduction, moving forward, exactly how a source is identified has become the key question.

As courts grapple with the internet beginning to surpass human judgment in certain areas, consumer sophistication with new technologies may alter what it means for trademark law to actually *encourage* more registrations, if consumers themselves are not really the ones doing the source identification. The conventional doctrines may not be as readily applicable as they once were.

As long as there is an emotional connection between a source and a consumer (the purpose of a trademark), the law remains straightforward and in favor of applicants seeking admission on the Principal Register, but as this Note argues, the law cannot give clear answers here. There is "at least some potential for AI to surpass human judgment and performance when it comes to analyzing and integrating a much wider array of variables in its assessments."[62] Trademark law has always been grounded in economic, consumer-based, demand-side considerations.[63] Trademark infringement, then, has been relatively straightforward, falling primarily under the most common causes of action: likelihood of confusion and dilution.[64] Trademark law *wants* more innovation and registered marks; an initially unregistrable mark, due to its descriptiveness, may, for example, acquire secondary meaning, and be protected if enough consumers come to associate the mark with its source.[65] A "plaintiff need *only* prove . . . that there is an economic interest in her identity, and that her identity has been commercially exploited."[66] This necessitates that the federal *DuPont* factor analysis for

---

[61] WORLD INTELL. PROP. ORG., *supra* note 1, at 10.
[62] Katyal & Kesari, *supra* note 6, at 586.
[63] *Id.* at 507.
[64] *Trademark Infringement*, https://law.jrank.org/pages/10850/Trademarks-Trademark-Infringement.html, (last visited Oct. 20, 2022).
[65] Abercrombie & Fitch Co. v. Hunting World, 537 F.2d 4, 9 (2d Cir. 1976).
[66] Rocha, *supra* note 35, at 132 (citing Landham v. Lewis Galoob Toys, Inc., 227 F.3d 619, 624 (6th Cir. 2000)) (emphasis added).

likelihood of confusion, particularly the "sophisticated consumers" prong, will need to be looked at from fresh eyes.[67]

C. Additional "Sophisticated" Setbacks: Personhood

As consumers adapt more and more to the use of creative technologies, the arena for infringement is about to change, especially as artificial intelligence is, literally, wired to make economic decisions in terms of purchases that otherwise belonged to consumers themselves. To emphasize the extent to which this has been taken, for example, the futuristic, stereotypical conception of robots as fully-functioning humans is no longer a distant possibility, but a reality.

Honorary legal personhood has been granted, albeit heavily scrutinized, to "Sophia," a robot created by artificial intelligence.[68] Unsurprisingly, this has raised an influx of alarming questions for the legal landscape. "'[G]enerally consumers place more trust in an independent third party to provide truthful information on quality,' suggesting a role for independent third-party private certification," or here, artificial intelligence itself.[69] Artificial intelligence, in particular forms like the "person" Sophia, might be dismissed for liability because they are now "art forms" generated by scientists. The courts are split already on the *Rogers* test, and the limits to what personhood encompasses are additionally complicated by the creation of other "beings" pushing the boundaries of "personhood." This is interesting to consider given that the name "Sophia" is described as having no doubt in being able to attain secondary meaning required by the USPTO.[70]

Given the inherently subjective nature of consumer emotion and product preference portrayed through survey evidence, trademark law must decide where it stands on this new type of technology. Such a sophisticated invention such as artificial intelligence can easily be deemed a form of expressive art as it has profound, human work going into its formation, which then seeks the attention of the viewer or user.

In effect, artificial intelligence technologies are beginning to make the decisions that previously were the responsibility of consumers themselves, and thus, this changes the entire nature of what it means for trademark owners to relate to consumers.

---

[67] *In re* E. I. du Pont deNemours & Co., 476 F.2d 1357, 1361 (C.C.P.A. 1973).
[68] Rocha, *supra* note 35, at 133. *See also* Dennis Crouch, *USPTO Rejects AI-Invention for Lack of a Human Inventor*, PATENTLYO (Apr. 27, 2020), https://patentlyo.com/patent/2020/04/rejects-invention-inventor.html.
[69] Katyal & Kesari, *supra* note 6, at 511.
[70] Rocha, *supra* note 35, at 141.

II. WHERE *ROGERS* STANDS TODAY

A. Circuit Split Implications

In application here, as the Second Circuit departed from typical trademark jurisprudence in *Rogers*, the landscape of "artistic relevance" has expanded. Courts are wary to subject trademark users to liability if an artist or creator deems his work as "artistically relevant," which usually comes out in favor of the artist or creator, not the trademark owner. This low bar is especially prevalent in the Ninth Circuit, with the court liberally protecting individuals and artists from corporate business operations.[71] Artificial intelligence's use of trademarks, celebrity names, advertisements, voice recognition, and algorithmic search engine scans, amongst other things, is entering new grounds.

For example, in an expressive use, *Rogers*-like case, *Mattel, Inc. v. MCA Record, Inc.*, the Ninth Circuit held that the use of the *Barbie Girl* song as a parody was considered expressive use.[72] In the parody, no matter the ways the defendant presented plaintiff's mark to the public, the use of the famous *Barbie* doll trademark was held not to constitute infringement of the famous toy company's trademark ownership, even after its fame for many years as a cultural icon. [73] The makers of the parody, under *Rogers* expressive use defense, were not liable for infringement, even though Barbie was recognizable worldwide and sought registration long before the party made the parody.[74] This was the first Ninth Circuit case to adopt the *Rogers* test, a significant action in that the Ninth Circuit has since routinely applied the Test's low artistic-relevance bar, despite the reputational implications for trademark owners.[75]

The tradition of protecting the freedom of expression may have been flipped on its face by the use of the *Rogers* test, creating more implications than necessary. If federal intellectual property registration,

---

[71] *See* ACLU of S. Cal., *Victory Over Mattel For Artist and First Amendment*, ACLU (Dec. 29, 2003), https://www.aclusocal.org/en/news/victory-over-mattel-artist-and-first-amendment. *See also* INT'L TRADEMARK ASS'N, ARTIFICIAL INTELLIGENCE (AI) AND THE FUTURE OF BRANDS: HOW WILL AI IMPACT PRODUCT SELECTION AND THE ROLE OF TRADEMARKS FOR CONSUMERS? (2019).
[72] Mattel, Inc. v. MCA Record, Inc., 296, F.3d 894 (9th Cir. 2002).
[73] *Id.* at 908.
[74] *Id. See also* Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC., 507 F.3d 252 (4th Cir. 2007) (protecting the use of a parody of dog toys labeled "Chewy Vuitton" as opposed to the actual famous brand, Louis Vuitton).
[75] *See* Mattel, 296 F.3d at 901–03.

fame, and strong consumer-product association do not protect against infringement, then we run the risk of disincentivizing trademark registration in the first place, especially amongst indecisive circuits.

B. Reigning in Freedom of Speech

With *Matal* and *Iancu* having set the background for seminal First Amendment-trademark-mix cases, we might look to one of the *purposes* of trademark law: the prevention of unfair competition. This has come down to an economic game, one which Tabrez Ebrahim (a leading scholar in intellectual property law, entrepreneurship, and technology) argues is primarily resting on each party's ability to discover relevant information.[76] Such a low bar has opened the door for artificial intelligence technologies to cross the line into unfair business practices with limited, if any, liability for the use of trademarks of already-registered owners.

All that artificial intelligence technology inventors need to do, under *Rogers*, is to explain, under the low bar for the Test, that usage of any trademarks was a mere expression of themselves or their own works. By doing so, those creators will have free range to use trademarks which do not belong to them. This is especially true when applied to modern artificial intelligence, as trademarks are not just mere physical words; they can also be sounds, scents, and colors, all of which are creative and innovative measures used by artificial intelligence to communicate and respond to its user or users to help make purchases. While courts are universally skeptical to inhibit freedom of expression by objectively defining what *is* and *is not* a creative work of art, it would be prudent for courts moving forward to develop a new standard for artistic relevance, especially for emerging technologies.

C. The Expanding Breadth of Related Case Law

By tracing related case law, it is understandable that the crossover between First Amendment law and trademark jurisprudence is a tense intersection for the courts.

First, in *Thaler v. Hirshfield*, while artificial intelligence as a machine was found to not be considered an "inventor" under the Patent Act,[77] the danger of the *Rogers* test in trademark—as opposed to patent—

---

[76] *See* Tabrez Y. Ebrahim, *Automation & Predictive Analytics in Patent Prosecution: USPTO Implications & Policy*, 35 GA. ST. U.L. REV. 1185, 1188 (2019).
[77] *See* Thaler v. Hirshfield, 558 F. Supp. 3d 2238 (E.D. Va. 2021).

law does not require such artificial intelligence to *be* the inventor. Rather, the *Rogers* test merely requires that any inventor of the artificial intelligence itself can very likely escape liability by having that inventor's "invention" be "artistically relevant." Therefore, the danger lies in the label of "art," as inventors often find their artificial intelligence technologies to be their own creations; the technology itself does not have to be viewed as an "inventor." In application, the artistic relevance bar is so shockingly low that it just needs to be above zero.[78] Essentially, any plausible, artistic connection is acceptable, and a reasonable consumer should decide so for himself.[79]

Next, the term "explicitly misleading," which is similar to the "intention to deceive" in unfair competition law, actually has a very *high* standard.[80] This can be seen in *Gordon v. Drape*.[81] In that case, the plaintiff made honey badger memes and a card company made greeting cards using those exact same memes.[82] Those cards showed the popular theme of "honey badger not giving a ****," a pop culture phrase used by thousands of users of social media, including generating millions of views on YouTube.[83] The Ninth Circuit held that such printing of the memes was an artistic use designed by the card company, even though the only content of the card was the exact meme itself. The case was remanded for further proceedings, but it is of particular importance here because it *still* applied *Rogers*, making the standard for "explicitly misleading" even higher than it was initially thought to be.[84]

This case can be distinguished from the others, however, because there usually needs to be a very explicit reference—such as the words "sponsored by"—in order to be considered within the "misleading" category. It is not enough that one is simply using the trademark within the work. While the Ninth Circuit described that "[t]he *Rogers* test is not an automatic safe harbor for any minimally expressive work that copies someone else's mark," it simultaneously admitted that "on every prior

---

[78] E.S.S. Ent. 2000, Inc. v. Rock Star Videos, Inc., 547 F.3d 1095, 1100 (9th Cir. 2008). *See also* Brown v. Elec. Arts, Inc.,724 F.3d 1235 (9th Cir. 2013) (holding that videogame producer, Electronic Arts, Inc. did not infringe on famous professional football player James "Jim" Brown's character likeness in the *Madden NFL* games when it used his avatar, as it was artistically relevant and because the video games were expressive works that were entitled to protection under the First Amendment).
[79] Rock Star Videos, 547 F.3d at 1100–01.
[80] "Explicitly misleading" is a "heightened standard," as recently reaffirmed by the Ninth Circuit in Punchbowl, Inc. v. AJ Press, L.L.C., 2022 U.S. App. LEXIS 31398 (9th Cir. 2022).
[81] Gordon v. Drape Creative, Inc., 909 F.3d 257, 261 (9th Cir. 2018).
[82] *Id.* at 260–261.
[83] *Id.* at 261.
[84] *Id.*

occasion in which we have applied the test, we have found that it barred an infringement claim as a matter of law."[85] Thus, the Ninth Circuit itself admitted that use of the *Rogers* test as a defense continues to enjoy one win after another and could potentially "turn trademark law on its head."[86]

Even though the *Rogers* case is about film titles, the court there was willing to extend the Test to insulate use inside of the body of a work, not just its title.[87] This manifested in *University of Alabama Board of Trustees v. New Life Art*.[88]In that case, the University of Alabama sued an artist who painted convincing, life-like paintings of Alabama Football games. Alabama claimed that the artist was unfairly using its trade dress. [89] If the Alabama paintings had the logo *outside* of the frame, that may have been held to fit within the explicitly misleading framework, but the court held that such paintings fell under the *Rogers* test. This was because paintings were argued to be a sort of artistic work that are centrally recognized, even though the paintings were representational of a famous user's mark. This raises a question about what kinds of artistic uses really fall within the physical boundaries of art pieces and within the metaphorical universe of *Rogers*.

III. NEGATIVE IMPACTS ON UNDERLYING TRADEMARK PHILOSOPHIES & FUNCTIONS

A. Inequitable Incentives

Regardless of the type of infringement committed by artificial intelligence or the degree to which harm results from such infringement, the *Rogers* test should not operate as a winner-takes-all approach, as many courts have already admitted it does. Such a defense that nearly always comes out in favor of the defendant is simply inequitable.

Further, no scientist or inventor should be able to scapegoat infringement with such a sweeping defense. With a ready-made and seemingly "complete" defense available, this removes incentives for those owners to police their trademarks (a requirement for federal ownership), since they could likely claim this defense with no further

---

[85] *Id.*
[86] *Id.* at 270.
[87] Rogers v. Grimaldi, 875 F.2d 994, 1005 (2d Cir. 1989).
[88] Univ. of Ala. Bd. of Trs. v. New Life Art, Inc., 683 F.3d 1266 (11th Cir. 2012).
[89] *Id.*; *cf.* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992) (explaining that a secondary meaning requirement in trade case cases could have anticompetitive effects).

action.[90] It is this type of "legal thinking" that inspires and innovates the economy, but with a sort of "invincibility" defense, market checks cannot be placed on such innovators. This is similar to the process of filing a trademark as per section 15 of the Lanham Act for "incontestability." With section 15 incontestability, a trademark becomes more challenging to dispute as it essentially "earns" its way in with consumers through use and recognition.[91] With this "market incontestability" switched to the other party, however, there arises a strong disincentive for further trademark registration. Either way, the dangerous future of the *Rogers* test could create a powerful disincentive to registration on the Principal Register for all parties involved.

B. An Invasive Search Process

As of now, there are more trademarks in use in commerce than there have ever been.[92] This makes sense especially considering the steady and consistent growth in the American economy—more growth means more entrepreneurs who want intellectual property protection. As part of such innovation, artificial intelligence is used to conduct private trademark searches in order to reduce costs for searches otherwise done manually by individual consumers. This is the primary efficiency aimed at by the use of that intelligence—maximizing usage in the least amount of time and effort. Practically, artificial intelligence has become responsible for initial trademark search results and scanning the cost of searches regarding trademark selection, supply, and quality, all while focusing heavily on the demand-side of consumers.[93]

Customarily, a trademark word search in a database—namely the United States Patent and Trademark Office's ("USPTO") Trademark Electronic Search System (TESS)[94]—is a quite straightforward way to verify the existence of other registered marks. When looking for which trademarks have already been registered, trademarks in the TESS search-context have conventionally relied on character-based technology to find similar marks. This is especially interesting to note considering that trademark rights and protections have been cited as the most

---

[90] *See generally* McKenna, *supra* note 27, at 117, 139 (discussing the policing of marks that deceive the preferences of consumers).
[91] U.S. PAT. & TRADEMARK OFF.,*supra* note 18, at § 1605. .
[92] Katyal & Kesari, *supra* note 6, at 506.
[93] *See id.* at 510.
[94] *Id.* at 558.

important type of intellectual property protection.[95] With the introduction of artificial intelligence, however, trademark searches have been expanded to include phonetic analogies, synonyms, and related permutations of letters.[96] "Other approaches rely on a constellation of comparisons—such as automated similarity assessments of image/pixel, text, and content."[97] These categories all have the possibility of becoming labeled as "art," whether such art be framed as a creation, production, or composition, if for nothing but for the fact that computer coding is a form of an individual's creativity. This massive increase in ability to search for and advertise different trademarks, while impressive, simultaneously raises the risk of potential infringements.

Despite its convenience, artificial intelligence, as technologically advanced as it is and will continue to be, may not be able to distinguish between marks that truly are in use in commerce and those that are merely *claiming* use but are not actually used in commerce. For trademark examiners at the USPTO, it might then potentially consider a mark "dead" or "abandoned" if it is no longer being used in a clear fashion, even if artificial intelligence finds some usage in a unique form.

There are some things that simply cannot take the place of the human brain, such as the ability to search for a mark on TESS and see its registration status as in use or not. With a high chance for confusion between marks both in and not in actual use in commerce, it poses the question: why even make the distinction at all? To not do so might even open the possibility of free-riding activity or variations on the explicitly misleading standard, altering the entire trademark system that is supposed to be based around the opposite: distinctiveness.[98]

C. Artificial Intelligence as a Creationist: A Mark of Creation Itself

The creation itself, here the artificial intelligence, is the "trademark" at issue. It is no longer the inventor and his trademarked brand name, but widespread, popular intelligence, such as Apple's Siri or

---

[95] *See Trademarks, Copyright and Patents: Should Business Owners Really Care About IP?*, VARNUM (May 1, 2019), https://www.varnumlaw.com/newsroom-publications-trademarks-copyrights-and-patents-why-business-owners-should-care-about-ip ("A trademark is one of the most important business assets that a company will ever own because it identifies and distinguishes the company and its products/services in the marketplace from its competitors.").

[96] Katyal & Kesari, *supra* note 6, at 523.

[97] *Id.* at 524.

[98] *Id.* at 514. *See also* WORLD INTELL. PROP. ORG., *supra* note 1, at 5, 9.

Amazon's "Alexa," which might be able to be trademarked as an almost intermediary mark. A trademark is not limited to mere word choice, but the "packaging" of it, and the emotional bond it creates with the public.[99] Such "packaging" has the potential to be found false or misleading under Section 43(a) of the Lanham Act.[100] To hold this would mean that the aforementioned robot Sophia is seen as a mark itself, as it is considered "packaging."

If this "electronic personhood" is art itself, the creation of this quasi-"life" would be hard to challenge in court under traditional concepts of personhood.[101] "The government's recognition of Sophia (the robot) would create the front of mind connection needed for secondary meaning."[102] *Abercrombie* held that a mark categorized as generic still cannot receive protection, even if the mark proves to have secondary meaning.[103] Such recognition of artificial intelligence as beyond merely generic but also possessing the necessary secondary meaning tips the *Abercrombie* spectrum is favor of trademark protection. To have another "being" make the front of mind connection and therefore diminish the human function for source recognition between "human" and product, alters commercial impression, a discriminating factor of the *DuPont* analysis.[104] It logically follows that more and more trademarks would then enter the marketplace with the influx of more and more artificial intelligence in aspects of everyday life. The USPTO cannot, of course, register every single mark. "Because of these gaps, several private trademark search engines have emerged to supplement TESS, using machine learning to provide more thorough results."[105] Such action is circular, however, and we might be left, then, with a higher rate of registration refusals since the system would be inundated with so many more marks.

There may also begin to develop an overreliance on the conveniences of artificial intelligence, resulting in an inaccurate ability for consumers to utilize their rational judgments, particularly in distinguishing what is considered "art." Artificial intelligence-driven tools might contribute to false positives for likelihood of confusion determinations since the created technology might not be as sound, nor as fast, as human judgment calls, especially in the markets that a

---

[99] LALONDE & GILSON, *supra* note 29, at § 2A.01.
[100] *Id.* at § 7.02 n. 110.156.
[101] Rocha, *supra* note 35, at 129.
[102] *Id.* at 141.
[103] Abercrombie & Fitch Co. v. Hunting World, 537 F.2d 4, 9 (2d Cir. 1976).
[104] *In re* E. I. du Pont deNemours & Co., 476 F.2d 1357, 1361 (C.C.P.A. 1973).
[105] Katyal & Kesari, *supra* note 6, at 506.

consumer is already familiar with.[106] "Given the large number of marks that are *not* in use, but which remain registered or may be unregistered, there is also a risk that assessments may not reflect the reality of the existing marketplace."[107] Given that trademark law is based in laws aiming to prevent unfair competition in the *marketplace*, to run the risk of a misunderstood market would be detrimental to source identification—the end goal.

D. Confusing the Likelihood of Confusion

Another implication of the *Rogers* test in artificial intelligence is that the use of names, sources, or companies advertised through screens, new visual shopping experiences, and through voice recognition will undoubtedly cause confusion amongst consumers, and not just intellectual property confusion. Such multi-layered understandings of a mark and its source are a type of "signaling within advertising,"[108] which might even "surpass human judgment and performance."[109] This means that it would be difficult to know the true usage or livelihood of the presented marks in any given case. The District Court in *Rogers*, by contrast, held the relevance of "Ginger" in the movie title at issue was clear to the consumer on two levels. As explained by the court, "[f]irst, the title accurately refers to the fictionalized nicknames of the Film's two central characters. Second, the screenplay establishes the reference to Rogers and Astaire as the basis for the Film's characters' livelihood."[110] For these reasons, this was recognized as a known element of "modern culture."[111] However, it is a whole new challenge to jump from consumers' understanding of a movie title at face value versus replicated marks displayed through artificial intelligence. Surely, there are some individuals who would be able to meet that level of understanding, but it is a very lofty presumption to think all consumers would be able to have that type of knowledge already stored in their minds.

Next, consumers are likely to be confused—or concerned—by artificial intelligence automating partial (or even full) decisions for them and tailoring their purchasing decisions based on observed behaviors and services. In addition to likelihood of confusion and dilution, this has the potential to constitute a cause of action for blurring. "Blurring

---

[106] *Id.* at 529.
[107] *Id.* at 586 (emphasis added).
[108] *Id.* at 513.
[109] *Id.* at 586.
[110] Rogers v. Grimaldi, 695 F. Supp. 112, 120 (S.D.N.Y. 1988).
[111] *Id. See also* LALONDE & GILSON, *supra* note 29, at § 7.02 n. 45.71–45.73.

happens when a famous mark's distinctiveness is harmed because it becomes or is likely to become associated with a similar mark or trade name."[112] This is because the nature of artificial intelligence and machine learning is often wired to produce similar marks and trade names as per the user's request, as the purpose is to accurately provide various, closely related options for the consumer to choose from. [113]

With any type of artificial intelligence, machine-learning suggestions to the consumer might then be considered an almost "secondary liability." The American Bar Association has even explained that, while artificial intelligence tools and software have their advantages, they can also be used in the reverse to "infringe the rights of other trademark owners—thus opening up questions of machine volition and liability."[114]

E. The "Forgotten" Consumer

Because the purpose of the *Rogers* test is to protect the artistic freedom of expression of inventors and creators, there may be a move *away* from the context and emotion-driven component to trademark law, as the consumer may simply be left out of the process because the average consumer might not be considered the "average internet consumer."[115] "The reactions of a real-world consumer, so often alluded to in trademark doctrine, may be muted even further as a result."[116] This is particularly problematic because one of the main components required to register a trademark is that the mark has demonstrated that it has a distinct commercial impression upon consumers. Now, those consumers might have become "forgotten" since there is a much lesser need for human cognition in the product suggestion and purchasing process.[117]

One of the biggest setbacks with using artificial intelligence is that it "lacks the human ability to consider context . . . which may result in a higher, expanded prediction of likelihood of confusion."[118] This is even more so a risk considering that not all consumers, especially those in more mature generations who do not have as much technological

---

[112] *Trademark Dilution*, JUSTIA (Oct. 2022), https://perma.cc/76LV-HQ2P.
[113] Joiner, *supra* note 10.
[114] Katyal & Kesari, *supra* note 6, at 528; *see also Letter from American Bar Association - Intellectual Property Law Section to Secretary of Commerce for Intellectual Property & Director of the United States Patent and Trademark Office*, USPTO (July 14, 2020), https://perma.cc/TQ3C-Y7UT.
[115] *See* WORLD INTELL. PROP. ORG., *supra* note 1, at 10.
[116] Katyal & Kesari*, supra* note 6, at 586.
[117] WORLD INTELL. PROP. ORG., *supra* note 1, at 5.
[118] Katyal & Kesari*, supra* note 6, at 586.

exposure, will have the level of knowledge needed to decipher such advanced options—let alone what is "art" or not—given to them for purchase. This allows a greater possibility to deceive consumers with "strategically driven recommendations."[119]

The consumer would be left to decide what exactly he is looking at and what is actually being branded. This confusion can lead to misleading advertising, as exemplified in *Allen v. National Video, Inc.* There, the Court held that the Lanham Act was violated because of its prohibition on misleading advertising.[120] The issue of the case was a false designation of origin, which would otherwise mislead the consumer to associate a mark as stemming from the wrong party.[121] The defendant's sole purpose was to capitalize his profits based on a popularized image of a character's face.[122] The idea was to capitalize on that character's familiar name, face and 'reputation for artistic integrity' to boost sales of its movie rentals.[123] In *Rogers*, while the film at issue did not damper any reputation for sake of profit, it is plausible that when adding artificial intelligence as an additional layer to advertising, a consumer would be required to take purchasing decisions a bit more seriously with more considerations so as to avoid confusion or being misled, making sales and market innovation less efficient for consumers.

Moving forward, a balancing of the above interests should be kept in mind when assessing a case under a *Rogers* defense.

IV. MOVING FORWARD: THE "GENUINE ARTIFICIAL INTELLIGENCE MOTIVE" TEST

Courts have been applying the *Rogers* test defense for many years now, and it is still facing a circuit split, despite many suggestions for frameworks under which *Rogers* could adopt, namely commercial speech and fair use or right of publicity. As has been described, though, Rogers does not fit neatly within any of those frameworks—this is a unique legal matter in question, not answerable by mere *stare decisis*. An innovative solution is needed to fill the gap in the law

A. Failing—and Already Existing—Frameworks

---

[119] *Id.* at 529; WORLD INTELL. PROP. ORG., *supra* note 1, at 10, 12.
[120] Allen v. Nat'l Video, Inc., 610 F. Supp. 612 (S.D.N.Y. 1985).
[121] *Id.* at 625–26.
[122] *Id.* at 618.
[123] *Id.* at 617.

We must narrow the *Rogers* test because artificial intelligence creators must get proper legal protection for their inventions in the competitive marketplace of science, including a *lack* of protection for property that rightfully belongs to someone else (here, trademarks owned by others). Some may argue that artistic relevance is a category under First Amendment jurisprudence, and therefore, freedom of speech or commercial speech frameworks should apply. However, as held in *Rogers*, the Second Circuit did not consider this fitting under commercial speech because it would have needed its *primary* intention to be serving a commercial purpose.[124] The Second Circuit even stated, that for some, the distinction between art and commerce has been "blurred beyond recognition."[125]

While assuming good faith in the growth of artificial intelligence, intentional misleading of the public would be incredibly hard to prove, as liability would extend to such a profoundly high number of people who use that technology. WIPO foresees this problem, asking the probing question, "[w]hat if only [a] few brands are inserted into the AI system keeping the other brands?"[126] This could actually create an increased risk of false positives for "likelihood of confusion."[127] With third-party suppliers, keyword advertising, and automated processes, [128] the source identifying purpose of a trademark continues to dwindle in clarity. With courts now on high alert of the extremely low bar for artistic relevance as a defense, some courts have proposed a stricter look at the *DuPont* likelihood of confusion factors.[129] With a reliance on the traditional factors, a court using this stricter look would merely assume that *truly* expressive works will not cause confusion. In *Rogers*, the film at issue was not an "ordinary subject of commerce," a simple "commodity," or a mere piece of "merchandise," but solely a piece of art.[130] Basically, this assumes the belief that a form of art should be so evident that it is *only* art, and that it is serves a different purpose from the trademark. In that instance, a court would pay no special attention to First Amendment concerns, but, rather, would stick exclusively to analyzing any potential

---

[124] Rogers v. Grimaldi, 695 F. Supp. 112, 119–120 (S.D.N.Y. 1988).
[125] *Id.* at 120.
[126] WORLD INTELL. PROP. ORG., *supra* note 1, at 14.
[127] Katyal & Kesari, *supra* note 6, at 586.
[128] *See Trade Marks: Cosmetic Warriors Ltd. and Lush Ltd. v. Amazon.co.uk Ltd.*, FIELDFISHER (Dec. 5, 2014), https://www.fieldfisher.com/en/insights/trade-marks-cosmetic-warriors-ltd-and-lush-ltd-v-amazoncouk-ltd.; WORLD INTELL. PROP. ORG., *supra* note 1, at 16.
[129] *In re* E. I. du Pont deNemours & Co., 476 F.2d 1357, 1361 (C.C.P.A. 1973).
[130] Rogers v. Grimaldi, 695 F. Supp. 112, 124 (S.D.N.Y. 1988).

confusion under *DuPont*.[131] This might be interpreted as being more along the lines of a right to publicity defense, but in a Third Circuit case that applied *Rogers*, the court held, the right of publicity does not implicate the potential for consumer confusion."[132] This type of analysis, then, logically leads to the opposite purpose of a mark—source identification—while also proving contrary to the purpose of landmark cases *Matal* and *Iancu*, where, as aforementioned, the Court held that First Amendment concerns were almost *superior* to trademark rights.[133]

Thus, we must look elsewhere for a new *Rogers* test framework.

B. The New Approach

The circuit split on the *Rogers* test demands answers. While many have been proposed, the most promising appears to be what is deemed the "Genuine Artistic Motive" test, a product of a Colorado district court, the first district court to explicitly reject a *Rogers* defense.[134]

That court, which belongs to the Tenth Circuit, created its own test for artistic relevance in 2020 when it rejected a *Rogers* application in *Stouffer v. National Geographic Partners*.[135] The case had a similar fact pattern to *Rogers*—a producer of a nature documentary series claimed that a National Geographic nature documentary, which was made after the producer's documentary, infringed his trademark rights by use of the National Geographic documentary's title, claiming a likelihood of confusion, unfair competition, and deceptive trade practices. The court, while having agreed with the underlying theory of the *Rogers* test, ultimately created its own test.[136]

The new six-prong test, aptly named the "Genuine Artistic Motive" test, included the following factors:

- Whether the senior and junior users use the mark to identify the same or similar kind of goods or services;
- The extent to which the junior user has added expressive content to the work beyond the mark itself;

---

[131] *In re* E. I. du Pont, 476 F.2d at 1361.
[132] Hart v. Elec. Arts, Inc., 717 F.3d 141, 158 (3d Cir. 2012).
[133] *Matal v. Tam*, 137 U.S. 1744 (2017); *Iancu v. Brunetti*, 139 U.S. 2294 (2019).
[134] Practical Law Intellectual Property & Technology, *"Genuine Artistic Motive" Test, Not Rogers Test, Applicable For Balancing Trademark And First Amendment Rights: D. Colo.*, THOMAS REUTERS PRACTICAL LAW (May 15, 2020), https://us.practicallaw.thomsonreuters.com/w-025-5350.
[135] Hervey, *supra* note 36; Stouffer v. Nat'l Geographic Partners, L.L.C., 460 F. Supp. 3d 1133 (D. Colo. 2020).
[136] *Stouffer*, 460 F. Supp. 3d at 1140.

- Whether the timing of the junior user's use suggests a motive to capitalize on popularity of the senior user's mark;
- ***How*** the mark is artistically related to the underlying work, service, or product;
- Whether the junior user has made any public statement or engaged in any public conduct that suggests a non-artistic motive; and
- Whether the junior user has made any statement in private or engaged in any conduct in private that suggests a non-artistic motive.[137]

Despite this new test, the outcome was the same as if *Rogers* had applied—National Geographic's title was considered its First Amendment expressive use, meaning it was not liable for infringement. The *Stouffer* court's reasoning provides a glimpse into the danger of the *Rogers* test moving forward. Citing the outcome in *Gordon*, the court reasoned that, the "*Rogers* test, taken at face value, essentially destroyed the value of the Honey Badger mark—and perhaps many other marks, if parties are willing to be sued and defend themselves under the *Rogers* test."[138] This does not even take into account the added potential for infringement on behalf of emerging technologies that can more readily display marks at an increased rate to consumers. Because of this, the "Genuine Artistic Motive" test must incorporate technological considerations for artificial intelligence under a "Genuine Artificial Intelligence Motive" test.

1. Alternative Avenues

With the "Genuine Artificial Intelligence Motive" test, there might be potential for an "alternative avenues" prong to take foot. This would pose a question to the creator, inventor, or artist seeking to use a trademark, asking him if he could make that exact same artistic and communicative point that his mark proposes to portray without actually using that mark. Basically, this would require an alternative use to express the idea of an artistic work but without incorporating an already-registered trademark to make that same expression.

---

[137] *Id.*
[138] *Id.* at 1142 (citing Gordon v. Drape Creative, Inc., 909 F.3d 257, 268–71 (9th Cir. 2018)).

To get this off the ground, courts might visit *Stouffer*'s "Genuine Artistic Motive" test to assess the intentions behind such use.[139] When analyzing the factor's above, courts would weigh the appropriateness of the junior user's subjective motives behind each prong.[140] This would mean that expressive works could not be protected from infringement claims if there are sufficient alternative means for an artist to convey his or her idea to the general consuming public. This type of test would fail, however, to give latitude for creativity and free expression.

C. A Final Suggestion for Artificial Intelligence

Though in *Stouffer*, the court rejected the notion that *Rogers* could strike an appropriate balance between freedom of speech and trademark rights, moving forward, courts might resort to a balancing of *harms* analysis instead, in which the potential harm to one party and harm to the public interest is considered in equity.[141] There might be a temptation, then, for courts to look to the framework for commercial speech, but with a caveat for the sophistication of consumers under *DuPont*.[142] The idea is that more sophisticated consumers will be able to distinguish between particular goods and services as marketed by the artificial intelligence and their respective sources, while other, less-technologically savvy consumers in that market might not be able to do so. This would be the equitable purpose of the "Genuine Artificial Intelligence Motive" test.

In addressing this factor, courts might consider the generational age differences between consumers, as younger consumers might be more in touch with the latest technologies. Thus, they would be able to more readily identify which marks the artificial intelligence is advertising, and ideally, more attune to what might be infringement or dilution of those marks.[143] Courts might then suggest that the USPTO invest in training some of these youthful consumers to "monitor" new artificial intelligence technologies to discern the genuine nature of "artistically relevant" functions and secondary liability of marks used for commercial exploitation. Without this, there is a high potential for the

---

[139] *Id.* at 1140, 1145.
[140] *Id.*
[141] Stouffer v. Nat'l Geographic Partners, L.L.C., 400 F. Supp. 3d 1161, 1177–80 (D. Colo. 2019).
[142] *In re* E. I. du Pont deNemours & Co., 476 F.2d 1357, 1361 (C.C.P.A. 1973).
[143] *See generally* Katyal & Kesari, *supra* note 6, at 515; *see* WORLD INTELL. PROP. ORG., *supra* note 1.

enabling of free-riding activity.[144] The *Stouffer* court agreed with this notion as it stated, "it seems that anyone can use a trademark, *even to sell the same good or service for which the trademark was granted*, if the good or service can be deemed 'art.'"[145]

Weighing the freedom of expression and intellectual property protection is not an uncommon balancing test for the courts, especially after *Matal* and *Iancu*.[146] In fact, both the Eighth and the Tenth Circuits have applied balancing tests to cases concerning *Rogers*, in favor of a "flexible, case-by-case approach."[147] While this might be sustainable in the short-term, the "Genuine Artificial Intelligence Motive" test is the best answer in the long term because there does not seem to be any movement so far, but only more confusion, from both a legal *and* a consumer standpoint.

CONCLUSION

Overall, artificial intelligence as artistically relevant under the *Rogers* test will likely become increasingly difficult to govern, monitor, and regulate. Since *Rogers* has been adopted more and more over the last two decades, courts must address its future application in terms of how broad the law is willing to go to protect both artistic expression in technologies and intellectual property at the expense of one another, ideally through the "Genuine Artificial Intelligence Motive" test. Otherwise, the United States Patent and Trademark Office simply will not have enough bodies to keep up with the necessary trademark prosecution and protection of already-registered trademarks. As courts grapple with these new and emerging technologies, we are left with urgency to find scholars, judges, and scientists who can navigate where artificial intelligence meets artistic relevance. "*Roger*" that!

---

[144] Katyal & Kesari, *supra* note 6, at 586.
[145] *Stouffer*, 460 F. Supp 3d at 1142.
[146] *Matal v. Tam*, 137 U.S. 1744 (2017); *Iancu v. Brunetti*, 139 U.S. 2294 (2019).
[147] Keller v. Elec. Arts Inc., 724 F.3d 1268, 1282 (9th Cir. 2013).