Data as Likeness

ZAHRA TAKHSHID*

Artificial intelligence (AI) and data collection practices pose an ongoing threat to consumers' privacy. But plaintiffs have struggled to articulate privacy harms associated with data collection in a way that would give them standing to sue. This is a particularly pressing issue given the advances in generative AI and the unauthorized uses of individuals' personal and biometric data.

This Article revisits the privacy tort of appropriation of likeness and argues that when data are conceptualized as likeness, this tort offers a unique opportunity to protect against the unauthorized collection and use of personal data. Grounding its argument in the historical evolution of the tort of appropriation, this Article contends that an individual's personal data are an aspect of a person's unique digital identity, mostly used by third parties in a data-driven world, which should be covered by this tort.

Conceptualizing unauthorized personal data collection in this manner underscores the evolving nature of the common law of torts in recognizing new forms of harms. It offers a solution for the current gridlock on data protection measures and the unauthorized use of one's data in emerging generative AI technologies such as deep voice. Recent Supreme Court decisions have insisted that privacy victims must show some form of concrete harm to achieve constitutional standing. Accordingly, employing the privacy tort of appropriation of likeness and recognizing the concept of digital persona allow plaintiffs to establish standing by identifying a close historical or common law analogue for their asserted privacy injury. Lastly, similar to other privacy torts, this approach can survive First Amendment objections.

TABLE OF CONTENTS

* Assistant Professor of Law, University of Denver Sturm College of Law, Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. For helpful comments and conversations, I am grateful to Intellectual Property Law Conference (IPLC) participants at Stanford Law School (particularly Jennifer Rothman, Rebecca Tushnet, and Zahr Z. Zaid), colleagues at Privacy Law Scholars Conference (PLSC) 2022 (special thanks to Jason Schmaltz, Margot Kaminski, Felix Wu, and Jessica Silbey), and participants at Governance of Emerging Technologies and Science, Arizona State University College of Law. This Article also benefited from comments at faculty workshops at the University of Denver Sturm College of Law. Many thanks to K. K. DuVivier, John Goldberg, Benjamin Zipursky, Nancy Leong, Laurent Sacharoff, Bernard Chao, and Viva Moffat. Special thanks to Garrett Ian Littenberg and Hannah Le for excellent research assistance.

INTRODUCTION

The average cell phone application (app) has six embedded trackers.[1] While data-driven marketing is not a new phenomenon,[2] with the advent of Big Data[3] and generative AI,[4] the understanding of what personalization means for consumers has rapidly and radically changed. Today, data-driven products based on individuals' personal behaviors are everywhere. Some notable examples are wearable AI devices telling you when you should see a doctor,[5] smart fridges knowing what your next grocery shopping list should include,[6] apps on your phone collecting your snore

1. APPLE, A DAY IN THE LIFE OF YOUR DATA: A FATHER-DAUGHTER DAY AT THE PLAYGROUND 3 (2021), https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf [https://perma.cc/DQS6-HDZS] ("Trackers are often embedded in third-party code that helps developers build their apps. By including trackers, developers also allow third parties to collect and link data you have shared with them across different apps and with other data that has been collected about you.").

2. For instance, Facebook unveiled its ad model in 2007. *See Facebook Unveils Facebook Ads*, META (Nov. 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/ [https://perma.cc/7KUG-ZPLE].

3. "'Big Data' refers to the massive amounts of digital information companies and governments collect about human beings and our environment." CLOUD SEC. ALL., EXPANDED TOP TEN BIG DATA SECURITY AND PRIVACY CHALLENGES 5 (2013), https://cloudsecurityalliance.org/artifacts/expanded-top-ten-big-data-security-and-privacy-challenges/ [https://perma.cc/2Q74-3CDP].

4. "Generative AI refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on." Kim Martineau, *What Is Generative AI?*, IBM: RSCH. BLOG (Apr. 20, 2023), https://research.ibm.com/blog/what-is-generative-AI [https://perma.cc/ZQL6-VMHD].

5. *See, e.g.*, Bertalan Mesko, *Feeling Sick? There's an App for That! – The Big Symptom Checker Review*, MED. FUTURIST (Apr. 11, 2019), https://medicalfuturist.com/the-big-symptom-checker-review/ [https://perma.cc/XV7U-JQQY]. For more on the privacy challenges of wearable AI devices, see Zahra Takhshid, *Wearable AI, Bystander Notice, and the Question of Privacy Frictions*, 104 B.U. L. REV. (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693396.

6. *See, e.g.*, Joe Fassler, *Is Your Smart Fridge Spying on You?*, COUNTER (Mar. 16, 2017, 7:49 PM), https://thecounter.org/smart-fridge-spying/ [https://perma.cc/N7TJ-B7ZJ]; *see also* Alex J. Rouhandeh, *How Cyber Thieves Use Your Smart Fridge as Door to Your Data*, NEWSWEEK (June 23, 2021, 4:00 PM), https://www.newsweek.com/how-cyber-thieves-use-your-smart-fridge-door-your-data-1603488 [https://perma.cc/6R8A-2SE7] (noting that a smart fridge is "the perfect site for [an] initial attack" by cyber thieves).

sounds to generate a personalized sleep cycle,[7] and websites that know when you are pregnant.[8]

Facial recognition technologies and revelations arising from recent litigation involving the facial recognition company Clearview AI have further heightened the concerns about collection of personal biometric data.[9] The expansion of the metaverse[10] and creation of avatars for digital spaces have also instigated intrusive data collection practices.[11] For example, "spending 20 minutes in a VR simulation leaves just under 2 million unique recordings of body language."[12] More recently, advances in generative AI, such as the ability to copy someone's voice, or create a similar version of it, have alarmed many.[13]

---

7. *See, e.g.*, *Privacy Policy*, SLEEP CYCLE, https://www.sleepcycle.com/privacy-policy-2021/ [https://perma.cc/4VGX-DMG6] (last visited Mar. 13, 2024) ("When using the Sleep Cycle app . . . some personal data will be collected through your device's accelerometer (such as your movements), microphone (such as snoring or other noises), camera (pulse), or device location (for weather and sleep location statistics), and some personal data will be derived (such as sleep efficiency and sleep quality).").

8. *See, e.g.*, Brian Contreras, *How Instagram and TikTok Prey on Pregnant Women's Worst Fears*, L.A. TIMES (May 25, 2022, 5:00 AM), https://www.latimes.com/business/technology/story/2022-05-25/for-pregnant-women-the-internet-can-be-a-nightmare; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=1d9339d06668; NEIL RICHARDS, WHY PRIVACY MATTERS 35–37 (2021) (discussing Target's data-based "pregnancy marketing").

9. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. "Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals." *What Is Biometrics? How Is It Used in Security?*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/biometrics [https://perma.cc/T4ZP-ALXG] (last visited Mar. 13, 2024). Personal biometric data can include "fingerprint mapping, facial recognition, and retina scans." *Id.* The ACLU settled its case with Clearview AI based on the Illinois comprehensive biometric data law; the "settlement require[d] Clearview to maintain an opt-out request form, allowing IL residents to upload a photo to ensure their faceprints will be blocked from appearing in their search results, including searches by police." ACLU (@ACLU), X (May 9, 2022, 1:12 PM), https://twitter.com/ACLU/status/1523712577389629440 [https://perma.cc/9BRY-RCRF?type=image].

10. "The metaverse is understood to be an immersive virtual world serving as the locus for all forms of work, education, and entertainment experiences." Jon M. Garon, *Legal Implications of a Ubiquitous Metaverse and a Web3 Future*, 106 MARQ. L. REV. 163, 163 (2022).

11. *See, e.g.*, Jesse Lake, *Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection*, 69 EMORY L.J. 833, 845–48 (2020); Yvonne Lau, *You'll Soon Be Able to Put Your Metaverse Avatar to Work—and Make Actual Money from It*, FORTUNE (Feb. 7, 2022, 7:00 PM), https://fortune.com/2022/02/07/metaverse-avatar-work-make-money-nft/.

12. Jeremy Bailenson, *Protecting Nonverbal Data Tracked in Virtual Reality*, J. AM. MED. ASS'N PEDIATRICS, Aug. 6, 2018, at E1, E1. "VR" stands for "virtual reality." Virtual reality is defined as "an artificial environment which is experienced through sensory stimuli (such as sights and sounds) provided by a computer and in which one's actions partially determine what happens in the environment." *Virtual Reality*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/virtual%20reality [https://perma.cc/62P2-LBLC] (last visited Mar. 13, 2024).

13. *See* Pranshu Verma & Will Oremus, *AI Voice Clones Mimic Politicians and Celebrities, Reshaping Reality*, WASH. POST (Oct. 15, 2023, 12:28 AM), https://www.washingtonpost.com/technology/2023/10/13/ai-voice-cloning-deepfakes/; Tripp Mickle, *Scarlett Johansson Said No, but OpenAI's Virtual Assistant Sounds Just Like Her*, N.Y. TIMES (May 20, 2024), https://www.nytimes.com/2024/05/20/technology/scarlett-johannson-openai-voice.html.

To address some of the modern digital privacy concerns and the lack of a comprehensive federal privacy law,[14] several states, including California,[15] Colorado,[16] Connecticut,[17] Virginia,[18] and Utah,[19] have passed consumer privacy acts, and a number of other states are in the process of regulating data and privacy at the state level.[20] However, as of now, most data collected and used in the United States remain unregulated, and when dealing with corporate use of personal data, consumers are bound to the boilerplate terms of private privacy policies, leading scholars to describe the American approach to privacy as "sectoral."[21]

Nevertheless, common law privacy torts have traditionally offered different forms of privacy protections. The four privacy torts widely recognized in most U.S. states,[22] outlined by Dean William Prosser in 1960, are:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.

---

14. A bipartisan federal privacy bill (The American Privacy Rights Act) was introduced in April of 2024, but the fate of it remains to be seen. Cristiano Lima-Strong, *Lawmakers Unveil Sprawling Plan to Expand Online Privacy Protections* (Apr. 7, 2024, 4:00 PM), https://www.washingtonpost.com/technology/2024/04/07/congress-privacy-deal-cantwell-rodgers/.

15. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199.100.

16. Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1313.

17. Consumer Data Privacy and Online Monitoring, CONN. GEN. STAT. §§ 42-515 to -525.

18. Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -585.

19. Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101 to -404.

20. *See* Andrew Folks, *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PROS. (Mar. 1, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker [https://perma.cc/RV7U-MATP]. For federal bills introduced in Congress, see, for example, the Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021) and the Digital Accountability and Transparency to Advance (DATA) Privacy Act, H.R. 5807, 117th Cong. (2021).

21. *See, e.g.*, RICHARDS, *supra* note 8, at 53. The sectoral nature of privacy laws in America means that "[t]he United States . . . doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix" of disparate federal and state laws. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/. For examples of federal laws contributing to the sectoral nature of privacy in the United States, see 42 U.S.C. § 1320d and 15 U.S.C. § 6502. For an exploration of the Children's Online Privacy Protection Act of 1998 (COPPA), see generally Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417 (2023).

22. *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1888–90, 1904 (2010) ("Today, due in large part to Prosser's influence, his 'complex' of four torts is widely accepted and recognized by almost every state." (citing ROBERT M. O'NEIL, THE FIRST AMENDMENT AND CIVIL LIABILITY 77 (2001))). However, due to their common law nature, and at times statutory companions, their scope and requirements may differ from one state to the other. *See* Jennifer E. Rothman, *Navigating the Identity Thicket: Trademark's Lost Theory of Personality, the Right of Publicity, and Preemption*, 135 HARV. L. REV. 1271, 1279 (2022) ("State publicity laws vary widely, with states making wildly disparate decisions about who can bring publicity claims and under what circumstances."); *Right of Publicity State-by-State*, ROTHMAN'S ROADMAP TO RIGHT PUBLICITY, https://rightofpublicityroadmap.com [https://perma.cc/895C-A5TU] (last visited Mar. 13, 2024) (an online guide to state right of publicity laws).

4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[23]

However, with modern data privacy challenges, there has been a decline in the relevance of these traditional torts.[24] Experts note that "[b]ecause courts cling rigidly to the elements of the privacy torts as set forth in the Restatement, the privacy torts have little application to contemporary privacy issues," including "the collection, use, and disclosure of personal data."[25]

Professor Anita Allen describes several reasons for the unpopularity of common law privacy in the eyes of contemporary critics. To many, as she notes, these torts are: "(1) inconsistent in principle with free speech and press; (2) duplicative of other torts such as trespass, defamation or infliction of emotional distress; or (3) impractical, unwanted, and old fashioned in the age of computer, internet, and electronic technology."[26]

---

23. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

24. *See* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357, 357 (2011) ("[P]rivacy in the age of information and social media requires new strategies and new legal tools. Some of these strategies might include tort privacy as presently understood, but others require new approaches. These approaches can take either a broader look at tort privacy, including new torts and new theories of injury beyond emotional harm, or they can include new conceptions of privacy altogether, such as confidentiality law."); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1827 (2010) ("[A]ppropriation claims are also insufficient to protect the rights of individuals harmed by database leaks. Appropriation claims arise when a defendant uses for his own benefit the name or likeness of another. In leaking sensitive personal information, database operators do not use plaintiffs' name or image for their commercial advantage. Instead, database operators fail to secure sensitive personal information from criminals. Appropriation claims simply have no application to database operators who leak sensitive personal information to identity thieves." (footnotes omitted)). *See generally* Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555 (2021) (arguing for reliance on unjust enrichment); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (arguing that data privacy protection requires autonomy); Eugene Volokh, *Tort Law vs. Privacy*, 114 COLUM. L. REV. 879 (2014) (arguing that tort law can "diminish" privacy).

25. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 810 (2022). For examples of a recent trend in scholarship proposing new torts beyond the traditional four common law privacy torts, see Zahra Takhshid, *Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort*, 68 BUFF. L. REV. 139, 182–90 (2020); Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 69 (2021) [hereinafter Solove & Citron, *Standing and Privacy*], https://www.bu.edu/bulawreview/files/2021/07/SOLOVE-CITRON-2.pdf [https://perma.cc/3WRZ-PLX9]; Julia Keller, *Eavesdropping: The Forgotten Public Nuisance in the Age of Alexa*, 77 VAND. L. REV. 169, 171 (2024); Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 449–60 (2018); and Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756–73 (2018)).

26. Anita L. Allen, *Natural Law, Slavery, and the Right to Privacy Tort*, 81 FORDHAM L. REV. 1187, 1189–90, 1190 n.17 (2012) (footnotes omitted) ("[F]urther clouding the incoherent development [of the privacy torts] is the fact that privacy expectations and norms are constantly challenged by technology. . . . [The] conventional view of privacy is inapplicable and misplaced in cyberspace, where there are no physical spaces or clear boundaries delineating behavior and propriety." (alternations and omission in original) (quoting Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 11–12 (2007))).

This unpopularity has not stopped plaintiffs from relying on privacy torts, albeit in addition to other causes of action for their digital privacy grievances. On occasions where plaintiffs asserted the commission of privacy torts for the unauthorized use of data by third parties, they cited to, for the most part, the tort of intrusion upon seclusion.[27] However, for reasons this Article will illustrate, that strategy has not been successful.[28] Instead, this Article argues that there is room to benefit from the tort of appropriation of name and likeness.

This Article asserts that emerging digital privacy claims can be best conceptualized under the rubric of the appropriation tort's protection of persona by considering data as *likeness*. To accomplish that, common law courts must recognize the expansion of what constitutes an individual's persona for the purpose of this tort. In essence, this Article argues, the new wave of digital privacy concerns is about appropriation of one's likeness in its digital form, or what should be called digital persona. Our digital persona or likeness is our personal data—the modern aspect of identity that third parties are increasingly using for their own benefit without authorization.

This is not a radical argument. The tort of appropriation has expanded and grown in the past. In its early years, the tort was understood to be concerned with the misuse of one's name or image. Over time, courts began to recognize new aspects of one's identity, with what is now commonly referred to as the right of publicity.[29] Later, courts expanded the scope of this tort and ruled that voice too can be part of one's likeness.[30] In its evolution, courts also stated that a look-alike robot that resembled a person could trigger the appropriation tort.[31] Indeed, "a broader concept [of a person's likeness] arose over time, one often referred to as 'persona.' Liability for using someone's persona is much broader than liability for using a person's name or likeness because it encompasses any use—including the mere evocation—of that person's identity."[32]

But today, our voices and personas can be used in a different way. A filmmaker or an advertising company does not need to hire a backup singer to mimic a singer's voice.[33] Using generative AI and deep voice, "a deepfake [AI-based]

27. *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 597 (9th Cir. 2020); *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 267 (3d Cir. 2016); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 133 (3d Cir. 2015); Hubbard v. Google LLC, 546 F. Supp. 3d 986, 990 (N.D. Cal. 2021); New Mexico *ex rel*. Balderas v. Google, LLC, 489 F. Supp. 3d 1254, 1256 (D.N.M. 2020).

28. *See, e.g.*, *In re Google Inc.*, 806 F.3d at 145; *Hubbard*, 546 F. Supp. 3d at 993–94; *Balderas*, 489 F. Supp. 3d at 1263–64.

29. *See* Robert C. Post & Jennifer E. Rothman, *The First Amendment and the Right(s) of Publicity*, 130 YALE L.J. 86, 93 (2020).

30. *See* Midler v. Ford Motor Co., 849 F.2d 460, 463 (9th Cir. 1988).

31. *See* White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1399 (9th Cir. 1992).

32. JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 89 (2018).

33. *See Midler*, 849 F.2d at 461, 463 (extending the protection of likeness to include voice when Midler sued under the appropriation tort after an advertising agency hired one of her backup singers to mimic her voice in a commercial for Ford Motor Co.).

technology that creates synthetic voices,"[34] a filmmaker can simply use a synthetic voice cloning their desired person's voice to read a script.[35] The tort of appropriation can successfully address this use of likeness, including the scams and unwanted consequences of generative AI and deepfake technology[36] that we face today.[37]

Consider another example: the collection and use of an individual's geolocation data. Indeed, these data are one of the most sought-after aspects of an individual's personal data.[38] Individual data can be aggregated to create a disquietingly accurate picture of that person's identity. For example, scholars have shown that:

> Muslims can be identified with a high degree of accuracy from geolocation data that reveals the rhythm of daily ritual practices, such as in the case of taxi drivers who make regular pauses in their trips at prayer times, which raises issues of heightened surveillance, incorrect classification of Muslim populations and governmental and economic discrimination.[39]

Such sensitive information in the hands of the wrong people can be very troubling, especially for minority community members. Recent Federal Trade Commission (FTC) lawsuits concerning the sale of location data under consumer protection law underscore this ongoing problem.[40] Tort law can intervene by offering a private right of action.

---

34. Yeajun Kang, Wonwoong Kim, Sejin Lim, Hyunji Kim & Hwajeong Seo, *DeepDetection: Privacy-Enhanced Deep Voice Detection and User Authentication for Preventing Voice Phishing*, APPLIED SCIS., Nov. 2022, at 1, 1.

35. Anthony Bourdain's voice was brought to life in a documentary titled *Roadrunner: A Film About Anthony Bourdain* using AI-generated voice. *See* Helen Rosner, *The Ethics of a Deepfake Anthony Bourdain Voice*, NEW YORKER (July 17, 2021), https://www.newyorker.com/culture/annals-of-gastronomy/the-ethics-of-a-deepfake-anthony-bourdain-voice.

36. "Deepfakes use AI to generate completely new video or audio, with the end goal of portraying something that didn't actually occur in reality. The term . . . comes from the underlying technology — deep learning algorithms — which teach themselves to solve problems with large sets of data . . . ." Dave Johnson & Alexander Johnson, *What Are Deepfakes? How Fake AI-Powered Audio and Video Warps Our Perception of Reality*, BUS. INSIDER (June 15, 2023, 10:58 AM), https://www.businessinsider.com/guides/tech/what-is-deepfake.

37. *See* Jesse Damiani, *A Voice Deepfake Was Used to Scam a CEO Out of $243,000*, FORBES (Sept. 3, 2019, 4:42 PM), https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=284d2ce42241.

38. *See* Danielle Citron, *BEWARE: The Dangers of Location Data*, FORBES (Dec. 24, 2014, 3:04 PM), https://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data/?sh=5a6b5bf243cb.

39. Mohammad Yaqub Chaudhary, *Initial Considerations for Islamic Digital Ethics*, 33 PHIL. & TECH. 639, 640 (2020) (citing Lanah Kammourieh, Thomas Baar, Jos Berens, Emmanuel Letouzé, Julia Manske, John Palmer, David Sangokoya & Patrick Vinck, *Group Privacy in the Age of Big Data*, *in* GROUP PRIVACY: NEW CHALLENGES OF DATA TECHNOLOGIES 37, 47 (Linnet Taylor et al. eds., 2017)).

40. *See* Press Release, FTC, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other [https://perma.cc/EL85-BUXW].

For William Prosser, who identified the concept of a tort of appropriation, the tort of appropriation was "the exploitation of attributes of the plaintiff's identity."[41] In his view, it was not the plaintiff's name itself that was the subject of this tort, but instead was "the plaintiff's name as a symbol of his identity . . . and not his name as a mere name."[42] It is thus long overdue for courts to reevaluate the meaning of persona and likeness in a data-driven world to include personal data, confined to personally identifiable information (PII), as an aspect of a person's identity and likeness. Our personal data are part of what constitute our modern digital identity.

We can see similar attempts at reviving this tort for the digital age: Plaintiffs are invoking the appropriation tort in contemporary cases against facial recognition companies,[43] and a minority of scholars are advocating for the use of privacy torts to address concerns with facial recognition technologies that use our biometric data.[44] New York, which has a statutory right of publicity, has expanded its right of publicity to include "digital replicas" to address some of the challenges associated with digital identity and the growing deepfake technologies, albeit in a narrow fashion.[45]

There are theoretical and practical benefits to adopting this approach. Scholars have laid out different theoretical approaches for privacy, justifying digital and information privacy in particular.[46] Two of the most popular approaches involve a right to control and a right to dignity.[47] Data as likeness can encompass both the

41. Prosser, *supra* note 23, at 401.

42. *Id.* at 403.

43. *See, e.g.*, *In re* Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1128 (N.D. Ill. 2022); Renderos v. Clearview AI, Inc., No. RG21096898, 2022 WL 17326440, at *1–2 (Cal. Super. Nov. 18, 2022). I discuss these cases in depth in Part III.

44. *See, e.g.*, Jason M. Schultz, *The Right of Publicity: A New Framework for Regulating Facial Recognition*, 88 BROOK. L. REV. 1039, 1050–63 (2023).

45. *See* N.Y. CIV. RIGHTS LAW § 50-f. The law only protects "deceased performer[s]." *Id.* § 50-f(a). According to the law:

> "[D]igital replica" means a newly created, original, computer-generated, electronic performance by an individual in a separate and newly created, original expressive sound recording or audiovisual work in which the individual did not actually perform, that is so realistic that a reasonable observer would believe it is a performance by the individual being portrayed and no other individual. A digital replica does not include the electronic reproduction, computer generated or other digital remastering of an expressive sound recording or audiovisual work consisting of an individual's original or recorded performance, nor the making or duplication of another recording that consists entirely of the independent fixation of other sounds, even if such sounds imitate or simulate the voice of the individual.

Id. § 50-f(c). A separate "[p]rivate right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual" has also been passed to protect "depicted individual[s]" who are the subject of a deepfake containing "sexually explicit material." *Id.* § 52-c.

46. *See* Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1905 (2013). Privacy "protects the situated practices of boundary management through which the capacity for self-determination develops." *Id.* Another commentator notes, "[T]o act with dignity is to present aspects of oneself to others in a selective manner, that is, to reveal information about oneself to different individuals, in different contexts, in accord with one's considered convictions about the appropriateness of doing so." David Matheson, *Dignity and Selective Self-Presentation*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 319, 327 (Ian Kerr et al. eds., 2009).

47. *See* Takhshid, *supra* note 25, at 177–79.

dignitary interest advocated for digital privacy protection and the proprietary interest in privacy as control theories. Professor Robert C. Post and Professor Jennifer E. Rothman have identified four interests at the heart of the appropriation tort: "the value of a plaintiff's performance, the commercial value of a plaintiff's identity, the dignity of a plaintiff, or the autonomous personality of a plaintiff,"[48] what they call the right of control.[49] The encompassing nature of the appropriation tort thus allows for its compatibility with different privacy theories.

Practical efficiencies of data as likeness are also important. First, relying on the appropriation tort solves the contested issue of a cognizable harm. When arguing for the violation of an appropriation tort in most states, one does not need to prove any distinct harm, such as financial or emotional injury, other than breaching what constitutes the tort.[50] Next, the tort is triggered not only if the likeness is identified, but also if the likeness is identifiable. This means that one can breach this tort even when, for example, the person's image is not identified and no face has been shown.[51] As this Article illustrates, this precedent can address the modern use of identifiable data versus identified data.[52] Lastly, this expansion is a strategic move in light of the Supreme Court's decision in *TransUnion LLC v. Ramirez* and its emphasis on a historical linkage to modern-day harms in order to satisfy the Article III standing requirement.[53]

This Article proceeds in three Parts: Part I briefly outlines the emergence of privacy common law torts and their theoretical dignitary roots. Part II turns to the evolution and specificities of the appropriation tort and right of publicity, including the protection of voice, reference to one's identity (such as robots and look-alikes), and the identifiable characteristics requirement of the tort. This sets the stage for expanding persona. Part III redefines the appropriation tort's concept of likeness and persona to encompass personal data. It offers a novel interpretation of the concept through numerous examples where personal data represent personal and identifiable characteristics of an individual. Part III also addresses

48. Post & Rothman, *supra* note 29, at 86, 120 ("Something like a right of control seems also to underlie the burgeoning worldwide movement to protect data privacy on the basis that there should be a right of 'individual control over personal data.'" (quoting Orla Lynskey, *Control over Personal Data in a Digital Age:* Google Spain v. AEPD and Mario Costeja Gonzalez, 78 MOD. L. REV. 522, 529 (2015))).

49. *Id.* at 116.

50. *See* RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (AM. L. INST. 1977).

51. In *Cohen v. Herbal Concepts, Inc.*, a mother and daughter bathing in a stream in Woodstock had nude photos taken and published in a magazine without their consent. 472 N.E.2d 307, 308 (N.Y. 1984). The defendant moved for summary judgment, arguing that since the image only showed the plaintiffs' backs and not their faces, there was no breach of privacy. *Id.* at 308–09. The court disagreed and stated that because a jury could find that the image had enough identifiable characteristics, the case could move forward. *Id.* at 309–10.

52. A person is "'[i]dentified' when, within a group of persons, he or she is 'distinguished' from all other members of the group." Malia Thuret-Benoist, *What Is the Difference Between Personally Identifiable Information (PII) and Personal Data?*, TECH GDPR (June 27, 2019) (emphasis omitted), https://techgdpr.com/blog/difference-between-pii-and-personal-data/ [https://perma.cc/QX9B-KL2T]. A "person is 'identifiable' when, although the person has not been identified yet, it is possible to do it." *Id.* (emphasis omitted).

53. 594 U.S. 413, 417 (2021).

challenges to the thesis, including defining the scope of protected data for the purposes of the appropriation tort, bypassing the notorious consent forms, Article III standing, and its compatibility with the First Amendment.

I. PRIVACY IN TORTS

The idea that a law review article can have lasting influence on the law is exemplified by the *Harvard Law Review* article *The Right to Privacy*.[54] In 1890, future Supreme Court Justice Louis Brandeis and his co-author Samuel Warren laid out the grounds for an individual's common law right to privacy.[55]

Upset by the "yellow journalism" that published pictures of a private wedding ceremony[56] and the challenges with the new technology of "[i]nstantaneous photographs,"[57] Mr. Warren turned to his co-author to advocate for "the right 'to be let alone.'"[58] The recognition of such a privacy right would mean that "the law will take cognizance of an injury, even though no right of property or contract may be involved and even though the damages resulting are exclusively those of mental anguish."[59] They built their argument on the precedent, yet moved beyond the common law protections afforded in property and defamation.[60] For them, the "inviolate personality"[61] should be protected, and this protection could come through recognition of a right to privacy.[62] This was a "fundamental legal reconceptualization" that proved to be a successful one.[63]

The first reported court case that expressly discussed the right of privacy in the United States was in 1891, a year after the article had been published.[64] Yet, it was the New York Court of Appeals that, in its famous 1902 case *Roberson v.*

54. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. RSRV. L. REV. 647, 647 (1991) (describing Warren and Brandeis's work as a "monumental article" (quoting Harold R. Gordon, *Right of Property in Name, Likeness, Personality and History*, 55 NW. U. L. REV. 553, 553 (1960))); Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624 (2002) ("Brandeis and Warren's article has attained what some might call legendary status.").

55. *See* Richards & Solove, *supra* note 22, at 1888, 1891.

56. Prosser, *supra* note 23, at 383.

57. Warren & Brandeis, *supra* note 54, at 195.

58. *Id.* (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1879)); *see also* Richards & Solove, *supra* note 22, at 1891 n.17 (noting that the term "the right to be let alone" was "borrowed . . . from Thomas Cooley's treatise on torts").

59. Post, *supra* note 54, at 648 (quoting Eick v. Perk Dog Food Co., 106 N.E.2d 742, 745 (1952)).

60. Some scholars have described the work of Warren and Brandeis in this article as "the legal equivalent of pulling a rabbit out of a hat." Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 125 (2007).

61. Warren & Brandeis, *supra* note 54, at 205.

62. Post, *supra* note 54, at 650 (noting that Warren and Brandeis equated privacy with "inviolate personality").

63. *Id.* at 666.

64. Schuyler v. Curtis, 15 N.Y.S. 787 (Sup. Ct. 1891), *rev'd*, 42 N.E. 22 (N.Y. 1895); *see* Richards & Solove, *supra* note 60, at 146.

Rochester Folding Box Co.,[65] became "[t]he first state court of last resort" to reject the idea of a common law right to privacy in the absence of a statute.[66]

In *Roberson*, the defendant had published and spread out around 25,000 lithographic prints and photographs of an individual named Ms. Roberson on their flour boxes without her knowledge.[67] Judge Parker, writing for the majority, rejected her privacy claim of unauthorized publication of her "lithographic likenesses."[68] With a sexist tone illustrating the prevailing social norms,[69] Judge Parker noted that "she has been caused to suffer mental distress where others would have appreciated the compliment to their beauty implied in the selection of the picture for such purposes."[70] The court reasoned that there had been no positive law recognizing such a right, and there was no case in common law, going back to the English courts, supporting a right to privacy.[71]

A few years after this decision, in *Pavesich v. New England Life Insurance Co.*, the Supreme Court of Georgia became the first court in the United States to recognize the common law right to privacy.[72] In this case, an artist named Paolo Pavesich brought an action for libel and the violation of his privacy against several defendants. Without Mr. Pavesich's consent or knowledge, they took and later published his photo in an advertisement in the *Atlanta Constitution* newspaper.[73] The defendants tried to dismiss his claim in the trial court, but Mr. Pavesich appealed to the state's supreme court.[74]

---

65. 64 N.E. 442 (N.Y. 1902).

66. Richards & Solove, *supra* note 60, at 146.

67. *Roberson*, 64 N.E. at 442.

68. Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 77 (Ga. 1905); *Roberson*, 64 N.E. at 447.

69. As Jessica Lake writes: "Chief Justice Parker's inability to identify with her meant he could not understand or empathize with her plight, which led to his unwillingness to provide her with a remedy." JESSICA LAKE, THE FACE THAT LAUNCHED A THOUSAND LAWSUITS: THE AMERICAN WOMEN WHO FORGED A RIGHT TO PRIVACY 67 (2016).

70. *Roberson*, 64 N.E. at 443. After the unpopular decision in *Roberson*, the New York legislature enacted a statute recognizing the right to privacy. Richards & Solove, *supra* note 60, at 147.

> Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent first obtained as [provided by the new law] may maintain an equitable action . . . to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use . . . .

N.Y. CIV. RIGHTS LAW § 51 (2014).

71. *See Roberson*, 64 N.E. at 445–47.

72. 50 S.E. 68 (Ga. 1905). *Pavesich* compares the lack of privacy to enslavement:

> [A]nd, as long as the advertiser uses him for these purposes, he cannot be otherwise than conscious of the fact that he is for the time being under the control of another, that he is no longer free, and that he is in reality a slave, without hope of freedom, held to service by a merciless master . . . .

Id. at 80. While *Pavesich* was the first common law case that recognized the common law right to privacy, see Allen, *supra* note 26, at 1204–10 for an argument that the narration of *Pavesich* misses the experience of African-Americans during the years of slavery. See also Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J. F. 907 (2022) for a discussion of the unique vulnerabilities to bias and discrimination African-Americans face when it comes to online data privacy.

73. *Pavesich*, 50 S.E. at 68; *see also* Allen, *supra* note 26, at 1189 (examining in detail the facts of *Pavesich*).

74. Allen, *supra* note 26, at 1195 (citing Jefferson James Davis, *An Enforceable Right of Privacy: Enduring Legacy of the Georgia Supreme Court*, 3 J.S. LEGAL HIST. 97, 106 (1994)). There was no intermediate court at the time. *Id.*

The Supreme Court of Georgia came out in favor of Mr. Pavesich and recognized a common law right to privacy. The court cited to the *Roberson* case as "the first and only decision by a court of last resort involving the existence of a right of privacy."[75] Judge Cobb disagreed with *Roberson*, opining that the right can be "inferred from what has been said by commentators upon the legal rights of individuals, and from expressions which have fallen from judges in their reasoning in cases where the exercise of the right was not directly involved."[76] The court noted that "[t]his conservatism of the judiciary has sometimes unconsciously led judges to the conclusion that, because the case was novel, the right claimed did not exist."[77] Judge Cobb recognized the right to privacy, stating that "[a] right of privacy in matters purely private is therefore derived from natural law" and ruled in favor of Mr. Pavesich.[78]

Although it took a while for courts across the United States to recognize a right to privacy, "[w]ithin a decade, courts were more open to the right."[79] Finally, the Restatement (First) of Torts of 1939 devoted a section to this new emerging right. It was initially recognized in the Restatement as an undifferentiated single tort of interference with privacy.[80] The Restatement read: "A person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other."[81]

About fifty-five years after *Pavesich*, the Dean of the University of California, Berkeley School of Law, William Prosser, wrote an article entitled *Privacy* that proved influential for common law tort development.[82] Dean Prosser, who had written on torts and published a torts casebook in 1952,[83] observed that by 1960, around 300 state court cases had recognized a form of a right to privacy.[84] In studying cases that referred to this right of privacy, Dean Prosser underscored his prior point that the privacy tort is essentially four distinct torts.[85] "Without any attempt to exact definition," he laid out the four distinct privacy torts which, in his view, "are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff . . . 'to be let alone.'"[86] The torts were as follows:

---

75. *Pavesich*, 50 S.E. at 77.
76. *Id.*
77. *Id.* at 78.
78. *Id.* at 70, 81.
79. Allen, *supra* note 26, at 1200–01.
80. Post, *supra* note 54, at 648 n.10.
81. RESTATEMENT (FIRST) OF TORTS § 867 (AM. L. INST. 1939).
82. *See generally* Prosser, *supra* note 23.
83. Richards & Solove, *supra* note 22, at 1897–98.
84. Prosser, *supra* note 23, at 388–89; *see also* Allen, *supra* note 26, at 1201 ("By 1960 there would be, according to William Prosser's count, some 300 state law cases recognizing a right to privacy . . . .").
85. Prosser had previously discussed his categorization of the privacy tort into four distinct torts in a series of 1953 Cooley lectures at the University of Michigan. Richards & Solove, *supra* note 22, at 1898. Moreover, false light was added as a tort category in these lectures and in the 1954 published book version of the lectures. For a detailed analysis on Prosser's views on privacy torts, see *id.* at 1895–901.
86. Prosser, *supra* note 23, at 389 (quoting COOLEY, *supra* note 58, at 29).

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[87]

As the Reporter for the American Law Institute's Restatement (Second) of Torts, Prosser successfully enshrined his four torts into the Restatement.[88] This Part continues to briefly discuss the first three privacy torts before diving into the appropriation tort.

The tort of public disclosure of private facts, or as titled by the Restatement (Second) of Torts, "Publicity Given to Private Life," imposes liability for invasion of privacy when the tortfeasor "gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[89] In this tort, "the tortfeasor has obtained certain information about an individual without necessarily intruding upon that individual's privacy."[90] Therefore, this is not a workable tort for data privacy, since it does not involve intrusion upon an individual's privacy.

The tort of false light, which has a resemblance to the interest that the law of defamation protects,[91] has been described by the Restatement (Second) of Torts as follows:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
>
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and

87. *Id.*

88. Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's* Privacy *and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF L. REV. 1925, 1939 (2010).

89. RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

90. Takhshid, *supra* note 25, at 158 (distinguishing this tort from the intrusion tort). The tort of public disclosure often triggers the First Amendment, and as such the U.S. Supreme Court has also had occasions to consider the application of this tort. *See, e.g.*, Fla. Star v. B.J.F., 491 U.S. 524, 527, 532 (1989) (holding that imposing damages on the *Florida Star* newspaper for publishing a rape victim's name obtained from a police report violated the First Amendment).

91. RESTATEMENT (SECOND) OF TORTS § 652E cmt. b (AM. L. INST. 1977); *see also* ELLEN M. BUBLICK, JANE R. BAMBAUER & DANIEL A. ARELLANO, *DOBBS* ON ECONOMIC AND DIGNITARY TORTS 231 (2d ed. 2022) (noting that defamation and false light differ in that "the false light tort requires publicity, but it does *not* require damage to the plaintiff's reputation. Rather, false light is considered a privacy tort because the harm is to the plaintiff's psyche and sense of self" (citing Godbehere v. Phx. Newspapers, Inc., 783 P.2d 781 (Ariz. 1989))).

> (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[92]

False light is the least popular tort amongst the state courts; several jurisdictions have openly rejected its recognition.[93] Given its unpopularity and the stated requirements for satisfying this tort, false light is also not ideal for data protection.[94]

The third tort on the list is the tort of intrusion upon seclusion.[95] According to the Restatement (Second) of Torts: "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."[96] The intrusion tort can be satisfied "even though there is no publication or other use of any kind of the . . . information outlined."[97]

The intrusion tort has been invoked in contexts such as secret recordings,[98] eavesdropping,[99] and more recently for digital privacy and data breach.[100] However, the requirement for the intrusion to be "highly offensive" has made successful data privacy suits an anomaly. Consider, for example, *Popa v. Harriet Carter Gifts, Inc.*[101] In this case, the plaintiff brought a class action lawsuit against a gift merchant website and the data collection company.[102] The plaintiff alleged a violation of Pennsylvania's wiretap statute and invasion of privacy, based on the intrusion upon seclusion tort for collection of her data, including PII, while she shopped online.[103] The court stated that in Pennsylvania, the invasion

92. RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1977). Like the publication torts, false light triggers First Amendment issues, and the Supreme Court has weighed in on this tort, too. In *Time, Inc. v. Hill*, the Court stated that the actual malice standard applies to false light. 385 U.S. 374, 387 (1967). The Court applied the *New York Times Co. v. Sullivan* standard in considering the false light claim. *See id.* at 390–91; N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279 (1964).

93. *See, e.g.*, Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1100 (Fla. 2008) (declining to recognize the tort of false light); Denver Publ'g Co. v. Bueno, 54 P.3d 893, 894 (Colo. 2002) (rejecting the tort of false light as "highly duplicative of defamation both in interests protected and conduct averted"); Cain v. Hearst Corp., 878 S.W.2d 577, 577 (Tex. 1994) (ruling that "false light substantially duplicates the tort of defamation," and therefore rejecting the tort of false light).

94. In a recent article, John Goldberg and Benjamin Zipursky argue that the tort of false light may help with modern privacy invasions. *See* John C. P. Goldberg & Benjamin C. Zipursky, *A Tort for the Digital Age: False Light Invasion of Privacy Reconsidered*, 73 DEPAUL L. REV. 461, 461 (2024).

95. *See* Prosser, *supra* note 23, at 389.

96. RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

97. *Id.* § 652B cmt. b.

98. Hamberger v. Eastman, 206 A.2d 239, 240–42 (N.H. 1964); *see also* BUBLICK ET AL., *supra* note 91, at 170 (noting that "[s]urreptitious surveillance inside the home by a snoop who isn't physically present is an intrusion").

99. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (AM. L. INST. 1977); Fowler v. S. Bell Tel. & Tel. Co., 343 F.2d 150, 156 (5th Cir. 1965) ("[T]apping a telephone amounts to an intrusion upon plaintiff's solitude as to which no publication of the overheard information is necessary.").

100. *See In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 293–94, 293 n.198 (3d Cir. 2016).

101. 426 F. Supp. 3d 108 (W.D. Pa. 2019).

102. *See id.* at 111–12.

103. *See id.* at 112.

must be "of the sort which would cause mental suffering, shame or humiliation to a person of ordinary sensibilities."[104] It therefore dismissed the intrusion claim for failure to plead sufficiently offensive conduct, which was a requirement for establishing a prima facie case of the intrusion tort.[105]

Another example of an unsuccessful digital privacy claim where plaintiffs invoked the intrusion tort is *McCoy v. Alphabet, Inc.*[106] In *McCoy*, the plaintiff sued Google, LLC in a class action, alleging "that [the d]efendant has been using an internal program called 'Android Lockbox' to monitor and collect sensitive personal data when users use non-Google applications ('apps') on their Android smartphones."[107]

The court in this 2021 case stated that Google's data collection did not amount to the "egregious violation[] of social norms" required for this tort.[108] It noted that many courts consider the alleged data collection "routine commercial behavior."[109] Having not reached the egregiousness level required for the intrusion tort, the district court granted Alphabet's motion to dismiss the plaintiff's common law privacy claim.[110]

In addition to the challenge of proving the element of a "highly offensive" and "egregious" intrusion, the discrepancies amongst courts' decisions in reaching a conclusion on this issue make alleging the commission of the intrusion tort for digital privacy and data collection lawsuits an unreliable strategy.[111] In lieu of relying on the intrusion tort, Part II proposes invoking the appropriation of likeness tort and illustrates how this tort's privacy protection can be expanded to include data privacy suits.

---

104. *Id.* (emphasis omitted) (quoting Chicarella v. Passant, 494 A.2d 1109, 1114 (Pa. Super. Ct. 1985)). Despite the ruling, the court noted that:

> The surreptitious gathering of this type of information may cause concern, even deep concern, about electronic privacy. Consumers may be troubled that their trip to an electronic marketplace may feature surveillance of their every behavior that is far more intrusive than a trip to the local mall, and that the data garnered from even ca[su]al browsing may be used by retailers—and others—for marketing or more sinister purposes. But even well-founded concern is not enough to give rise to tort liability.

Id. at 122–23.

105. *See id.* at 122.

106. No. 20-cv-05427, 2021 WL 405816 (N.D. Cal. Feb. 2, 2021).

107. *Id.* at *1.

108. *Id.* at *7 ("[C]ourts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." (quoting *In re* Google, Inc. Priv. Pol'y Litig., 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014))).

109. *Id.* (quoting *In re* Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 830 (N.D. Cal. 2020)).

110. *Id.* at *8. *But see In re* Google Location Hist. Litig., 514 F. Supp. 3d 1147, 1158 (N.D. Cal. 2021) (denying Google's motion to dismiss for the intrusion tort, and ruling that precedent did not compel a finding that defendant's alleged conduct was not highly offensive where "defendants tracked the plaintiffs after the plaintiffs stopped using the defendant's services" (quoting *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 606 n.8 (9th Cir. 2020))).

111. *See In re* Google Location Hist. Litig., 514 F. Supp. 3d at 1157 (stating that the "highly offensive analysis 'essentially involves a "policy" determination as to whether the alleged intrusion is highly offensive under the particular circumstances'" (quoting Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009))).

II. THE EVOLUTION OF THE TORT OF APPROPRIATION

As previously discussed, the canonical story of the tort of appropriation of likeness begins with *Roberson v. Rochester Folding Box Co.* and the court's rejection of a right to privacy.[112] The public's dismay with this decision led to New York passing a law protecting name, image, and likeness.[113] In *Pavesich v. New England Life Insurance Co.*, a state court also recognized the interest in one's likeness.[114] Since the cases were discussed above, we continue with Prosser's description of the appropriation tort.

Prosser carved out the appropriation tort as the last category of the four "archetypal forms" of invasion of privacy.[115] He wrote that "[i]t is the plaintiff's name as a symbol of his identity that is involved here, and not his name as a mere name."[116] Thus, "the question before the courts has been first of all whether there has been appropriation of an aspect of the plaintiff's identity."[117] Once that has been established, "there is the further question whether the defendant has appropriated the name or likeness for his own advantage."[118]

As the tort evolved both through state common law and statutes, the Restatement (Second) of Torts described it as: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[119] Although the tort is commonly invoked when the defendant has used the name or likeness for a commercial purpose, "[i]t applies also when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one."[120]

The appropriation tort protects a number of interests, including "a privacy interest in protecting a person against unwanted public exposure (i.e., the right to remain anonymous); an autonomy interest in controlling how one's image is presented to others; and an economic interest in the value of one's image for marketing and trade."[121] But as celebrities began to rely on this tort, it was evident that

112. 64 N.E. 442, 447 (N.Y. 1902).

113. *See* Richards & Solove, *supra* note 60, at 147; N.Y. CIV. RIGHTS LAW § 51 (2014).

114. 50 S.E. 68, 70 (Ga. 1905).

115. John C.P. Goldberg & Benjamin C. Zipursky, *Unrealized Torts*, 88 VA. L. REV. 1625, 1628 (2002).

116. Prosser, *supra* note 23, at 403.

117. *Id.*

118. *Id.* at 405.

119. RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977).

120. *Id.* § 652C cmt. b (adding that some state statutes, however, limit the liability for this tort to commercial use only); *see also id.* § 652C reporter's note ("Under the statutes in New York, Oklahoma, Utah, and Virginia, the appropriation must be for advertising, or for purposes of trade . . . ."). For illustrations of the tort of appropriation being statutorily limited to those instances involving advertising and trade, see, for example, N.Y. CIV. RIGHTS LAW § 51; OKLA. STAT. tit. 12, §§ 1448–1450; UTAH CODE ANN. §§ 45-3-1 to -6; and VA. CODE ANN. § 8.01-40.

121. JOHN C.P. GOLDBERG & BENJAMIN C. ZIPURSKY, THE OXFORD INTRODUCTIONS TO U.S. LAW: TORTS 336 (Dennis Patterson ed. 2010).

their interest in anonymity paled in comparison to their interest in control or economic gain.[122]

Thus, in *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, Judge Jerome Frank coined the term "right of publicity"[123] for prominent persons to receive money for unauthorized "public exposure of their likenesses."[124] Harold R. Gordon, in his 1960 law review article, further argued for what has been characterized as "an independent action for commercial appropriation" of public figures.[125] After his law review article, more courts treated the two differently, and "[t]he connection between commercial and personal harms was severed. . . . [However, f]rom 1953 to 1970 few cases actually held that there was an independent right of publicity" separate from that of a privacy-based tort, with a "vast majority" of courts treating both as privacy rights.[126]

Nevertheless, in 1977, the Supreme Court's decision in *Zacchini v. Scripps-Howard Broadcasting Co.*[127] boosted the idea of an independent right of publicity, placing it "in the pantheon of [intellectual property]."[128] In *Zacchini*, the petitioner claimed that his Ohio-based right of publicity was violated when the respondent, a broadcasting company, videotaped and later broadcasted his act in a show.[129] Hugo Zacchini was an entertainer who performed a "human cannonball" stunt, wherein he was shot from a cannon into a net.[130] The respondent claimed that their broadcasting of the show was privileged under the First and the Fourteenth Amendment and that they were thus immune from paying any damages.[131] The Ohio Supreme Court ruled that although Mr. Zacchini's right of publicity was violated, the invasion of privacy was privileged, since the broadcasting company had the right to broadcast matters of legitimate public interest.[132] But the United States Supreme Court weighed in and disagreed.[133]

In reaching its decision, the Court elaborated on the differences between the tort of false light and the right of publicity. The Court noted that the interest of the state in protecting the right of publicity "is closely analogous to the goals of patent and copyright law, focusing on the right of the individual to reap the

122. *Id.*

123. Post, *supra* note 54, at 666 (quoting Haelan Lab'ys, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953)).

124. *Haelan Lab'ys, Inc.*, 202 F.2d at 868 ("This right might be called a 'right of publicity.' For it is common knowledge that many prominent persons (especially actors and ball-players), far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money for authorizing advertisements, popularizing their countenances displayed in newspapers, magazines, busses, trains and subways.").

125. ROTHMAN, *supra* note 32, at 73 (discussing Gordon's article); *see* Harold R. Gordon, *Right of Property in Name, Likeness, Personality and History*, 55 NW. U. L. REV. 553, 555, 613 (1960).

126. ROTHMAN, *supra* note 32, at 75.

127. 433 U.S. 562 (1977).

128. ROTHMAN, *supra* note 32, at 87.

129. *Zacchini*, 433 U.S. at 564–65.

130. *Id.* at 563.

131. *See id.* at 565.

132. *Id.* at 565.

133. *Id.* at 566.

reward of his endeavors and having little to do with protecting feelings or reputation."[134]

Today, the distinctions between the appropriation tort and the right of publicity remain imprecise, with disparities across different U.S. states.[135] Some states have passed statutes differentiating the two, and others have treated both as one.[136] In a recent article, Post and Rothman observe: "Although some courts (and scholars) distinguish the privacy tort of appropriation (which they define as protecting personality interests in identity) from the tort of right of publicity (which they define as protecting the market value of identity), many states treat the two torts interchangeably."[137]

Whether we choose to call it the right of publicity, as Post and Rothman do, or hold on to the differences in the theoretical interest behind the right of publicity and the tort of appropriation of name and likeness—as illustrated by Professor John C. P. Goldberg and Professor Benjamin C. Zipursky[138]—the protection of identity remains a core principle of this common law privacy tort. Warren and Brandeis "were advocating that privacy be embodied within a regime of *personal* rather than property rights," where the dignitary aspect of the right to privacy can be emphasized, unlike common law copyright, which bases its protection in the perceived value of property rights and ownership.[139]

This Article chooses to use "appropriation" because the so-called publicity right, even if distinguished from appropriation, is one that grew out of the personality interests the appropriation tort aimed to protect. Therefore, the core of the right of publicity cannot be something different from its origins. The focus of this Article is the contours of the persona which the appropriation tort aims to protect.

While image and likeness in early cases were limited to unauthorized use of photographs and video recordings, the various aspects of one's identity protected by the tort evolved over time. One of the prominent cases is *Onassis v. Christian Dior–New York, Inc.*, in which Jacqueline Kennedy Onassis, former First Lady of the United States, sued multiple "defendants, all of whom were associated with an advertising campaign to promote the products and the image of Christian

134. *Id.* at 573. Rothman notes that "[b]ecause [intellectual property] is often thought to be in the public interest, . . . the right of publicity has proliferated across the United States." ROTHMAN, *supra* note 32, at 87.

135. Post & Rothman, *supra* note 29, at 89–90 (noting that the uncertainty in what type of harm the tort is protecting has caused the disparities).

136. *See* ROTHMAN'S ROADMAP TO THE RIGHT OF PUBLICITY, *supra* note 22; OKLA. STAT. tit. 12, §§ 1448–1450 (differentiating between the tort of appropriation and the right of publicity); 765 ILL. COMP. STAT. 1075/1–60 (subsuming the tort of appropriation into the right of publicity); Moore v. Sun Publ'g Corp., 881 P.2d 735, 743 (N.M. Ct. App. 1994); Benally v. Hundred Arrows Press, Inc., 614 F. Supp. 969, 977–78 (D.N.M. 1985) (demonstrating a common law approach to privacy torts as exemplified by the state of New Mexico).

137. Post & Rothman, *supra* note 29, at 93–94 (footnote omitted). Scholars have noted that the transferability of the right of publicity separates the right from the appropriation tort, similar to intellectual property rights. *See id.* at 93 n.22.

138. GOLDBERG & ZIPURSKY, *supra* note 121, at 336.

139. Post, *supra* note 54, at 663.

Dior—New York, Inc."[140] The case arose from an advertising image in which Christian Dior–New York, Inc. (hereinafter Dior) used an image of a female who "bore a striking resemblance to the plaintiff" in its ad campaign.[141] The plaintiff sued for a preliminary injunction under New York's § 51 Civil Rights Law, which established a statutory right of privacy resembling the tort of appropriation of likeness.[142]

The main issue was that Dior had not used Jacqueline Kennedy's portrait or picture, as § 51 had stated; they had used the picture of a "look-alike."[143] The question was, therefore, "what is comprehended by the term 'portrait or picture?'"[144] Did this privacy protection only include a person's portrait or picture? Or could the court have a broader interpretation of this appropriation privacy protection? The New York court relied on precedent to show that expansion of this protection was warranted. It cited to a case, *Young v. Grenerker Studios, Inc.*,[145] in which the "court [had] extended the literal definition of portrait or picture to include a manikin or sculpture for which plaintiff was the model."[146] The court noted that "[t]he words 'portrait or picture' were construed to be broad enough to cover any likeness or representation of the plaintiff, whether two or three dimensional."[147]

The court continued to reason that using a look-alike was akin to using one's identity because "[t]here are many aspects of identity," and "[t]he essence of what is prohibited, as the statute, the cases, and the dictionary definitions make clear, is the exploitation of one's identity as that is conveyed verbally or graphically."[148]

---

140. 472 N.Y.S.2d 254, 256 (Sup. Ct. 1984), *aff'd*, 488 N.Y.S.2d 943 (App. Div. 1985).

141. *Id.* at 257.

142. *Id.* at 256, 258.

> Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent first obtained as above provided may maintain an equitable action in the supreme court of this state against the person, firm or corporation so using his name, portrait, picture or voice, to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use and if the defendant shall have knowingly used such person's name, portrait, picture or voice in such manner as is forbidden or declared to be unlawful by section fifty of this article, the jury, in its discretion, may award exemplary damages.

N.Y. CIV. RIGHTS LAW § 51. Note that the law was amended to include voice after *Onassis*. Section 50 states,

> A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.

N.Y. CIV. RIGHTS LAW § 50. As previously explained, this law was passed in reaction to the rejection of the recognition of a right to privacy by a New York court in *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (1902). *See* Richards & Solove, *supra* note 60, at 147.

143. *Onassis*, 472 N.Y.S.2d at 256.

144. *Id.* at 259.

145. 26 N.Y.S.2d 357 (Sup. Ct. 1941).

146. *Onassis*, 472 N.Y.S.2d at 259.

147. *Id.*

148. *Id.* at 261. The court also rejected any First Amendment argument that "this advertisement [wa]s privileged as a protected form of free speech." *Id.* at 262.

In its analysis, the court also mentioned that "conveying the likeness of a person . . . through . . . voice" was not covered by the statute, but not as a matter of principle; rather, such exclusion was "possibly an oversight, since the possibility of reproducing and disseminating the sound of a voice was not contemplated in 1903 when the §§ 50 and 51 of the Civil Rights Law were first enacted."[149]

Indeed, it did not take long for courts to explicitly extend the protection to include voice. In 1988, the singer Bette Midler sued Ford Motor Company for having used one of her former backup singers to record an advertisement.[150] In the televised ad, the backup singer sings one of Ms. Midler's songs with minor alternations, "leaving out only a few 'aahs.'"[151] Although neither Ms. Midler's name nor image was used, the ad sounded as if it were Ms. Midler singing the song.[152] Thus, at issue for the Ninth Circuit Court of Appeals was the question of the imitation of Ms. Midler's voice—not the use of the singer's actual voice.[153]

California's Civil Code had "afford[ed] damages to a person injured by another who uses the person's 'name, voice, signature, photograph or likeness, in any manner.'"[154] But because the exact voice of Ms. Midler had not been used, the court turned to the common law appropriation tort.[155] The court noted that California recognized "an injury from 'an appropriation of the attributes of one's identity.'"[156] It stated that a voice is even more personal than attributes that had previously been protected, and its imitation could constitute the commission of the common law appropriation tort in California.[157]

This evolution of protecting one's identity as a privacy tort did not stop here. Moving beyond voice as one of a person's biometric identifiers, the appropriation tort expanded to protect persona by "including the mere evocation . . . of [one's] identity."[158] In *White v. Samsung Electronics America, Inc.*, Vanna White, one of the hosts of the television gameshow *Wheel of Fortune*, sued Samsung over an advertisement that depicted a robot which resembled Ms. White on the show.[159]

149. *Id.* at 259.

150. Midler v. Ford Motor Co., 849 F.2d 460, 461 (9th Cir. 1988).

151. *Id.*

152. *Id.* at 461–62.

153. *Id.* at 463.

154. *Id.* (quoting CAL. CIV. CODE § 3344).

155. *See id.* (ruling that the California statute did not preclude common law-based actions).

156. *Id.* (quoting Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 824 (9th Cir. 1974)) ("It was irrelevant that Motschenbacher could not be identified in the ad. The ad suggested that it was he. The ad did so by emphasizing signs or symbols associated with him. In the same way the defendants here used an imitation to convey the impression that Midler was singing for them.").

157. *Id.* ("We hold only that when a distinctive voice of a professional singer is widely known and is deliberately imitated in order to sell a product, the sellers have appropriated what is not theirs and have committed a tort in California.").

158. ROTHMAN, *supra* note 32, at 89.

159. 971 F.2d 1395, 1396 (9th Cir. 1992); *see also* Wendt v. Host Int'l, Inc., 125 F.3d 806, 809, 811–12 (9th Cir. 1997) (allowing a common law right of publicity claim to move forward, and providing for identity protection in a case where defendant used animatronic robots that were based on plaintiffs' likenesses (identities) and that resembled the plaintiffs).

The ad did not include the name, picture, or even the voice of Ms. White.[160] However, the resemblance was enough for a majority in the Ninth Circuit Court of Appeals to hold that a jury could find that Samsung violated her privacy right and appropriated her identity.[161]

After reviewing the precedent, including *Midler*, the *White* court stated: "These cases teach not only that the common law right of publicity reaches means of appropriation other than name or likeness, but that the specific means of appropriation are relevant only for determining whether the defendant has in fact appropriated the plaintiff's identity."[162] In other words, the court elaborated, "It is not important *how* the defendant has appropriated the plaintiff's identity, but *whether* the defendant has done so."[163] Limiting the tort to specific means of appropriating one's identity would encourage "the clever advertising strategist to come up with" new ways to appropriate one's identity.[164]

The reasoning of the court falls well in line with the argument of this Article. In the new digital era, where advertisers, private companies, and other players in the market may be benefiting from an individual's personal data more than any other aspect of one's being, the tort of appropriation should be revisited by courts. Reconceptualizing what constitutes one's persona worthy of protection via the appropriation tort will allow courts to decide cases alleging tortious invasion of privacy for unauthorized personal data collection more coherently. Our personas now encompass our personal data. As the court stated in *White*, "[I]f we treated the means of appropriation as dispositive in our analysis of the right of publicity, we would not only weaken the right but effectively eviscerate it."[165] Part III illustrates how this approach can be conceptualized and used by both plaintiffs and courts struggling with unauthorized data collection suits.

III. APPROPRIATION OF DIGITAL LIKENESS AND PERSONA

A. DATA AS LIKENESS

Data are personal. Consider, for example, headsets used for experiencing the metaverse. A recent report observed that "the sensing found in [Extended Reality] XR headsets and their associated peripherals will enable the capture of a range of data," such as "[m]ovements and physical actions" that can include "[o]ptical and inertial tracking of head/body/limb movements"; "sensing of facial expressions, auditory sensing of speech and non-speech activity"; "[n]eural activity"; context data that include "[l]ocation tracking" and

160. *See White*, 971 F.2d at 1396.
161. *Id.* at 1399.
162. *Id.* at 1398.
163. *Id.*
164. *Id.* For more on the advertisement and intellectual property discussion of the tort of publicity, see generally REBECCA TUSHNET & ERIC GOLDMAN, *Featuring People in Ads*, *in* ADVERTISING & MARKETING LAW: CASES AND MATERIALS 551 (6th ed. 2022).
165. *White*, 971 F.2d at 1399.

"Simultaneous Localization and Mapping (SLAM)"; and physiological data such as "[e]ye/gaze tracking."[166]

Thus, the ways third parties benefit from our data—or as this Article argues, our identity—increasingly involve various forms of distinctive features of our beings. It is these personal data that shape our modern-day *likeness*, our *persona*.[167] For the appropriation tort to be responsive to the modern technologies and their potential tortious dignitary violations, the privacy law of torts should extend its protection to our personal data, our digital persona.

This expansion is warranted both from a theoretical standpoint and as a matter of practical necessity. From a theoretical standpoint, while privacy is a multidimensional notion, one of its major focuses has been "preventing objectification and preserving personhood" of the self.[168] In tort law, privacy torts are commonly referred to as dignitary torts[169]—civil wrongs that encompass stand-alone dignitary harms.[170] "The personal right of privacy advocated by Warren and Brandeis . . . attaches personality firmly to the actual identity of a living individual."[171] Yet, the protection of dignity, identity, and, in essence, persona throughout the recent

166. MARK MCGILL, INST. OF ELEC. & ELECS. ENG'RS, INC., EXTENDED REALITY (XR) AND THE EROSION OF ANONYMITY AND PRIVACY 7 (2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf [https://perma.cc/7GRE-JRAF]. *See generally* Dean Takahashi, *The Ethics of the Metaverse*, VENTUREBEAT (Jan. 26, 2022, 4:20 PM), https://venturebeat.com/consumer/the-ethics-of-the-metaverse-2/ [https://perma.cc/6T66-AUGF] (quoting Kent Bye on the complexities of data collection in the metaverse).

167. Among the European Union member states, this broad category of rights is known as personality rights and "tend[s] to refer to a cluster of rights, such as privacy, identity and dignity." Susanna Lindroos-Hovinheimo, *Jurisdiction and Personality Rights – in Which Member State Should Harmful Online Content Be Assessed?*, 29 MAASTRICHT J. EUR. & COMPAR. L. 201, 203 (2022). Scholars in the United States are increasingly becoming interested in understanding a broader concept of self and personal rights. Mitchell Crusto has argued for a broad "Right of Self" that is grounded in property rights and would encompass all aspects of one's attributes, including name, image, and likeness (NIL), and would address wealth inequalities. *See generally* Mitchell F. Crusto, *Right of Self*, 79 WASH. & LEE L. REV. 533 (2022). Crusto writes, "Right of Self is a fundamentally, constitutionally, and jurisprudentially based natural property right that every person in the United States is entitled to enjoy." *Id.* at 548.

168. Margot E. Kaminski, *The Case for Data Privacy Rights (or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 390 (2022) (first citing Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83, 121 (2019); then citing Lee A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUT. L. & SEC. REP. 17, 18 (2001); then citing Meg Leta Jones, *The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood*, 47 SOC. STUD. SCI. 216, 231 (2017); then citing Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1016–17 (2017); and then citing Martha C. Nussbaum, *Objectification*, 24 PHIL. & PUB. AFFS. 249, 256–57 (1995)). Another lens through which privacy scholars analyze privacy is that of autonomy and liberty. *See id.*

169. *See* DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, HORNBOOK ON TORTS 932 (2d ed. 2016) (defining dignitary torts as involving "legally cognizable invasions of rights that stand independent of both physical and economic harms, that is, invasions of human dignity in the sense of human worth").

170. *See* BUBLICK ET AL., *supra* note 91, 169–71 (discussing examples of "intrusive privacy invasion"); Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 76 (Ga. 1905) (explaining that other dignitary torts include, but are not limited to, defamation cases).

171. Post, *supra* note 54, at 668.

development of this tort since the emergence of contemporary data collection technologies has failed to progress compared to what we have witnessed in the advancement of technologies in the past decade. Data privacy is the talk of the town, but common law privacy torts appear to have nothing much to add to the conversation.[172]

But as Part II illustrated through numerous court cases, the longstanding nature of common law torts, and of the tort of appropriation in particular, has been to extend the right of privacy in line with visual and audio advancements of technologies. Courts noted that name or likeness is not an element of the tort, but it is relevant for determining whether the defendant has appropriated the plaintiff's identity.[173]

In extending privacy protection to include the use of a look-alike image, *Onassis v. Christian Dior–New York, Inc.* noted that "[i]n those days, as the touchstone of recognition, name was all, conveyed in writing or by word of mouth. Today, the visual have superseded the verbal arts, and news photography, television, and motion pictures can accord instant world-wide recognition to a face."[174] *Onassis* was decided in 1984. Today, our personal data have become the newest aspect of our identity. In 2024, this aspect of self in the age of the Internet of Things (IoT), data collection, and what Shoshana Zuboff calls "surveillance capitalism" is the most-used feature of our identity by third parties.[175] Our digital experiences, Zuboff notes, have now turned into a "commercial project."[176] This surveillance capitalism, which "claims human experience as free raw material for translation into behavioral data," has only grown and become more intrusive as the technologies that allow for such collection have become more sophisticated.[177] Google's CEO once stated, "We know where you are. We know where you've been. We can more or less know what you're thinking about."[178] Tort law can rise up to the occasion.

The protection of the self from third parties is not only entrenched in the appropriation privacy tort, but its expansion and conceptualization to include the digital persona is one of common-sense pragmatism. Data-driven technologies have added to the way that one's image or identity can be appropriated. Consider the case of Clearview AI's facial recognition technology.[179] The company developed its app by collecting aspects of individuals' identities, most visibly their images,

172. See *supra* notes 24–26 for scholars' observations on the irrelevance of common law privacy torts for the modern age. *See generally supra* note 24 (citing scholarship discussing the inadequacy of common law privacy torts).

173. *See* White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1397–98 (9th Cir. 1992).

174. 472 N.Y.S.2d 254, 260 (Sup. Ct. 1984), *aff'd*, 488 N.Y.S.2d 943 (App. Div. 1985).

175. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 7 (2019) (emphasis omitted).

176. *Id.*

177. *Id.* at 8.

178. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 22 (2015) (quoting Eric Schmidt).

179. *See* Hill, *supra* note 9.

and has compiled more than three billion images to date.[180] The app allows users to take or upload an image of a person and pull up the available information about them collected by Clearview AI.[181] Because it has so far been used primarily by law enforcement,[182] the company identifies itself as "the leading facial recognition technology company that provides powerful and reliable photo identification technology to law enforcement agencies across the country."[183] The company purports to "help law enforcement and governments in disrupting and solving crime, while also providing financial institutions, transportation, and other commercial enterprises to verify identities, prevent financial fraud, and combat identity theft."[184]

But Clearview AI's means of accumulating images and the ways in which the app has been used have resulted in backlash and ongoing lawsuits.[185] In a recently filed complaint, four activists and two community organizations sued Clearview AI and the Alameda Police Department, among others, alleging violations of their privacy rights under California common and statutory law.[186] The plaintiffs aimed to enjoin both the company and the Alameda Police Department from "acquiring . . . their likenesses, and the likenesses of millions of Californians, in [their] quest to create a cyber surveillance state."[187]

Applying the framework of this Article to the case, one can argue that Clearview AI has accumulated, without consent, images of millions of people, distilled these images into individual biometric data, and used these data to create and enhance its facial recognition technology.[188] As such, it has violated the

180. *Id.*

181. *See id.*

182. *See* Kashmir Hill, *Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands*, N.Y. TIMES (June 21, 2023), https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html. Clearview AI's facial recognition app is also used at a reduced rate by public defenders; however, many public defenders are opposed to its use due to privacy concerns. *Id.*

183. Press Release, Clearview AI, Clearview AI Launches Clearview Consent Company's First Consent Based Product for Commercial Uses (May 25, 2022), https://www.clearview.ai/clearview-ai-launches-clearview-consent-companys-first-consent-based-product-for-commercial-use [https://perma.cc/J8KX-2CFR].

184. CLEARVIEW AI, https://www.clearview.ai [https://perma.cc/63MR-RHL2] (last visited Mar. 17, 2024). Clearview AI CEO, Hoan Ton-That, stated in a recent interview with BBC that Clearview AI has run nearly a million searches for U.S. law enforcement. James Clayton & Ben Derico, *Clearview AI Used Nearly 1m Times by US Police, It Tells the BBC*, BBC NEWS (Mar. 27, 2023), https://www.bbc.com/news/technology-65057011 [https://perma.cc/E27D-GRPS]. This figure comes from Clearview AI and has not been confirmed by law enforcement. *Id.*

185. *See, e.g.*, Thornley v. Clearview AI, Inc., 984 F.3d 1241 (7th Cir. 2021).

186. *See* Complaint at 1, 19–23, Renderos v. Clearview AI, Inc., No. RG21096898, 2022 WL 17326440 (Cal. Super. Ct. Apr. 22, 2021).

187. *Id.* at 1.

188. In May 2022, the company announced that it has now moved to create a consent-based product for commercial use. *See* Press Release, Clearview AI, *supra* note 183. This does not negate causes of action for images previously collected without consent. I discuss Article III standing in this case below. *See infra* Section III.D.

appropriation privacy tort of common law by using the likeness of others, in the shape of biometric data, for its own benefit, without their consent.[189]

Another example of how our data are increasingly used as our personas is the model personas that some engineers have created based on real individuals' personal data. One research institute calls its product Automatic Persona Generation (APG).[190] The "tool . . . automatically turn[s] . . . user[] data into personas"—a process it describes as "giving faces to data."[191]

The institute notes that this "system retrieves data . . . and automatically generates user personas that represent central behavioral and demographic patterns."[192] It adds that it is compatible with programs such as "YouTube Analytics, Google Analytics, Facebook Ads, Facebook Insights, [and] Instagram."[193] Data-driven personas, several authors note, are "a revolutionary step forward in user-centric, customer-centric, and audience-centric focus during the planning, creation, development, and implementation of systems, campaigns, products, ergonomics, content, and so on."[194] They write that "whatever endeavor where actionable decisions about people need to be made, and those decisions need to be made on actual data about real people," these data-driven personas can be helpful for their intended market players because these fictitious personas are made of real people's personal data—their identities.[195]

To add to our poll of examples, recall the types of data collected via an XR headset.[196] Companies are now also working on building devices to enable our

189. *See* Amici Curiae Brief of Science, Legal, and Technology Scholars in Support of Plaintiffs' Opposition to Special Motion to Strike Pursuant to California Code of Civil Procedure § 425.16 at 9–11, Renderos v. Clearview AI, Inc., No. RG21096898, 2022 WL 17326440 (Cal. Super. Ct. Nov. 18, 2022). The author of this Article, along with several other leading scholars, has signed the amici curiae brief. However, "Clearview [AI] has argued its data collection is protected by the First Amendment." Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, WASH. POST (Feb. 16, 2022, 12:47 PM), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

190. *APG (Automatic Persona Generation)*, QATAR COMPUTING RSCH. INST., https://persona.qcri.org/[https://perma.cc/Q6ZQ-83AU] (last visited Mar. 17, 2024).

191. *Id.*

192. *Id.*

193. *Id.*

194. Bernard J. Jansen, Joni Salminen, Soon-gyo Jung & Kathleen Guan, *Data-Driven Personas*, *in* SYNTHESIS LECTURES ON HUMAN-CENTERED INFORMATICS, at x, xxv (John M. Carroll ed., 2021).

195. *Id.* (emphasis omitted). For a picture of such digital personas (APG), see *Sample*, QATAR COMPUTING RSCH. INST., https://persona.qcri.org/persona/ [https://perma.cc/459R-ZCXA] (last visited Mar. 19, 2024).

196. *See supra* note 166 and accompanying text; Christian Tenkhoff, Jonathan Alexander Kropp & Jan Phillip Rektorschek, *The Metaverse: Legal Challenges and Opportunities*, LEXOLOGY (Jan. 31, 2022), https://www.lexology.com/library/detail.aspx?g=c1872705-ccbe-49bb-98f4-77092e4f26ec [https://perma.cc/3WYS-HCUA] ("[T]he technical equipment used for users to experience virtual realities without stepping outside may track data from each user's most private environment – their home."). This issue raises some of the most challenging questions with respect to data collection and its boundaries. *Id.*; *see also* Martin Schwirn, *A Legal Minefield Called the Metaverse*, COMPUT. WKLY. (Jan. 11, 2022), https://www.computerweekly.com/feature/A-legal-minefield-called-the-metaverse [https://perma.cc/VCJ6-CD7V] (stating some of the challenges with data leak and data collection as they relate to virtual realities).

sense of smell in the metaverse.[197] Thinking about the type of data already being collected in the metaverse and what is yet to come, such as physiological data collection, underscores the necessity of recognizing a digital persona in the appropriation of likeness tort.[198]

Critics may argue that even if we recognize that our data are personas and extend likeness to personal data, an individual's data are, in most circumstances, only valuable in the aggregate. Companies collect and use data in massive amounts, and with Big Data, an individual's identity is no longer a central focal point.[199] In that sense, appropriation of one's individual data does not trigger the use of one's persona for purposes of the privacy tort. But this argument is flawed. Mass data extraction does not equate to loss of identifiable information. Big Data is also often accompanied by metadata—"information that describes primary data."[200] Metadata "is a term to describe 'data about data,' a type of purportedly innocuous form of personal data about communications and the usage of digital products and services . . . ."[201] As Professor Daniel Solove observes, attempts "to single out metadata for lesser protection . . . ha[ve] proven to be a fool's errand."[202] Bruce Schneier quotes Stewart Baker, former general counsel for the National Security Agency, as saying that "[m]etadata absolutely tells you everything about somebody's life."[203] Privacy risks with metadata continue to exist, even though the levels of the risk may differ. [204]

---

197. Mikaela Lefrak, *Vermont Tech Firm Believes to Experience the Metaverse, You Have to Smell It Too*, NPR (Mar. 16, 2022, 5:10 AM), https://www.npr.org/2022/03/16/1086832763/vermont-tech-firm-believes-to-experience-the-metaverse-you-have-to-smell-it-too [https://perma.cc/56TG-4CGU].

198. *See* Takahashi, *supra* note 166. For a discussion of some of the legal issues related to extended reality, see Suchismita Pahi & Calli Schroeder, *Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy Is Several of Them*, 4 NOTRE DAME J. ON EMERGING TECHS. 1, 12–36 (2023).

199. On Big Data, see Margot E. Kaminski, Response, Carpenter v. United States*: Big Data Is Different*, GEO. WASH. L. REV. ON THE DOCKET (2018), https://www.gwlr.org/carpenter-v-united-states-big-data-is-different [https://perma.cc/QR4P-SG4Q] (discussing the *Carpenter* concurrence, which opined that in the world of Big Data, location data is not just location data but is transformed through inference-making into more historically sensitive information such as familial, political, professional, religious, and sexual associations).

200. PRAKASH M. NADKARNI, METADATA-DRIVEN SOFTWARE SYSTEMS IN BIOMEDICINE: DESIGNING SYSTEMS THAT CAN ADAPT TO CHANGING KNOWLEDGE 2 (Kathryn J. Hannah & Marion J. Ball eds., 2011).

201. Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081, 1116 (2024).

202. *Id.*

203. SCHNEIER, *supra* note 178, at 23.

204. For examples of legal scholarship exploring privacy risks posed by metadata and Big Data, see generally 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; Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393 (2014); Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41 (2013), https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_41_RichardsKing.pdf [https://perma.cc/3JK5-X6ZE]; and Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014).

Moreover, it is the collection of each and every user's personal data that enables the creation of data sets required for many product designs, targeted advertisements, modeling, etcetera. The mere existence of current individually focused opt-out schemes for cookies and personal data underscores the importance and value of one person's individual data in the new digital market.[205] Recent state legislative efforts for personal data privacy have incorporated rights such as the right to deletion, the right to correction, the right to data portability,[206] and the right to access personal information and know what data is being collected.[207] The inclusion of such rights further points to the importance of an *individual's* data and the importance of an individual's ability to have control over their data.[208]

The White House also published the *Blueprint for an AI Bill of Rights*, which underscores these individual data privacy rights.[209] While the Blueprint "is nonbinding and does not constitute U.S. government policy," "[i]t is intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems."[210] The Data Privacy principle in the Blueprint emphasizes personal agency by stating that "[y]ou should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."[211] It further explains: "Designers, developers, and deployers of automated systems should seek your permission and respect your decisions regarding collection, use, access, transfer, and deletion of your data in appropriate ways and to the greatest extent possible . . . ."[212]

Lastly, data could reveal personality traits unique to each user, which are then used to manipulate consumers. "Cambridge Analytica used personality information to manipulate people on Facebook to vote for" a certain presidential candidate or make a decision on Brexit.[213] Daniel Solove cites to a study that showed "matching the content of persuasive appeals to individuals' psychological characteristics significantly altered their behavior as measured by clicks and

205. *See* Sarah Rippy, *Opt-In vs. Opt-Out Approaches to Personal Information Processing*, INT'L ASS'N PRIV. PROS.: THE PRIV. ADVISOR (May 10, 2021), https://iapp.org/news/a/opt-in-vs-opt-out-approaches-to-personal-information-processing/ [https://perma.cc/Z6ZN-9JCC].

206. Colorado Privacy Act, COLO. REV. STAT. § 6-1-1306(c)–(e).

207. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.110.

208. *See id.*; Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to -1313; Consumer Data Privacy and Online Monitoring, CONN. GEN. STAT. §§ 42-515 to -525; Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to -585; Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101 to -404.

209. *See* OFF. OF SCI. & TECH. POL'Y, EXEC. OFF. OF THE PRESIDENT, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 30 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/UB7D-PN2K].

210. *Id.* at 2.

211. *Id.* at 6.

212. *Id.*

213. Solove, *supra* note 201, at 37.

purchases."[214] Thus, the use of data to distill personality traits of consumers is illustrative of the importance of recognizing digital persona as likeness.

B. WHAT TYPE OF DATA?

Having laid out the argument for why data are personal and unique to each individual, the next pressing question is where to draw the line for such data protection. This Article stipulates that the threshold for what counts as our digital identity and personal likeness is "Personally Identifiable Information," known as PII, which is "any data that is identified or identifiable to a specific living individual."[215] A major problem with PII is that there is no uniform definition in the laws of the United States.[216] Paul Schwartz and Daniel Solove identify three approaches for defining PII: "(1) the 'tautological' approach, (2) the 'non-public' approach, and (3) the 'specific-types' approach."[217]

The tautological approach "defines PII as any information that identifies a person."[218] An example of this model is the Video Privacy Protection Act (VPPA), which defines PII "as 'information which identifies a person.'"[219] For reasons that will be explained below, this type of information falls neatly within the digital persona for purposes of the appropriation tort.

The "non-public" approach defines PII as "information not found within the public domain."[220] This definition of PII is not well-suited for digital persona protection. As Solove and Schwartz note: "The problem with the non-public approach is that it does not map onto whether the information is in fact identifiable. The public or private status of data often does not match up to whether it can identify a person or not."[221] Moreover, the appropriation tort historically includes protection of public aspects of one's identity, such as one's face. The use of one's publicly available image can still be valid grounds for a violation of the appropriation tort.

For example, in *Binion v. O'Neal*, the plaintiff sued NBA star Shaquille O'Neal, who had 8.6 million Twitter followers at the time, for committing the appropriation tort, among other allegations such as intentional infliction of emotional distress.[222] Mr. O'Neal used the plaintiff's selfie from the plaintiff's public

214. *Id.* at 38 (quoting Sandra C. Matz, Michal Kosinski, Gideon Nave & David J. Stillwell, *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 PROC. NAT'L ACAD. SCIS. 12714, 12714 (2017)).

215. PRINCIPLES OF THE L., DATA PRIV. § 2(b) (AM. L. INST. 2020).

216. 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, 1816 (2011).

217. *Id.* at 1828.

218. *Id.* at 1829.

219. *Id.* at 1829 & n. 73 (quoting Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(3)) ("The VPPA prohibits 'videotape service providers' from knowingly disclosing personal information, such as the titles of items rented or purchased, without the individual's written consent." (citing 18 U.S.C. § 2710(a)(4))).

220. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 795 (6th ed. 2018) (citing Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(4)(A)–(B)).

221. Schwartz & Solove, *supra* note 216, at 1830.

222. No. 15-60869, 2016 WL 111344, at *1–2 (S.D. Fla. Jan. 11, 2016).

Instagram page to create a post in which he appeared to mimic Mr. Binion's facial expression.[223] Mr. Binion was suffering from ectodermal dysplasia, a disease that made his facial expression appear "disfigured."[224] Applying Michigan law, the court concluded that plaintiff's appropriation claim survived a motion for summary judgment because the defendant had appropriated the plaintiff's likeness, noting that as a private figure, the plaintiff retained the right to protection of his likeness from use without his authorization.[225] This case illustrates that the appropriation tort has protected aspects of one's likeness that were publicly available but were acquired by third parties without authorization and for such third parties' personal gain.[226]

The third approach identified by Schwartz and Solove is listing the specific types of data that we want to protect in a rule-like format.[227] One example of this approach is the Children's Online Privacy Protection Act (COPPA) and its list of data as it relates to protecting children's digital privacy.[228] The problem with this method, as the authors also note, is the limitation of its scope.[229] Once the protected data have been listed, that puts a restriction on scenarios of privacy violations that may not have been anticipated.

The problem with this approach is particularly important for purposes of the appropriation tort, since the digital persona described in this Article should not be a fixed notion because "[t]he common law is not static, but is a dynamic and growing thing and its rules arise from the application of reason to the changing conditions of society."[230] As the evolution of the tort has shown, persona and likeness evolve to protect new aspects of oneself. Moreover, as it pertains to technological advancement, it is yet to be seen what kinds of data collection will be possible as the metaverse expands and grows into a digital universe. Therefore, listing certain data for protection would be counterintuitive in this context.

While none of the three approaches to defining PII are ideal, reliance on the tautological approach as a standard for identifying PII is a practical necessity to stop privacy law from "grow[ing] to regulate all information use."[231] Thus, for our purposes, the American Law Institute's *Data Privacy* recommendations are a well-suited framework. The Reporters opine that personal data "means any data that is identified or identifiable to a specific living individual."[232] This definition

223. *Id.* at *1.

224. *Id.*

225. *Id.* at *5.

226. This case also makes it clear that once we recognize the protection of digital persona by the appropriation tort, publicly available data can too, under the requisite circumstances, fall into the category of protected persona for the purposes of the appropriation tort.

227. Schwartz & Solove, *supra* note 216, at 1831.

228. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501(8). For a discussion on COPPA, see Takhshid, *supra* note 21.

229. Schwartz & Solove, *supra* note 216, at 1832.

230. McCormack v. Okla. Publ'g. Co., 613 P.2d 737, 740 (Okla. 1980) (citing Barnes Coal Corp. v. Retail Coal Merch.'s Ass'n, 128 F.2d 645, 648 (4th Cir. 1942)).

231. SOLOVE & SCHWARTZ, *supra* note 220, at 805.

232. PRINCIPLES OF THE L., DATA PRIV. § 2(b) (AM. L. INST. 2020).

"reflects the modern use of the term 'personally identifiable data.'"[233] Data are "'identifiable' when there is a moderate probability that [they] could be identified."[234] This is also in line with the global trend of defining personal data in terms of identifiability.[235]

An old privacy tort case that exemplifies the modern applicability of identifiable data for likeness is *Cohen v. Herbal Concepts, Inc*.[236] In *Cohen*, defendant James Krieger had taken a photo of a mother and daughter, without their permission, while they were bathing in a stream on a private property.[237] The photo depicted the mother and daughter from behind and to the right of them.[238] The defendant sold the photo, and it appeared in magazines for an advertisement.[239] Although the image did not depict their faces, Ira Cohen, the woman's husband and the father of the child, saw the image and instantly recognized his family.[240] The plaintiffs brought a privacy action under § 51 of the New York Civil Rights Law, which "protects against the appropriation of a plaintiff's name or likeness for defendants' benefit."[241] The defendant claimed that because the depicted plaintiffs were not identifiable, he had not committed a wrong.[242]

The New York Court of Appeals ruled in favor of the plaintiffs and stated:

> The statute is designed to protect a person's identity, not merely a property interest in his or her "name", "portrait" or "picture", and thus it implicitly requires that plaintiff be capable of identification from the objectionable material itself . . . . That is not to say that the action may only be maintained when plaintiff's face is visible in the advertising copy.[243]

The court noted that "identifiability may be enhanced also in a photograph depicting two persons because observers may associate the two and thus more easily identify them when they are seen together."[244]

In its modern-day application, this analysis can apply to the challenges of metadata and its ability to allow an individual to be identified by inference.[245]

---

233. *Id.* § 2 cmt. b.

234. *Id.* § 2 cmt. c.

235. Solove, *supra* note 201, at 7 (citing Graham Greenleaf, *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*, 168 PRIV. L. & BUS. INT'L REP. 13, 15 (2020)). This PII approach is robust and encompasses the concept of "sensitive data"—data that includes categories such as racial origins, religious beliefs, health, and sexual orientation. GENERAL DATA PROTECTION REGULATION art. 9, ¶ 1(Eur.). For a full discussion on the history of sensitive data, see Solove, *supra* note 201, at 8–18.

236. 472 N.E.2d 307 (N.Y. 1984).

237. *Id.* at 308.

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.* The plaintiff also argued for defamation. *Id.*

242. *Id.* at 309.

243. *Id.* (citations omitted).

244. *Id.*

245. An example of this can be found with telephone metadata, such as the numbers you dial and the lengths of your calls. In a 2016 Stanford University study, researchers were able to infer that an individual who received a long phone call from the cardiology group at a regional medical center,

Scholars have identified inference as a problem for categorizing certain data, such as sensitive data, for protection.[246] Inference allows "organizations [to] use available data collected from individuals to generate further information about both those individuals and about other people."[247] Solove argues that inference allows for data that are otherwise not personal to fall into the sensitive data category because those data allow for inference that leads to identification.[248] This way, carving out "sensitive data would swallow up nearly all personal data."[249] But this worry for the purposes of the appropriation tort is not warranted. A canonical feature of the common law is the balancing tests established and applied by courts case by case. Similar contextual and case-by-case analysis can be envisioned by courts in evaluating the extent of identifiable data that would constitute the commission of the tort of appropriation. In *Cohen*, the court stated that the evaluation of the plaintiffs' claim to survive a motion to dismiss "will necessarily depend upon the court's determination of the quality and quantity of the identifiable characteristics displayed in the advertisement and this will require an assessment of the clarity of the photograph, the extent to which identifying features are visible, and the distinctiveness of those features."[250] Courts can apply similar evaluations based on the characteristics of data and their identifiable features. This flexibility is also necessary to allow the digital persona and likeness concept to shape and evolve as technological advancements continue to develop.[251]

Dean Prosser "understood that, if tort law were to continue to be a high-status field within the law, it needed to be re-imagined. Instead of being thought of as (old fashioned, regressive, formalistic) private law, it had to be seen as law that empowers courts to engage in 'social engineering.'"[252] Thus, digital persona and likeness, for purposes of the appropriation tort, encompass an individual's PII as defined by the Data Privacy Principles and analyzed by courts in each case.

C. CONSENT

Another challenge for the application of data as likeness is bypassing the lack of consent requirement of the appropriation tort. It is sensible to ask whether—with technologies heavily relying on tailored and increasingly sophisticated

answered several calls from a local drugstore, and placed calls to a self-reporting hotline for a cardiac arrhythmia monitoring device likely suffers from cardiac arrhythmia. Jonathan Mayer, Patrick Mutchler & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROC. NAT'L ACAD. SCIS. 5536, 5540 (2016).

246. *See, e.g.*, Solove, *supra* note 201, at 22.

247. Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022). Solow-Niederman calls this the "inference economy." *Id.* (emphasis omitted).

248. Solove, *supra* note 201, at 22.

249. *Id.*

250. Cohen v. Herbal Concepts, Inc., 472 N.E.2d 307, 309 (N.Y. 1984).

251. This is also in line with the position of the reporters of *The Principles of the Law, Data Privacy*, who note that computer scientists will continue to "develop different preferred methodologies for use in different contexts." *See* PRINCIPLES OF THE L., DATA PRIV. § 2(d) cmt. d (AM. L. INST. 2020).

252. John C. P. Goldberg, *Benjamin Cardozo and the Death of the Common Law*, 34 TOURO L. REV. 147, 153 (2018) (citing WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS § 3 at 25 (1941)).

boilerplate contracts, privacy policies, user agreements, and browsewraps[253]—there is any room left to claim that one's data were collected without consent. At times, a mere sign-in or checking "accept and continue" has resulted in courts ruling in favor of the formation of a contract.[254] More recently, the American Law Institute's Restatement of Consumer Contracts proposed "a highly simplified model for the enforceability of consumer contract," by which boilerplate assent is enforceable but "the domain of possible unconscionable provisions that courts could identify is expanded."[255]

To overcome this skepticism, it is crucial to note that many scholars take a stand against the validity of boilerplate contracts.[256] Boilerplate contracts become even more problematic in the context of online activities because of the often-dubious methods by which a user's consent is allegedly acquired. As Gregory Klass notes, "[I]t is not yet settled whether the fact that a business provides notice of how it uses consumer information—for example, by posting its privacy policy online—establishes effective consumer consent to that use."[257] And consumers continue to challenge the terms and their alleged consent in court on various grounds such as a violation of public policy or the doctrine of unconscionability.[258]

The scope of the consent granted by individuals to these companies is also well-litigated. Consider *McCoy v. Alphabet, Inc.* and the court's treatment of a

253. "[B]rowsewraps" are "statements of terms of use placed on a website that claim that the mere use of the website constitutes agreement to the terms." Mark A. Lemley, *The Benefit of the Bargain*, 2023 WIS. L. REV. 237, 251.

254. *Id.* at 252 n.71 (discussing *Nevarez v. Forty Niners Football Co.*, No. 16-CV-07013, 2017 WL 3492110 (N.D. Cal. Aug. 15, 2017), which "enforce[ed] a browsewrap contract that 'prominently informed [users] on at least two occasions prior to [the purchase]'" that they were agreeing to the terms of service of the webpage, and, "since they clicked 'Accept and Continue' or 'Sign In,' and after that 'Submit Order' . . ." had assented to the terms of service "'which were always hyperlinked and available for review'" (second and third alterations in original)).

255. Benjamin C. Zipursky & Zahra Takhshid, *Consumer Protection and the Illusory Promise of the Unconscionability Defense*, 103 TEX. L. REV. (forthcoming) (manuscript at 6) (citing RESTATEMENT OF THE LAW, CONSUMER CONTRACTS: TENTATIVE DRAFT NO. 2 (AM. L. INST. 2022)), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4777902.

256. *See generally, e.g.*, Nancy S. Kim, *Developments in Digital "Wrap" Contracts*, 77 BUS. LAW. 275 (2021); MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013); Gregory Klass, *Boilerplate and Party Intent*, 82 LAW & CONTEMP. PROBS. 105 (2019); Emily Strauss, *Crisis Construction in Contract Boilerplate*, 82 LAW & CONTEMP. PROBS. 163 (2019); NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (2013); Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002).

257. Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 48 (2019). Moreover, "[m]ost sites provide that their terms will change periodically and that the user is automatically bound to those changed terms." Lemley, *supra* note 253, at 253 n.76.

258. *See* Lemley, *supra* note 253, at 255; Klass, *supra* note 257, at 48 (discussing whether proper notice establishes effective consumer consent); Zahra Takhshid, *Assumption of Risk in Consumer Contracts and the Distraction of Unconscionability*, 42 CARDOZO L. REV. 2183, 2183 (2021) (arguing that "unconscionability doctrine should be kept out of the law of express assumption of risk"). Some courts have found that use of a product did not constitute acceptance. *See, e.g.*, Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1341 (D. Kan. 2000) (holding that "the act of keeping [a product] past five days [is] not sufficient to demonstrate that [a] plaintiff expressly agreed to" a contract's terms).

privacy policy.[259] In a class action lawsuit, the plaintiff sued defendant Google, LLC[260] and alleged "that [the d]efendant ha[d] been using an internal program [on Android phones] to monitor and collect sensitive personal data when users use[d] non-Google applications ('apps')."[261] Mr. McCoy alleged that such collection of data fell outside of the defendant's privacy policy. He alleged that the "Privacy Policy d[id] not adequately disclose or seek consent" for such monitoring, collection, and use of sensitive personal data.[262] Moreover, "while users are told [the d]efendant will collect personal data 'to offer a more personalized experience,'" the defendant used the sensitive personal data for its own benefit to "obtain lucrative behind the scenes technical insight that it can use to develop competing apps against its competitors."[263]

In this case, the court analyzed the privacy policy to determine whether consent was adequate for this data practice.[264] The plaintiff alleged that the language of the consent form was vague in explaining how the collected data were used and "set[] forth misleading examples of using collected data."[265] The court noted that the phrase "'[a]ctivity on third-party sites and apps that use our services' may not be understood by a reasonable user to include data from apps that are not associated with [the d]efendant's services."[266] It sided with the plaintiff and stated that the privacy policy did not offer the level of specificity to allow for a motion to dismiss or an absolute bar to the plaintiff's claims.[267] This case is a good illustration of courts allowing a lawsuit for unauthorized data collections to move forward despite a complicated and lengthy privacy policy.

Another case that is illustrative of bypassing the consent objection is *Thornley v. Clearview AI, Inc*.[268] The plaintiffs sued Clearview AI, alleging violation of Section 15(c) of Illinois's Biometric Information Privacy Act (BIPA).[269] The law states, "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[270] While the court rejected the

259. No. 20-cv-05427, 2021 WL 405816, at *6 (N.D. Cal. Feb. 2, 2021).

260. Defendant Alphabet, Inc. was dismissed. *Id*. at *1 n.1.

261. *Id*. at *1.

262. *Id*.

263. *Id*.

264. *Id*. at *4–5.

265. *Id*. at *5.

266. *Id*. at * 6.

267. *See id*. The court distinguished this case from *Smith v. Facebook, Inc*., 745 F. App'x 8 (9th Cir. 2018), in which the court had ruled in favor of Facebook by determining that its terms and policies constituted adequate disclosure and consent. *See id*.

268. 984 F.3d 1241 (7th Cir. 2021).

269. *Id*. at 1242, 1246.

270. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(c). Notably, a 2021 New York City ordinance allowed business owners to display "signs posted at shop doors" as a replacement for "obtaining explicit consent before biometric data [are] collected." Hayley Tsukayama, *Trends in Biometric Information Regulation in the USA*, ADA LOVELACE INST. (July 5, 2022), https://www.adalovelaceinstitute.org/blog/biometrics-regulation-usa/ [https://perma.cc/QB2Y-4RSP]. Regulations such as this undermine consent requirements because a sign posted on a business door may be missed, not understood, or, most likely, not be sufficient in explaining to a consumer all of the ways in which their biometric data may be used. *Id*.

claim as too narrow to satisfy an Article III standing challenge in this specific case,[271] the concurring opinion noted that it could envision similar lawsuits that would satisfy standing in cases such as when "a person who has consented to collection, retention, and use of her biometric information, perhaps for non-profit scientific research, . . . objects to the sale of her data to a third party."[272] As such, challenging the scope of the consent remains an opportunity for many data collection and unauthorized use of data lawsuits that can invoke the appropriation of likeness tort.

D. STANDING

This Article's approach can further assist with questions of standing that have been a challenge for plaintiffs bringing data privacy claims to courts. Using this tort in the context of data privacy, plaintiffs can overcome the concrete injury dilemma.[273] An application of this concept is echoed in the concurring opinion in *Thornley v. Clearview AI, Inc*. As previously discussed, in *Thornley* the court ruled that Ms. Thornley and her co-plaintiffs had no Article III standing.[274] Despite the unauthorized data collection, they had allegedly "suffered no injury from [the] [d]efendant's violation of Section 15(c) of BIPA other than statutory aggrievement."[275] However, the concurring opinion offered a way forward. Judge Hamilton of the Seventh Circuit stated that the ruling was "determined by the choices that these plaintiffs ha[d] made to narrow both their claims and the scope of their proposed class."[276]

Judge Hamilton wrote that it is possible to have standing to sue for unauthorized collection and use of data.[277] In such cases, "[t]he resulting injury . . . would be comparable to injuries in invasion-of-privacy and unjust enrichment cases that the law has long recognized."[278] Here, Judge Hamilton cited to the Restatement (Second) of Torts § 652C, which covers the tort of appropriation of another's name or likeness for one's own use or benefit.[279] The concurring opinion further noted: "In fact, the misuse of a person's biometric information presents an especially dangerous modern version of these traditional injuries. A victim of identity theft can obtain a new email address or even Social Security number, but

271. *Thornley*, 984 F.3d at 1242. The court noted that "they have described only a general, regulatory violation, not something that is particularized to them and concrete." *Id.* at 1248.

272. *Id.* at 1249 (Hamilton, J., concurring).

273. The U.S. Supreme Court has held that, in order to have Article III standing, a "plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest which is . . . concrete and particularized, and . . . 'actual or imminent, not "conjectural" or "hypothetical."'" Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (citations omitted) (first quoting Allen v. Wright, 468 U.S. 737, 756 (1984); and then quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

274. *Thornley*, 984 F.3d at 1248.

275. *Id.* at 1246.

276. *Id.* at 1249 (Hamilton, J., concurring).

277. *Id.*

278. *Id.*

279. *Id.*

'biometric identifiers . . . are immutable, and once compromised, are compromised forever.'"[280]

The acknowledgment that biometric identifiers are immutable is a clear indication of circuit courts' willingness to recognize and adopt the approach advocated herein. Indeed, the tort of appropriation in such cases does not require any physical or emotional concrete injury. The unauthorized use of one's data for the benefit of the user can suffice to trigger the tort.

Thus, the recognition of data as likeness can further assist with questions of the Article III standing requirement raised in *TransUnion LLC v. Ramirez*.[281] In *TransUnion*,

> the Supreme Court held that some members of a class lacked standing to bring claims under the Fair Credit Reporting Act (FCRA) because they lacked a concrete injury when TransUnion erroneously included an alert for creditors that class members were linked to a Treasury Department terrorist database, but had not yet disseminated those files.[282]

Writing for the majority, Justice Kavanaugh stated: "Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm."[283]

As commentators have noted, this ruling complicated satisfying the requirement for an injury-in-fact to sue for data and privacy rights violations by requiring a common law nexus.[284] However, recognizing data protection through the lens of tort law can help many plaintiffs overcome this hurdle of proving standing for many personal data-related privacy violations.[285] Data as likeness is benefiting from the evolving nature of the common law. Common law has historically protected privacy through the so-called dignitary torts. Interests underlying data protection are at the core of privacy torts and, in particular, the appropriation tort. As noted in the Introduction, two of the four interests at the core of the appropriation tort's protection are the right of control and the right of dignity.[286] Both of these

280. *Id.* (alteration in original) (quoting Fox v. Dakkota Integrated Sys. LLC, 980 F.3d 1146, 1155 (7th Cir. 2020)).

281. 594 U.S. 413 (2021).

282. Comment, *Article III Standing — Separation of Powers — Class Actions* — TransUnion v. Ramirez, 135 HARV. L. REV. 333, 333 (2021) (footnote omitted).

283. *TransUnion*, 594 U.S. at 417 (citing Spokeo, Inc. v. Robins, 578 U.S. 330, 340–41 (2016)).

284. Solove & Citron, *Standing and Privacy*, *supra* note 25, at 67–69.

285. For how this would apply to children's data, see Takhshid, *supra* note 21.

286. Post & Rothman, *supra* note 29, at 116, 121. As previously explained, the author uses the right of publicity to include appropriation. While the author believes that data protection measures are addressed in the interest of having a right to control, the author believes that the right of dignity in the appropriation tort is also an aspect of data privacy rights and that an action need not be highly offensive to trigger the dignitary interest in the appropriation tort. The author reserves this discussion for future work.

interests underscore the need for data privacy protection and can square easily with the *TransUnion* standing requirement.

Indeed, in a recent multi-district litigation, *In re Clearview AI, Inc., Consumer Privacy Litigation*, the case survived an Article III standing challenge despite the defendant's efforts, relying on *TransUnion* and *Thornley*.[287] In this case, the plaintiffs brought a class action against Clearview AI, Inc. (Clearview) and its executives, *inter alia*, "under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA"), as well as statutory and common law claims under Virginia, California, and New York law."[288]

Ultimately, the court found that the plaintiffs had Article III standing.[289] In denying the defendants' motion for reconsideration, the court stated that the "defendants' reliance on *TransUnion* for the proposition that a victim of a privacy harm can only suffer an injury-in-fact for Article III standing if the victim's information is disseminated to a third-party is also unavailing."[290] The court distinguished its case from *TransUnion*: "In *TransUnion*, the Supreme Court analogized the FCRA violations to the tort of defamation, which requires that the defamatory statement be published to a third party."[291] But as it relates to data collection and the Clearview AI lawsuit, "[t]he Seventh Circuit has analogized BIPA violations to common law privacy torts, which are different common law torts than defamation."[292] They have different requirements, and in the case of the appropriation tort, do not involve dissemination.[293] In denying the defendants' motion for reconsideration, the court also noted that because the "defendants' arguments concerning Article III standing and plaintiffs' state law claims were made for the first time in their reconsideration motion," the claims were waived.[294] The court's willingness to distinguish *TransUnion* and to compare BIPA to common law privacy torts is a promising decision in allowing such claims to move forward by relying on common law privacy torts.[295]

---

287. 585 F. Supp. 3d 1111, 1119, 11126 (N.D. Ill. 2022).

288. *Id*. at 1118.

289. *Id*. at 1126.

290. *In re* Clearview AI, Inc., Consumer Priv. Litig., No. 21-cv-0135, 2022 WL 2915627, at *3 (N.D. Ill. July 25, 2022).

291. *Id*.

292. *Id*. at *4.

293. While many cases of the appropriation tort involve dissemination of an image, or likeness, dissemination it is not an element of the tort as defined by the Restatement. *See supra* note 120 and accompanying text.

294. *Clearview*, 2022 WL 2915627, at *4.

295. *See* Renderos v. Clearview AI, Inc., No. RG21096898, 2022 WL 17326440, at *8 (Cal. Super. Ct. Nov. 18, 2022). The *Clearview* court also quoted *Bryant v. Compass Group USA, Inc*.: "Bryant was asserting a violation of her own rights—her fingerprints, her private information—and . . . this is enough to show injury-in-fact without further tangible consequences. This was no bare procedural violation; it was an invasion of her private domain, much like an act of trespass would be." *Clearview*, 2022 WL 2915627, at *4 (quoting Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 624 (7th Cir. 2020)).

E. DATA AS LIKENESS AND THE FIRST AMENDMENT

The First Amendment doctrine "prohibits the government from 'abridging the freedom of speech.'"[296] "Preserving privacy, however, by definition often impedes the free flow of information."[297] And as state law torts are designed to prevent certain actions that at times entail different forms of speech, a defendant understandably may rely on their First Amendment rights to avoid liability or justify their actions. Nevertheless, courts have retained privacy torts by carving out First Amendment exceptions and balancing the competing interests.[298]

For example, in *Zacchini v. Scripps-Howard Broadcasting Co.*, the Supreme Court determined "whether the First and Fourteenth Amendments immunized respondent from damages for its alleged infringement of petitioner's state law 'right of publicity.'"[299] The defendant televised the entirety of an actor's performance involving a human cannonball. The Court, applying state law, sided with the plaintiff and upheld the right of publicity claim.[300] *Zacchini* often stands for "the broad proposition that '[t]here is no First Amendment privilege with respect to the appropriation of another's name or likeness for commercial purposes.'"[301]

Scholars have noted that First Amendment doctrine and its interplay with the appropriation tort lack clarity and have created chaos,[302] but for the purposes of this Article's argument, it is important to note that the torts themselves have survived, and courts have found ways to accommodate competing interests while recognizing First Amendment defenses such as newsworthiness, public interest, parody, etcetera, as they relate to privacy rights.[303]

---

296. Jordan v. Jewel Food Stores, Inc., 743 F.3d 509, 515 (7th Cir. 2014) (quoting U.S. CONST. amend. I).

297. NOAH R. FELDMAN & KATHLEEN M. SULLIVAN, FIRST AMENDMENT LAW 90 (7th ed. 2019).

298. *See, e.g.*, Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 565–66 (1977) (holding that the First Amendment does not immunize respondent from damages for alleged infringement of petitioner's right of publicity); Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1234–35 (7th Cir. 1993) (balancing a publisher's right to discuss another's "intimate physical details" in their writings with the embarrassment, pain, and shock felt "by the average person subjected to such exposure"); *In re* NCAA Student–Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1271 (9th Cir. 2013) (balancing the right of publicity against the First Amendment right to use another's likeness in expressive works); Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 478 (Cal. 1998) (finding newsworthiness to be an element of the tort for publication of private facts and concluding that "newsworthiness inevitably involves accommodating conflicting interests in personal privacy and in press freedom as guaranteed by the First Amendment").

299. 433 U.S. at 565.

300. *Id.* at 578–79.

301. Post & Rothman, *supra* note 29, at 126 (alteration in original) (quoting Fitzgerald v. Penthouse Int'l, Ltd., 525 F. Supp. 585, 601–02 n.79 (D. Md. 1981), *aff'd in part, rev'd in part*, 691 F.2d 666 (4th Cir. 1982)). In a recent federal decision, a district court distinguished the New York statutory right of publicity interest from that of a common law right of publicity, noting that the former is "not about property at all," but rather about an injury to the person. Ratermann v. Pierre Fabre USA, Inc., No. 22-CV-325, 2023 WL 199533, at *6 (S.D.N.Y. Jan. 17, 2023).

302. *See* Post & Rothman, *supra* note 29, at 127.

303. For an in-depth analysis, see Gloria Franke, Note, *The Right of Publicity vs. the First Amendment: Will One Test Ever Capture the Starring Role?*, 79 S. CAL. L. REV. 945, 946 (2006); Natasha Singer, *Students Target Teachers in Group TikTok Attack, Shaking Their School*, N.Y. TIMES (July 6, 2024) https://www.nytimes.com/2024/07/06/technology/tiktok-fake-teachers-pennsylvania.html.

We must now consider how a First Amendment challenge may be invoked with regards to personal data collection and the applicability of the appropriation tort. In *Sorrell v. IMS Health Inc.*, the majority opinion of the Supreme Court noted that "the creation and dissemination of information are speech within the meaning of the First Amendment."[304] *Sorrell* involved Vermont data miners and an association of brand-name drug manufacturers that challenged a Vermont law as against their free speech rights enshrined in the First Amendment.[305] The law provided that unless the prescriber consented, "the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors . . . may not be sold, disclosed by pharmacies for marketing purposes, or used for marketing by pharmaceutical manufacturers."[306]

The state argued that "the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech."[307] It further argued that the law "regulates not speech but simply access to information."[308] The Court disagreed and ruled that § 4631(d) "impose[d] a burden based on the content of speech and the identity of the speaker."[309] It also noted that "[t]here is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes."[310]

The state also invoked the commercial speech argument, which involves a lesser degree of scrutiny, or an "intermediate" test.[311] To prove that a law is constitutionally regulating commercial speech, "the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest."[312] The Supreme Court disagreed as it applied the test to the Vermont law. It stated that the law was too broad and that Vermont could have addressed physician confidentiality through other policies or "advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances."[313]

---

304. 564 U.S. 552, 570 (2011).

305. *Id.* at 561.

306. *Id.* at 557; *see also* VT. STAT. ANN. tit. 18, § 4631(d) ("A health insurer, a self-insured employer, an electronic transmission intermediary, a pharmacy, or other similar entity shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use of regulated records containing prescriber-identifiable information for marketing or promoting a prescription drug, unless the prescriber consents as provided in subsection (c) of this section. Pharmaceutical manufacturers and pharmaceutical marketers shall not use prescriber-identifiable information for marketing or promoting a prescription drug unless the prescriber consents as provided in subsection (c) of this section.").

307. *Sorrell*, 564 U.S. at 567.

308. *Id.*

309. *Id.*

310. *Id.* at 570.

311. *Id.* at 571. As the dissent noted, "[T]he First Amendment imposes tight constraints upon government efforts to restrict, *e.g.*, 'core' political speech, while imposing looser constraints when the government seeks to restrict, *e.g.*, commercial speech, the speech of its own employees, or the regulation-related speech of a firm subject to a traditional regulatory program." *Id.* at 582 (Breyer, J., dissenting).

312. *Id.* at 572 (majority opinion).

313. *Id.* at 573, 575.

Despite this ruling, the Supreme Court also noted in its decision that "[t]his is not to say that all privacy measures must avoid content-based rules. Here, however, the State has conditioned privacy on acceptance of a content-based rule that is not drawn to serve the State's asserted interest."[314] It further stated:

> The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.[315]

Thus, while a law could have been too broad in a specific case, that would not negate the possibility of imposing limitations on data collection as it relates to personally identifiable data, such as facial biometrics, and invoking the appropriation tort.[316]

Commentators have also observed that there is no need to interpret *Sorrell* broadly.[317] For one thing, "*Sorrell* specifically approved the Health Insurance Portability and Accountability Act (HIPAA), even though HIPAA far more strictly restrains the transmission of information than does the Vermont law *Sorrell* found unconstitutional."[318] Post and Rothman note that "[i]nsofar as a person's identity is a matter of public information, the state cannot create rules that constrain its use in public discourse, except for specific, narrow, and compelling reasons."[319] However, as they observe:

> Regulating the storage, sale, and manipulation of privately held data, however, is quite different from regulating public discussion based on otherwise public information. It is one thing to prevent Google from selling data gathered from its surveillance of our online searches; it is quite another to prevent Google from communicating to the general public otherwise publicly available information on the web. Freedom of public discourse entails the latter, but not the former.[320]

Contemporary cases against Clearview AI and its facial recognition technology affirm the position that the data-as-likeness concept can survive First Amendment

314. *Id.* at 574. In using the term "content-based rule," the Court is referring to rules based in large part on the content of the speech, as opposed to "speaker-based" rules or restrictions that disfavor certain speakers. *Id.* at 564.

315. *Id.* at 579–80.

316. *See In re* Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1120 (N.D. Ill. 2022) (citing *Sorrell*, 564 U.S. at 570).

317. Post & Rothman, *supra* note 29, at 163 n.332.

318. *Id.* at 164 n.332.

319. *Id.* at 163.

320. *Id.*

challenges.[321] To reiterate, my purpose here is to show that the data-as-likeness concept will not be "swallowed" by First Amendment challenges.[322] Needless to say, carving out exceptions and balancing the two competing interests will be on the agenda for the courts because the theory would apply differently in each case.

Consider *Renderos v. Clearview AI, Inc*.[323] In *Renderos*, the plaintiffs are suing Clearview AI, Inc. (Clearview), claiming invasion of privacy based on, *inter alia*, the violation of the common law right of publicity and California's constitutional right to privacy.[324] They allege that Clearview has "illicitly collect[ed] over three billion photographs of unsuspecting individuals," with its database "almost seven times the size of the FBI's."[325] As the complaint explains:

> After obtaining these images, Clearview uses algorithms to extract the unique facial geometry of each individual depicted in the images, creating a purported "faceprint" that serves as a key for recognizing that individual in other images, even in photographs taken from different angles. Clearview's "faceprints" rely on an individual's immutable biological characteristics—for example, the position, size, and shape of the eyes, nose, cheekbones, and jaw—to purportedly capture their biometric signature.[326]

This means that Clearview can also use the collected faceprints in the future.[327] The company has provided its services to law enforcement, including "several police agencies across California."[328] Accordingly, the complaint invokes the appropriation tort and alleges that:

> Without providing notice to or obtaining consent from Plaintiffs and Plaintiffs' members, Clearview knowingly and surreptitiously collected Plaintiffs' and Plaintiffs' members' names, photographs, biometric information, and other identifiers (which constitute Plaintiffs' and Plaintiffs' members'

321. *See* Kaixin Fan, *Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data*, HARV. J.L. & TECH. (Feb. 25, 2020), https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data [https://perma.cc/M9WA-DFW7].

322. In *Shulman v. Group W Productions, Inc*., the court was deciding whether newsworthiness would prevail over a claim for publication of private facts and intrusion upon seclusion against a media company. 955 P.2d 469 (Cal. 1998), *as modified on denial of reh'g* (July 29, 1998). In that case, the court noted that "[i]f 'newsworthiness' is completely descriptive — if all coverage that sells papers or boosts ratings is deemed newsworthy — it would seem to swallow the publication of private facts tort, for 'it would be difficult to suppose that publishers were in the habit of reporting occurrences of little interest.'" *Id*. at 481 (quoting Comment, *The Right of Privacy: Normative-Descriptive Confusion in the Defense of Newsworthiness*, 30 U. CHI. L. REV. 722, 734 (1963)).

323. *See* Complaint, *supra* note 186.

324. *Id*. at 19–21; *see also* CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

325. Complaint *supra* note 186, at 1.

326. *Id*.

327. *Id*. at 19.

328. *Id*. at 14.

> "identities") by scraping images from websites in violation of many of the websites' policies prohibiting such conduct.[329]

All of which collectively amounts to "data as likeness," or the collection and use of an individual's digital persona, as this Article has argued.

While a final decision in this lawsuit and the ability of this tort to challenge the use of facial recognition technologies remain to be seen,[330] in a small victory for the plaintiffs, the Superior Court of California denied Clearview AI's motion to dismiss the complaint as a strategic lawsuit against public participation (SLAPP).[331] In California, the "anti-SLAPP statute is designed to discourage suits that 'masquerade as ordinary lawsuits but are brought to deter common citizens from exercising their political or legal rights or to punish them for doing so.'"[332] Most SLAPP complaints involve First Amendment free speech challenges.[333]

In this case, the Superior Court of California noted that to survive a SLAPP motion to dismiss, the court applies a two-step legal test. First, it must determine "whether the moving party has made a showing that the acts complained of were 'arising from any act of [the defendant] in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue.'"[334] Second, the court "must evaluate whether the plaintiff has 'establish[ed] a reasonable probability that the plaintiff will prevail on his or her . . . claim."[335]

The California court ruled that Clearview "ha[d] not demonstrated that the claims arise from its actions 'in furtherance of' free speech 'in connection with[] a public issue.'"[336] It noted that "the biometric analysis and maintenance of the database and the subsequent sale of that information [was] not 'conduct in furtherance of . . . the constitutional right of free speech in connection with a public issue or an issue of public interest.'"[337] Importantly, the court ruled that "[t]he biometric analysis and maintenance of the database *is not 'speech.'*"[338] The court ruled that "[t]he sale of the biometric data is not protected by the First

---

329. *Id.* at 20. To clarify, the complaint alleges that scraping the plaintiffs' and plaintiffs' members' images from websites is a violation of many of the websites' policies. The complaint does not suggest that plaintiffs or plaintiffs' members bear the responsibility of objecting to such practices. *See id.*

330. For a full analysis of the applicability of the right of publicity to challenge facial recognition technologies, see Schultz, *supra* note 44, at 1050–63.

331. Renderos v. Clearview AI, Inc., No. RG21096898, 2022 WL 17326440, at *2 (Cal. Super. Ct. Nov. 18, 2022).

332. *In re* NCAA Student–Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1272 (9th Cir. 2013) (quoting Batzel v. Smith, 333 F.3d 1018, 1024 (9th Cir. 2003)).

333. "[T]he common features of SLAPP suits are their lack of merit and chilling of defendants' valid exercise of free speech and the right to petition the government for a redress of grievances." Wilcox v. Superior Ct., 33 Cal. Rptr. 2d 446, 454 (Ct. App. 1994), *as modified on denial of reh'g* (Sept. 15, 1994).

334. *Renderos*, 2022 WL 17326440, at *2–3 (alteration in original) first citing CAL. CIV. PROC. CODE § 425.16(b)(1); and then citing Navellier v. Sletten, 52 P.3d 703, 708 (2002)).

335. *NCAA*, 724 F.3d at 1273 (alterations in original) (citing *Batzel*, 333 F.3d at 1024).

336. *Renderos*, 2022 WL 17326440, at *3 (citing CAL. CIV. PROC. CODE § 425.16(b)(1)).

337. *Id.* (second alteration in original) (citing CAL. CIV. PROC. CODE § 425.16(e)(4)).

338. *Id.* (emphasis added).

Amendment in the same way that the sale of t-shirts with 'literal, conventional depictions of the Three Stooges' is not protected by the First Amendment."[339]

The court further stated that

> [a] person does not have a [F]irst Amendment right to appropriate a photograph or likeness of another person and then use it for a profit-making business. . . . This is a business that is based on aggregating and analyzing photographs of California residents and then selling the data related to those images.[340]

This ruling was consistent with the federal court ruling in *In re Clearview AI, Inc., Consumer Privacy Litigation* that was discussed in connection with standing.[341] In this case, "the Clearview defendants maintain[ed] that the capture of faceprints from public images and Clearview's analysis of the public faceprints is protected speech."[342] However, the plaintiffs "assert[ed] that the capturing of faceprints and the action of extracting private biometric identifiers from the faceprints is unprotected conduct."[343] In other words, "Clearview defendants' business model is not based on the collection of public photographs from the internet, some source code, and republishing information via a search engine, but the additional conduct of harvesting nonpublic, personal biometric data."[344]

The court agreed with the plaintiffs and stated that "Clearview's process in creating its database involves both speech and nonspeech elements" and thus applied the intermediate scrutiny standard to BIPA and denied the defendants' motion to dismiss in this respect.[345] The court further noted that the plaintiffs had plausibly stated a common law right to publicity claim as well.[346]

These contemporary decisions demonstrate the possibility of the data-as-likeness theory surviving a First Amendment challenge. Not all cases will involve transmission of data to third parties, and while the act of collecting and maintaining the database does not necessarily trigger First Amendment protections, it could potentially invoke the appropriation tort if used in other ways for the third parties' own benefit.

Common law cases provide illustrations of the law protecting privacy while also balancing First Amendment concerns. In 2020, New York's statutory right of publicity was expanded to include a postmortem right of publicity that encompasses a digital likeness of a "deceased performer[]" called a "digital replica."[347] The law defines this as

> a newly created, original, computer-generated, electronic performance by an individual in a separate and newly created, original expressive sound recording

339. *Id.* at *4 (citing Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797 (Cal. 2001)).
340. *Id.*
341. 585 F. Supp. 3d 1111 (N.D. Ill. 2022).
342. *Id.* at 1120.
343. *Id.*
344. *Id.*
345. *Id.* at 1120–21.
346. *Id.* at 1129.
347. N.Y. CIV. RIGHTS LAW § 50-f(2)(b).

> or audiovisual work in which the individual did not actually perform, that is so realistic that a reasonable observer would believe it is a performance by the individual being portrayed and no other individual.[348]

This law also carved out First Amendment-related exemptions.[349] They include a work that

> is a play, book, magazine, newspaper, or other literary work; musical work or composition; work of art or other visual work; work of political, public interest, educational or newsworthy value, including comment, criticism, parody or satire; audio or audiovisual work, radio or television program, if it is fictional or nonfictional entertainment; or an advertisement or commercial announcement for any of the foregoing works.[350]

The New York law continues to add other protected categories to the list. Similar exemptions can be applied to handling common law data and likeness claims in a manner that is aligned with the First Amendment's requirements while preserving individuals' data privacy. In the words of Justice Greenfield, "If we truly value the right of privacy in a world of exploitation, where every mark of distinctiveness becomes grist for the mills of publicity, then we must give it more than lip service and grudging recognition."[351] By allowing the likeness concept to encompass personal data while recognizing First Amendment exemptions, states and courts can succeed in elevating citizens' data protection and information privacy measures via the common law of torts.

CONCLUSION

Our data are personal and can reveal intimate information about us. From the color of one's eye to one's religion, data in the digital age have become the most-used aspect of our identities by third parties. The tort of appropriation of likeness has historically offered protection to one's identity. Its protection expanded from mere image to the protection of one's persona—encompassing broader aspects of identity. It is now time for the common law to recognize data as likeness, that our personal data are our digital personas, and that collecting our data without our consent and using data for the collector's benefit is a form of tortious invasion of privacy. This Article has argued for this expansion of the appropriation tort and

---

348. *Id.* § 50-f(1)(c). The full definition further notes:

> A digital replica does not include the electronic reproduction, computer generated or other digital remastering of an expressive sound recording or audiovisual work consisting of an individual's original or recorded performance, nor the making or duplication of another recording that consists entirely of the independent fixation of other sounds, even if such sounds imitate or simulate the voice of the individual.

Id.

349. *Id.* § 50-f(2)(d)(i).

350. *Id.*

351. Onassis v. Christian Dior–N.Y., Inc., 472 N.Y.S.2d 254, 261 (Sup. Ct. 1984), *aff'd*, 488 N.Y.S.2d 943 (App. Div. 1985).

the recognition of the concept of data as likeness and digital persona as an effective way to reconcile the old common law of privacy torts with unsettling new privacy harms. It also has demonstrated that data as likeness can survive First Amendment and standing challenges, opening the way for reviving the common law privacy torts in the digital age.