University of Massachusetts Law Review

Volume 16 | Issue 1 Article 3

Biometric Data Regulation and the Right of Publicity: A Path to Regaining Autonomy Over Our Commodified Identity

Lisa Raimondi

UMass Law Review

Biometric Data Regulation and the Right of Publicity: A Path to Regaining Autonomy Over Our Commodified Identity

Lisa Raimondi

16 U. MASS. L. REV. 198

ABSTRACT

This Note explores how a right of publicity action might be used to address present-day concerns regarding biometric data ownership rights where an individual's likeness can essentially be bought and sold. As social networking and use of the internet has grown, so has the opportunity for people to engage with others and share their lives. However, that opportunity also comes with risk. More and more, people are required to accept the terms of use and privacy policies detailing how their biometric data will be collected and stored if they want to download and use certain technological applications. Most of these applications are offered to the public free of charge, so how is it these companies continue to increase their revenue? This Note purports that the users' biometric data stands as a bargaining chip that is shared with tech companies in exchange for use of their product. After the companies collect this biometric data, it is sold for profit. By this very act it is proven that a person's likeness has commercial value— and should not be misappropriated for another's benefit. At the time of this Note, a few U.S. states have enacted biometric data regulations, but in the majority of states, consumers remain vulnerable. This is where the common law right of publicity comes in, as a potential vehicle to help everyday citizens regain control over their likeness, or at minimum, receive compensation where it is misused. Biometric data regulation is in its nascent stage and the extent of damage resulting from the individual's loss of control over their biometric data is as yet unknown, but this Note endeavors to work out a possible avenue to regain control over commodified identity.

AUTHOR'S NOTE

J.D. Candidate, Class of 2021, University of Massachusetts School of Law; Executive Articles Editor, UMass Law Review; B.A. International Relations, Boston University. Thank you to Professor Dustin Marlan, Assistant Professor of Law, University of Massachusetts School of Law, for all his helpful contributions, comments, and exemplary guidance.

Roses are red
Violets are blue
When the product is free
The product is you.[1]

I. INTRODUCTION

In today's modern world, individuals are essentially compelled to engage with social media and smart technology in order to maintain their social circles, professional presence, or even romantic relationships.[2] This is not to say that online engagement is necessarily a burden. Arguably, technological advancements have made lives easier and more secure.[3] Yet, ironically, these same advancements can bring serious risks regarding the security of sensitive biometric data.[4]

---

1 Matt Cagle (@Matt_Cagle), TWITTER (Feb. 14, 2019, 11:47 PM), https://twitter.com/Matt_Cagle/status/1096269666412986373 [https://perma.cc/HLU6-HXFJ].

2 *See* Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ [https://perma.cc/GAA4-6VCM] (survey showing Americans' conflicting feelings about the essential nature of an internet presence versus privacy concerns); *New Poll: Americans Overwhelmingly Support Existing Net Neutrality Rules, Affordable Access, and Competition Among ISPs*, FREEDMAN CONSULTING, LLC 1–2 (July 10, 2017), https://tfreedmanconsulting.com/wp-content/uploads/2017/08/Tech-Policy-Poll-Summary-Final_20170710.pdf [https://perma.cc/N493-PXWC] (2017 poll showing that a broad majority of Americans believe the internet is essential to their everyday lives).

3 For example, the use of facial recognition or fingerprint recognition software to authenticate identity for security purposes. *See* Kristine Hamann and Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A., https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/L5D6-M8FT].

4 *See* Slobodan Ribarić & Nikola Pavešić, *De-identification for Privacy Protection in Biometrics*, *in* USER-CENTRIC PRIVACY AND SECURITY IN BIOMETRICS 293, 295 (Claus Vielhauer ed., 2017) ("There are two different approaches to the relation between privacy and biometrics technology. The first approach is based on the assumption that biometrics protects privacy and information integrity by restricting access to personal information. The second approach is based on the belief that biometrics technology introduces new privacy threats . . . ." (footnote omitted)).

Biometric data generally refers to the unique physiological or behavioral characteristics that both identify and distinguish us from all other persons, e.g. fingerprints or facial scan.[5]

Many individuals, either willingly or unwittingly, have exchanged their highly valuable data for the ability to use the services of companies like tech giants Google and Facebook. While there has been a nationwide push to strengthen data privacy laws to include biometric data,[6] specific protections to address ongoing ownership of identity are largely absent. As it stands, once a person consents to share their biometric data, they may be powerless to restore exclusive ownership.[7] However, there are data protection models, both in Europe and most recently in the state of California, that may adequately address these autonomy concerns.[8]

Part II of this Note discusses the timely and controversial topic of biometric data, the reason for its value, and which entities use it. Part III describes the disparate state privacy laws relating to the use of biometric data—most prominent in Illinois, Texas, and Washington. Part IV will briefly look to the historic roots of the right of publicity and its progenitor, the right of privacy,[9] and end with the present-day hodge-podge collection of right of publicity statutes littered across the U.S. This sets the stage to theorize how a reimagined right of publicity, coupled with the dignitary right of privacy, might address

---

5 *Id.* at 294.

6 *See, e.g.*, H.R. 72, 30th Leg., 1st Sess. (Alaska 2017); H.R. 350, 149th Gen. Assemb. (Del. 2018); S. 120, 191st Sess. (Mass. 2019); H.R. 5019, 99th Leg. Reg. Sess. (Mich. 2017); S. 1203, Reg. Sess. (N.Y. 2019). It should be noted that some states, while not always adopting a separate statute dedicated to biometric privacy, have "expanded how they define 'personal information' under their state data breach notification laws to include biometric information . . . ." Chris Brook, *Biometric Privacy Legislation Catching on Across America*, DIGITAL GUARDIAN: DATA INSIDER (Aug. 29, 2019), https://digitalguardian.com/blog/biometric-privacy-legislation-catching-across-america [https://perma.cc/H5MY-C7GN].

7 *See* Alan S. Wernick, *Biometric Information – Permanent Personally Identifiable Information Risk*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/ [https://perma.cc/UAZ8-3XYY].

8 *Biometrics: definition, trends, use cases, laws and latest news*, THALES (Sept. 10, 2020) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [https://perma.cc/T24H-ABC3] [hereinafter *Biometrics Review*].

9 Mark P. McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U. PITT. L. REV. 225, 234 (2005).

current biometric data concerns. Part V first turns the focus overseas to Europe and then westward to California to examine how other data privacy regulations might help reinstate autonomy over biometric data. The conclusion in Part VI reviews the current U.S. and European data regulation landscapes and asserts that whether those regulations succeed or fail, a re-imagined right of publicity can serve as a secondary protection over our newly commodified identity.

II. BIOMETRIC DATA – WHAT IS IT WORTH AND TO WHOM DOES IT HAVE WORTH?

Biometric data is often divided into two categories: physiological and behavioral.[10] Physiological biometrics are the more permanent, unique, physical attributes of a person that typically remain unaffected by outside stress and time, such as fingerprints, the shape of the face or hand, and iris scans.[11] Behavioral biometrics typically include "voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), keystroke dynamics, the way we use objects, gait, the sound of steps, gestures, etc."[12]

A. The Marketability of Biometric Data and User Concerns

Because biometric data provides a quick and reliable method of identifying individuals or authenticating their identity,[13] the value of the "biometric system market" has skyrocketed and is projected to almost double in size "from USD 33.0 billion in 2019 to USD 65.3 billion by 2024."[14] The gargantuan size of the biometric system market yields strong implications for both users and companies,[15] and not always for the better.[16] In 2018, the University of Texas at Austin's Center for Identity conducted a survey detailing consumer attitudes

---

10 *See Biometrics Review*, *supra* note 8.

11 *Id.*

12 *Id.*

13 *Id.*

14 *Biometric System Market - Global Forecast to 2024*, MKTS. AND MKTS. (Oct. 2019), https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html [https://perma.cc/SH9T-5XA7].

15 *See Biometrics Review*, *supra* note 8.

16 *New Survey on Biometric Technology Shows Consumers Are OK with Some Forms and Wary of Others*, UT NEWS: CAMPUS & COMMUNITY (May 3, 2018), https://news.utexas.edu/2018/05/03/new-survey-on-consumer-attitudes-toward-biometric-technology/ [https://perma.cc/H7PX-2SHT].

toward biometrics and their comfort level with its various uses.[17] The survey showed that "58 percent of those surveyed [said] they [felt] very comfortable with fingerprint scanning biometrics. Only about a third reported feeling very comfortable with any other biometric type. Survey respondents were most unsure about facial recognition technology, with 13 percent feeling 'not at all comfortable' . . . ."[18] This discomfort likely results from the absence of an overarching standard across the U.S. to regulate how companies store and collect the data, and the lack of concrete protection against its unauthorized use.[19] Additionally, "people struggle to understand the nature and scope of the data collected about them. Just 9% believe they have 'a lot of control' over the information that is collected[.]"[20] Transparency as to what data is collected, who collects the data, and for what purpose is sorely lacking.

B. Efforts of Companies to Self-Regulate due to Consumer Concerns

In the absence of an expansive biometric data privacy right, some companies have made efforts to self-regulate and appear more transparent with their privacy policies;[21] however, this effort leaves

---

17 *Id.*

18 *Id.*; *see also* Rachel L. German & K. Suzanne Barber, *Consumer Attitudes About Biometric Authentication*, U. TEX. AUSTIN: CTR. FOR IDENTITY 15 (May 2018), https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf [https://perma.cc/E22Y-PVPP] (This is the survey referenced within the article *supra* note 16.).

19 Carra Pope, Note, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 783–84 (2018).

20 Rainie, *supra* note 2.

21 *See Apple Platform Security: Introduction to Apple Platform Security*, APPLE, https://support.apple.com/guide/security/introduction-seccd5016d31/web [https:// perma.cc/AB7Q-Z6PL]. Surprisingly, Apple's use of biometric identifiers in the authentication services used by its products do not bring the same associated risks that one would expect when one needs to scan their face almost 20 times per day. The simple reason being that Apple never shares your facial mapping template with any third party because the data is strictly housed within the tangible phone on a secure server. *Apple Platform Security: Facial Matching*, APPLE, https://support.apple.com/guide/security/facial-matching-sece151358d1/web [https://perma.cc/B2JW-QWTX]. Even when Apple allows you to use Face ID to access or authenticate your identity in third-party apps, the third-party app never has access to your Face ID, rather "the app is notified only as to whether the authentication was successful; it can't access Touch ID, Face ID, or the data associated with the enrolled user." *Apple Platform Security:*

much to be desired.[22] Google, for instance, has its privacy policy set across multiple pages that requires constant clicks and scrolls.[23] Though the privacy policies on Google's web page are not written in complex legalese or unbearably small font, the language is ambiguous and often leaves out explanations of certain policies requiring yet another click to access them.[24] Add a Google Nest system to the user's household and there is a separate series of privacy and data policy

---

Other Uses for Touch ID and Face ID, APPLE, https://support.apple.com/guide/security/other-uses-for-touch-id-and-face-id-sec50f82ec35/1/web/1 [https://perma.cc/4PZT-6HQS].

22 Romain Dillet, *French Data Protection Watchdog Fines Google $57 Million Under the GDPR*, TECH CRUNCH (Jan. 21, 2019, 10:46 AM), https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/ [https://perma.cc/59KN-EKCN].

23 *Id.*

24 *See Our Commitment to Privacy in the Home*, GOOGLE, https://store.google.com/category/google_nest_privacy [https://perma.cc/7UAT-6CHF?type=image] ("We'll also more clearly explain what types of information these sensors send to Google, as well as examples of how we use that information, to help you better understand their purpose.").

Additionally, see an excerpt from Google's Nest Privacy Policy:

> In addition to the data described in the Privacy Policy, when you use our connected home devices and services, we save: . . . Audio and video data from devices with cameras and microphones, and information derived from this data, such as facial recognition information (if you've set up this feature), and person, object, sound, motion or activity detection information, all subject to your permissions and settings. For example, we store your video footage if you choose to receive video storage services from Google for your Nest Cams.
>
> . . . .
>
> Device usage data is also collected when a device is used with a Google service . . . such as voice or touch interactions, long presses on the device, or other device interactions or adjustments, including related device state, settings, and features used.

FAQs on Privacy: Google Nest, GOOGLE NEST, https://support.google.com/googlenest/answer/9415830?co=GENIE.Platform%3DAndroid&hl=en [https://perma.cc/2CJ6-CPQR] (select the first option entitled "What types of data are collected when I use Google Nest's connected home devices and services?" under the heading "Information Google collects").

pages to click through.[25] Eventually, the site states that Google Nest and Google Home (in accordance with user preferences) can collect and store video, audio, and behavioral biometric data.[26] However, Google does provide an opt-out option and an option to delete the recordings manually—though this process involves additional clicking, scrolling, and searching.[27]

Conversely, Smule, an American mobile app developer with a popular singing app of the same name, is relatively transparent about the data it can collect within its Privacy Policy:

> To be clear, we don't ask you to provide us with any sensitive personal information, such as information relating to your race or ethnic origin . . . [or your] genetic or biometric information . . . . However, if you decide to share this kind of information on Smule Services, you explicitly consent to us displaying it or sharing it in accordance with your selection.[28]

While it is true that Smule does not explicitly ask users to provide them with biometric data, in the form of uploaded video and audio content, it does compel users to consent to Smule sharing that data once it is uploaded.[29] Otherwise, Smule instructs users to leave the site immediately: "[i]f you do not agree to this Agreement or to the use of your personal information in accordance with our Privacy Policy, do not click on one of the 'Account Creation Options' . . . and do not access or otherwise use any portion of the Service."[30]

C. Use of Biometric Data in Security and the Non-Commercial Realm

It is worthwhile to note how companies and public bodies utilize biometric data. Individuals, companies, and governments alike use

---

25 *FAQs on Privacy: Google Nest*, GOOGLE NEST, https://support.google.com/googlenest/answer/9415830?co=GENIE.Platform%3DAndroid&hl=en [https://perma.cc/2CJ6-CPQR].

26 *Id.*

27 *Id.*

28 *Privacy Policy*, SMULE, https://www.smule.com/en/privacy [https://perma.cc/BF7J-3C65]. The terms and conditions also allow revocation of consent and deletion of account, albeit with stipulations that Smule has discretion over when it is deleted. *Id.*

29 *Smule Terms of Service*, SMULE, https://www.smule.com/en/termsofservice [https://perma.cc/792D-K8FK].

30 *Id.*

biometric software for non-commercial and security purposes.[31] For example, retail business owners use facial recognition technology to identify shoplifters[32] and daycare centers have long employed the use of fingerprint scanners to ensure only registered parents access the center.[33] Recently, a non-commercial biometric identifier software, FakeApp AI, garnered some attention when viral videos demonstrated that any person with access to the software could make a video and, through the use of photoshop and facial-mapping technology, don the face of a famous person to fool the audience into believing it was the celebrity depicted.[34] Additionally, law enforcement agencies in the U.S. have been collecting biometric data from citizens since the implementation of fingerprinting and in this aspect there is no substantive commercial use employed.[35] The purpose behind biometric data collection by the Federal Bureau of Investigation was, and is, to use the data to correctly identify suspects (e.g. through fingerprint

---

31 Clare Garvie, *Facial Recognition Is Here. The iPhone X is Just the Beginning*, GUARDIAN (Sept. 13, 2017, 2:00 AM), https://www.theguardian.com/commentisfree/2017/sep/13/facial-recognition-iphone-x-privacy [https://perma.cc/RVE6-GRDA].

32 *Id*.

33 *See* T'ash Spenser, *Daycare Centers Using Biometrics to Protect Kids*, BIOMETRICUPDATE.COM (July 26, 2012), https://www.biometricupdate.com/201207/daycare-centers-using-biometrics-to-protect-kids [https://perma.cc/75NX-5HXY].

34 *See* David Singer & Camila Connolly, *How Hollywood Can (and Can't) Fight Back Against Deepfake Videos*, HOLLYWOOD REP. (Sept. 7, 2019, 9:59 AM), https://www.hollywoodreporter.com/thr-esq/how-hollywood-can-can-t-fight-back-deepfake-videos-guest-column-1237685 [https://perma.cc/ZHB9-6N3N]; Brian Higgins, *At the Intersection of AI, Face Swapping, Deep Fakes, Right of Publicity, and Litigation*, ARTIFICIAL INTELLIGENCE TECH. & L. (June 17, 2018), http://aitechnologylaw.com/2018/06/at-the-intersection-of-ai-face-swapping-deep-fakes-right-of-publicity-and-litigation/ [https://perma.cc/X4MQ-9JLD]. In April 2018, a "deepfake" video featured comedian Jordan Peele using the AI software, donning the face of Former President Barack Obama, to deliver a public service announcement to people about the use of the software and possible subsequent fake news affect it would have, especially come election time. James Vincent, *Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA About Fake News*, VERGE (Apr. 17, 2018, 1:14 PM), https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed [https://perma.cc/52RC-SYJ7].

35 *See Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [https://perma.cc/84FL-QRL9].

detection) to further the Bureau's security goals.[36] However, in early 2019 the use of facial recognition software was banned in the city of San Francisco as an anti-surveillance ordinance measure.[37] Although law enforcement has traditionally supported using new software to address safety concerns, their interests were no match for the outcry against facial recognition and its civil rights implications, citing the technology for its bias and poor track record of misidentifying people of color.[38]

III. CURRENT DISPARATE STATE BIOMETRIC PRIVACY STATUTES

Multiple states have legislation pending before their respective legislatures that focus on providing protection for user control over biometric data.[39] This section, however, will focus primarily on states whose biometric privacy laws are already in full effect: Illinois,[40] Texas,[41] and Washington.[42] These states have not simply broadened

---

36 *Id.*

37 *See* Rachel Metz, *San Francisco Just Banned Facial-Recognition Technology*, CNN: BUSINESS (May 14, 2019, 7:15 PM), https://edition.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html [https://perma.cc/H4FH-J5WB].

38 *Id.* Recently, Amazon's "Rekognition" software came under fire from its investors who did not think it was wise to aggressively market the surveillance software to law enforcement because it implicated civil rights issues.

> Shareholders have introduced two proposals on facial recognition for a vote. One asks the company to prohibit sales of its facial recognition system, called Amazon Rekognition, to government agencies, unless its board concludes that the technology does not facilitate human rights violations. The other asks the company to commission an independent report examining the extent to which Rekognition may threaten civil, human and privacy rights, and the company's finances.

Natasha Singer, *Amazon Faces Investor Pressure Over Facial Recognition*, N.Y. TIMES, May 21, 2019, at B1.

39 *See* sources cited *supra* note 6 and accompanying text.

40 Biometric Information Privacy Act ("BIPA"), 740 ILL. COMP. STAT. 14/1–99 (2020).

41 Capture or Use of Biometric Identifier ("CUBI"), TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019).

42 Biometric Identifiers ("BI"), WASH. REV. CODE § 19.375.010–.040 (2020). *See also Biometric Data and Data Protection Regulations (GDPR and CCPA)*, THALES (Oct. 26, 2020), https://www.thalesgroup.com/en/markets/digital-

their data security breach laws to include biometric data, but have passed statutes designed specifically for the regulation of biometric data.[43] Although all three statutes regulate the collection, use, and security of biometric data, they differ in certain regards. Key differences to note are (1) the types of biometric data the statute protects and what it excludes; (2) the prohibited and/or allowable purpose or use of an individual's biometric data; and (3) who may bring suit.

A. First of Its Kind: The Illinois BIPA

The Illinois Biometric Information Privacy Act ("BIPA") was the first state biometric privacy statute, entering the scene in 2008.[44] The statute protects biometric information such as: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[45] The statute excludes, *inter alia*, "writing samples, written signatures, photographs, . . . tattoo descriptions" and "physical descriptions such as height [or] weight," from protection; nor does it "include information derived from" these excluded identifiers.[46]

While the BIPA does *not* apply to government entities, it does apply to private businesses or corporations, allowing them to "collect, capture, purchase, receive through trade, or otherwise obtain a person's" biometric identifier once they have informed the individual in writing that: (1) the individual's "information is being collected or stored"; (2) "the specific purpose and length of term" for which the individual's information is being used; and (3) the entity must also obtain a written release signed by the individual.[47] A person in possession of another's biometric information is prohibited from selling, disclosing, redisclosing, or otherwise disseminating "a person's . . . biometric identifier" unless the individual whose data it is

---

identity-and-security/government/biometrics/biometric-data [https://perma.cc/6DFX-T39A].

43 Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 648 (2018); see also Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/ZUG3-ZBKN].

44 BIPA, 740 14/1–99.

45 *Id.* at 14/10.

46 *Id.*

47 *Id.* at 14/15(b).

consents to the disclosure.[48] The private entity is required to "store, transmit, and protect" all biometric data from disclosure with a reasonable standard of care typical of their industry and in the same fashion they would secure "other confidential and sensitive information."[49] A cause of action under BIPA can be pursued by "[a]ny person aggrieved by a violation of this Act."[50] The aggrieved is entitled to recover damages ranging from approximately $1,000 to $5,000, as well as reasonable attorney's fees and costs.[51]

Since the statute's inception in 2008, there has been substantial development of BIPA case law, perhaps because the statute allows citizens to file complaints on their own. There are two cases worth noting: *Patel v. Facebook, Inc.*[52] and *Rosenbach v. Six Flags Entertainment Corp*.[53]

1. Rosenbach v. Six Flags Entertainment Corp.: What it Means to Be "Aggrieved"

In *Rosenbach*, the plaintiff, a minor teen, picked up a Six Flags season pass that his mother had purchased for him online.[54] When he collected his pass he was instructed to provide his "thumbprint" in accordance with the amusement parks' procedures for season pass-holders.[55] After scanning his thumb and returning home, he informed his mother of the fingerprinting.[56] Ms. Rosenbach was never informed that the park would collect her minor son's biometric data; she was not provided information about how the data was stored, for what purpose, and for how long; nor had she given express consent to the collection of her son's data.[57] The Illinois Appellate Court found in favor of the

---

48 *Id.* at 14/15(d)(1). This sentence only describes one exclusion, but there are three other exclusions to when a private entity may be permitted to disclose an individual's biometric identifiers, for example, if the disclosure completes a financial transaction requested or authorized by the individual; when compelled by state or federal law or municipal ordinance; or the disclosure is made pursuant to a valid warrant or subpoena. *Id.* at 14/15(d)(2)-(4).

49 *Id.* at 14/15(e)(1)-(2).

50 *Id.* at 14/20.

51 *Id.* at 14/20(1)-(4).

52 Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

53 Rosenbach v. Six Flags Entm't Corp., 2019 Ill 123186.

54 *Id.* at ¶ 5.

55 *Id.* at ¶ 6.

56 *Id.* at ¶ 7–8.

57 *Id.* at ¶ 8.

defendant theme park who argued that in order to receive a remedy under the statute, the plaintiff must have plead some actual injury or harm "beyond infringement of the rights afforded them under the law."[58] However, the Illinois Supreme Court disagreed with this finding, particularly because of the unambiguous language in the statute,[59] which included a detailed statement of legislative intent.[60] The court reasoned, "[w]hen the statutory language is plain and unambiguous, we may not depart from the law's terms by reading into it exceptions, limitations, or conditions the legislature did not express . . . ."[61] Aggrieved is commonly defined as "suffering from an infringement or denial of legal rights."[62] Thus, a more stringent requirement of actual harm or adverse effect would be inconsistent with the straightforward legislative intent in protecting a person's right of privacy.[63]

2. Patel v. Facebook, Inc: The Latest Victory for BIPA

In *Patel*, the class action plaintiffs brought suit against the tech giant, Facebook, for BIPA violations.[64] Facebook had—through its Tag Suggestions feature—scanned and collected the face templates of users via its facial recognition software and stored the biometric data on its servers.[65] Facebook did not inform the plaintiffs of the collection, obtain their written consent, or maintain a retention schedule as required by the statute. [66]

The court in *Patel*, held that plaintiffs had sufficient Article III standing under BIPA because the "statutory provisions at issue were established to protect [the plaintiffs'] concrete interests," namely their privacy.[67] The Ninth Circuit recognized that the right of privacy was "traditionally . . . regarded as providing a basis for a lawsuit . . . ."[68]

---

58 *Id.* at ⁋ 38.

59 *Id.*

60 BIPA, 740 ILL. COMP. STAT. 14/5(a)-(g) (2020).

61 *Rosenbach*, 2019 Ill 123186 ⁋ 24.

62 *Id.* at ⁋ 32 (quoting MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 25 (11th ed. 2006)).

63 *Id.* at ⁋ 37.

64 Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).

65 *Id.*

66 *Id.* at 1274.

67 *Id.* at 1271.

68 *Id.* at 1273 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

Furthermore, when bolstered by recent Supreme Court jurisprudence citing that privacy concerns are amplified by technological advancements in monitoring systems, the court concluded "that an invasion of an individual's biometric privacy rights 'has a close relationship to a harm'" giving rise to a lawsuit.[69] Additionally, the court found "concrete and particularized harm" where violations of the procedures in BIPA can actually harm or pose a material risk of harm to substantive privacy interests. [70]

B. One Year Later, Here Comes Texas: CUBI

In 2009, "Texas became the second state to pass a law protecting citizens' biometric data."[71] The Texas Capture or Use of Biometric Identifier statute ("CUBI"), while relatively similar to BIPA, has key differences. CUBI protects biometric identifiers, such as "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry[,]" and does not name any exclusions.[72] CUBI allows for the collection of biometric data of an individual for a commercial purpose, provided the person receives notice of this purpose and consents to its use (though a writing is not required).[73] Although CUBI prohibits a person who possesses the biometric information of another to engage in a third-party transfer, there are certain enumerated exceptions to this prohibition.[74] Perhaps the biggest difference between the Texas CUBI statute and the Illinois BIPA statute is that CUBI does not allow for a private right of action; it is only actionable via the state's Attorney

---

69 *Id.* (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

70 *Id.* at 1275.

71 Pope, *supra* note 19, at 791.

72 CUBI, TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2019).

73 *Id.* § 503.001(b).

74 The exceptions are as follows:

> A person who possesses a biometric identifier of an individual that is captured for a commercial purpose: (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (B) the disclosure completes a financial transaction that the individual requested or authorized; (C) the disclosure is required or permitted by a federal statute or by a state statute . . . (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant . . . .

Id. § 503.001(c)(1)(A)-(D).

General, who can pursue up to $25,000 per violation.[75] Additionally, CUBI requires biometric data be destroyed within one year of its collection,[76] whereas BIPA provides a longer, three-year window.[77] To date, there are no published actions under CUBI.

C. Washington Makes Three: Biometric Identifiers

Last, but not least, Washington passed its own biometric data privacy statute ("BI"), which went into effect in July of 2017. In similar fashion to Illinois, Washington included a statement of legislative intent at the forefront of its statute. The "finding of intent" section reads: "[t]he legislature finds that citizens of Washington are increasingly asked to disclose sensitive biological information that uniquely identifies them for commerce, security, and convenience. The collection and marketing of biometric information . . . is of increasing concern." [78] Through this section the legislature makes clear its intent to require businesses to first obtain the consent of users prior to "enrolling" their identity into any database, provide notice of this enrollment, and disclose how the biometric data collected will be used.[79]

Like CUBI, Washington's statute is only actionable by the Attorney General.[80] Additionally, it has a broader definition of what is considered protected biometric data, but provides for exclusions to this definition such as "physical or digital photograph, video or audio recording or data generated therefrom[.]"[81] The most notable difference distinguishing the Washington statute from Illinois and Texas is the broad exclusion of liability for entities that enroll and collect biometrics "in furtherance of a security purpose."[82] "'Security purpose' means the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications,

---

75 *Id.* § 503.001(d).

76 *Id.* § 503.001(c)(3).

77 BIPA, 740 ILL. COMP. STAT. 14/15(a).

78 BI, WASH. REV. CODE. § 19.375.900 (2020).

79 *Id.*

80 *Id.* § 19.375.030(2).

81 *Id.* § 19.375.010(1).

82 *Id.* § 19.375.020(7).

online services, or any person."[83] Similar to Texas, there are no published actions under this Washington Biometric Identifiers statute as of the date of this Note.

IV. THE REUNIFICATION OF PRIVACY AND PUBLICITY: BRINGING DIGNITY AND AUTONOMY BACK TO THE RIGHT OF PUBLICITY

A person's biometric data—their identity—is personal and extremely sensitive, yet also a commodity and ultimately assignable to others via consent or contract under current law.[84] Although there are state privacy laws in place that specifically govern the use of a person's biometric data, these laws are relatively new and vary greatly in how, and when, a person can bring a cause of action predicated on the misuse of their data.[85] To address this issue, it should be considered how the right of publicity, harmonized again with the right of privacy, could operate as a solution where a state is silent on biometric data regulation. This common law tort can be used to evaluate a cause of action under the right of publicity resulting from the misappropriation of biometric data, or identity.

A. A Brief History of Misappropriation and its Alter Ego: The Right of Publicity

In the early 1900s, the right of an individual to defend against the unwanted use of their name or likeness existed under an established right of privacy.[86] It was not until the 1953 decision of *Haelan Laboratories v. Topps Chewing Gum* that the term "right of publicity" was first coined, although the idea was not new.[87] Indeed, by the time *Haelan* was decided it was widely recognized that a person had a property right in their name and likeness, and some states even had privacy laws specifically including misappropriation language.[88] Jennifer Rothman, author of *The Right of Publicity* explains, "[f]rom

---

83 *Id.* § 19.375.010(8).

84 *See* Jennifer E. Rothman, *The Inalienable Right of Publicity*, 101 GEO. L.J. 185, 190 (2012); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. g (AM. LAW INST. 1995) ("The interest in the commercial value of a person's identity is in the nature of a property right and is freely assignable to others.").

85 *See supra* Part III.

86 *See, e.g.*, Pavesich v. New England Life Ins. Co., 50 S.E. 68, 80–81(Ga. 1905).

87 Haelen Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953).

88 *Id.*

the start there was a property-based conception of the right of privacy. It was understood as a right of self-ownership."[89] This autonomous right was generally considered "personal and not assignable,"[90] and private or public figures could pursue claims of misappropriation which inflicted emotional, economic, or reputational injury.[91] Even though the right of publicity was not a novel idea, the expansion of publicity rights into a quasi-intellectual property right[92] was a new concept, to which the *Haelan* court gave credence by allowing the transferability of publicity rights.[93]

In his *Right of Privacy* article, Judge Richard Posner discussed the right of publicity and its importance as a vendible property right.[94] He argued that there are "good economic reasons for assigning the property right in a photograph used for advertising purposes to the photographed individual: this assignment assures that the advertiser to whom the photograph is most valuable will purchase it. [Alternatively,] [m]aking the photograph the communal property of advertisers would not achieve this goal."[95] While Judge Posner's approach hints at prioritizing the protection of an individual's

---

89 JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 48 (2018).

90 *Id.* at 47. "The Fifth Circuit in *Hanna Manufacturing v. Hillerich & Bradsby* held that a company could not divest a person of his name even if that company had an exclusive right to its use." *Id.* at 48. "The court concluded that [even though persons had property rights in their names] this property was not 'vendible in gross' so as to pass from purchaser to purchaser unconnected with any trade or business." *Id.* at 48–49. *See also* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 408 (1960); Melville B. Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203, 209 (1954). *But see Haelen Labs., Inc.*, 202 F.2d at 868 (re-interpreting publicity rights to be licensable and assignable).

91 *See* ROTHMAN, *supra* note 89, at 30, 32–33.

92 Separate from publicity rights, which are individuals' rights against the misappropriation or misuse of their likeness and name for another's benefit (resulting in a harm), are intellectual property rights, "[a] category of intangible rights protecting commercially valuable products of the human intellect. The category comprises primarily trademark, copyright, and patent rights, but also includes trade-secret rights, publicity rights, moral rights, and rights against unfair competition." *Intellectual Property*, BLACK'S LAW DICTIONARY (11th ed. 2019).

93 *See* ROTHMAN, *supra* note 89, at 64.

94 Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 411 (1978).

95 *Id.*; *See also* ROTHMAN, *supra* note 89, at 111 ("In the absence of control over our own identities, we are all like puppets that can be used to speak others' words and messages.").

autonomy by giving them control over who their image is sold to, the article glosses over the possible emotional and economic harms that may result from the commodification of a person's likeness compounded by the complete transferability of publicity rights.[96]

Justification for transferability of the right of publicity appears primarily when viewed as a purely economic right, which endorses the idea that identity or likeness is akin to a commodity that can be sold to the highest bidder with control over its future use forfeited. [97] To some, the very idea of this is degrading.[98] Yet, the right of publicity has grown because of this "singular focus on protecting the economic value of commodified identity, which can be exploited in a variety of ways."[99] Identity as a transferrable commodity cuts against the origins of the right—protection against the misuse of one's identity or likeness—and the reason for the right's existence: the need to protect one's autonomy.[100] However, this is not to argue for strict non-transferability, but rather in favor of limited transferability. The limiting of transferability has been used before, specifically with property that is impossible to transfer or when allowing its transfer would infringe upon fundamental rights.[101]

Transferability is not an all or nothing concept.[102] "Blood, babies, historic buildings, human organs, military service, voting rights, endangered species, and alcohol all have limits placed on their transferability[,]" ranging from strictly non-transferable to only partially limited.[103] Most of these commodities can be separated from a person in ways that the identity or likeness cannot be.[104] Typically, it would seem easier to transfer property that is severable from the person, which strengthens the argument for limiting transferability of

---

96 ROTHMAN, *supra* note 89, at 127–28.

97 *See id.* at 121 (discussing parents assigning their children's right of publicity resulting in the child's involuntary forfeiture of that right in the future).

98 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 988 (1964) (expounding upon the conventional notion that "[n]o man wants to be 'used' by another against his will").

99 McKenna, *supra* note 9, at 233.

100 *See* ROTHMAN, *supra* note 89, at 111.

101 *Id.* at 125.

102 *Id.*

103 *Id.*

104 *See id.*

something that is essentially non-severable from the person.[105] Moreover, if one contemplates the serious implications a freely transferable right of publicity would have on daily life, the outlook becomes bleak. For instance, assume an individual uses an internet service in a state that allows the free transfer of publicity rights, or is silent on transferability.[106] To use the service, the person has to agree to certain terms and conditions that enable the internet service to obtain an exclusive license to the individual's publicity rights in their images, or likeness, in perpetuity. In essence, this individual has signed away their right of publicity. That internet service can now potentially impose limits on this person's ability to market themselves in any other way. Or even worse, it can use their likeness in the future, without their consent. In this scenario, there are fundamental rights at risk that perhaps were never considered by that individual before they joined the internet service.[107] Through marketing the unsuspecting individual's likeness in accordance with certain groups or services, the internet service could infringe upon the individual's freedom of association.[108] A court could conceivably find that, in contracting with this internet service, the individual voluntarily assigned their publicity rights and would have to live with the consequences. Recalling John Stuart Mill's famous quote, Rothman writes that "it is not freedom, to be allowed to alienate [one's] freedom," but that is what has occurred since the creation of the IP-like right of publicity.[109]

B. Right of Publicity Today: "A Haystack in a Hurricane"[110]

Because the right of publicity was severed from the "personal" tort of privacy, "[w]hat may have originated as a concern for the right to be left alone has become a tool to control the commercial use and, thus, protect the economic value of one's [identity]."[111] The state of disarray in publicity cases springs from conflicting state laws barring certain

---

105 *Id.* at 127.

106 *Contra id.* at 119 (Some states, like Nebraska, explicitly prohibit the transferability of the right of publicity, or at least prohibit the forcible transference of the right to creditors, like Illinois).

107 *Id.* at 128.

108 *Id.*

109 *Id.* at 129 (quoting JOHN STEWART MILL, ON LIBERTY 101 (Elizabeth Rapaport ed., Hackett Publishing Co. 1978) (1859)).

110 Ettore v. Philco Television Broad. Corp., 229 F.2d 481, 485 (3d Cir. 1956) (characterizing the state of publicity rights laws across the United States).

111 KNB Enters. v. Matthews, 92 Cal. Rptr. 2d 713, 717 (Cal. Ct. App. 2000).

plaintiffs' right to publicity actions for a variety of reasons, including failure to exploit their identity or commercially profit from it before the defendant did.[112] States whose laws impose this requirement in particular provide for a cause of action exclusive to celebrities, leaving non-celebrities without a remedy. Meanwhile, in other states, non-celebrity plaintiffs are allowed to pursue right of publicity claims.[113] Indeed, courts themselves grapple to find a meaningful distinction between the proprietary economic right of publicity (commonly pursued by celebrities) and the privacy tort of misappropriation (commonly reserved for non-celebrities). It is not difficult to surmise that a non-celebrity may suffer economic harm from the exploitation of his identity, while a celebrity claiming misappropriation may very well experience emotional or reputational harm from the unauthorized use of their identity.[114] If we persist with this needless dichotomy—where certain torts are reserved for different classes and statuses—the inquiry becomes: to what end?

Fraley v. Facebook provided a compromise between these two ideas in that a non-celebrity could bring a claim for the right of

---

[112] *See, e.g.*, Grant v. Esquire, Inc., 367 F. Supp. 876, 880 (S.D.N.Y. 1973) (noting that plaintiffs should not have to be required to show they commercially exploited their own property to justify economic injury when defendants exploit it).

[113] For example, in *Motschenbacher v. R.J. Reynolds Tobacco Co.*, the federal court held:

> Generally, the greater the fame or notoriety of the identity appropriated, the greater will be the extent of the economic injury suffered. However, it is quite possible that the appropriation of the identity of a celebrity may induce humiliation, embarrassment and mental distress, while the appropriation of the identity of a relatively unknown person may result in economic injury or may itself create economic value in what was previously valueless.

498 F.2d 821, 824 n.11 (9th Cir. 1974).

Likewise, in *Bullard v. MRA Holding, LLC*, the state supreme court said:

> While a private citizen may not have the same commercial value in his or her name and likeness that a celebrity may have, or any preexisting commercial value in his or her name and likeness at all for that matter, that would not foreclose that person from pursuing a cause of action against a wrongdoer who appropriated the person's name and likeness for their own commercial gain.

740 S.E.2d 622, 626 (Ga. 2013).

[114] *Bullard*, 740 S.E.2d at 626.

publicity where a defendant's valuation of the user's identity demonstrated that their identity had value in the first place.[115] In *Fraley*, plaintiffs claimed a violation of their right of publicity when Facebook, through its Sponsored Stories feature, exploited the plaintiffs' identity to profit from the value of the plaintiffs' "endorsement" in Facebook's advertising scheme.[116] The court required a showing of economic injury, and was persuaded by plaintiffs' use of the company's own statements that Facebook greatly valued the plaintiffs' identities in their advertising.[117] Even though the plaintiffs' identities may not have had commercial value prior to their engagement with Facebook, by exploiting the plaintiffs' identities, Facebook created the presumption of commercial value, thereby enabling the plaintiffs to show economic injury—at least for purposes of standing.[118]

The motley collection of state right of publicity statutes may never be sorted and unified. Nevertheless, there is hope that courts may recognize non-celebrities as capable of claiming violations of their right of publicity,[119] and in so doing, perhaps users' biometric data could find protection as well.

C. The Right Of Publicity, Unified with the Right of Privacy, Could Make Rights Over Personal Identity Stronger and Address Biometric Data Concerns

Shifting the right of publicity from a solely economic property right—where identity is merely an assignable commodity, "vendible in gross,"[120]— back to a personal right of privacy, may help strengthen autonomy over one's identity. In this light, identity can continue as a bargained-for commodity, but the underlying person, or "identity-

---

115 Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 807 (N.D. Cal. 2011).

116 *Id.* at 799.

117 *Id.* at 800.

118 *Id.* at 800–01. This presumption has been found in other courts presiding over publicity cases. *See* Fanelle v. Lojack Corp., No. CIV.A.99-4292, 2000 WL 1801270, at *11 (E.D. Penn. Dec. 7, 2000) ("Inherent in the act of a defendant using a person's name, identity, or persona in a commercially advantageous manner is the presumption that the identity has commercial value . . . . I am convinced that the right of publicity resides in every person, not just famous and infamous individuals.").

119 *See Fraley*, 830 F. Supp. 2d at 799.

120 *See* ROTHMAN, *supra* note 89, at 59.

holder,"[121] can never be fully divested of ownership. Thus, the individual is rendered invulnerable to the intentions of the commercial entity, sometimes referred to as the "publicity-holder," absent options to recuperate.[122] This would require that some limitations be placed on the transferability of identity, as property, recognized either by statute or under common law.

To defend against the misuse of one's biometric data, the right of publicity must be reharmonized with the right of privacy. By shifting the right of publicity away from its current status as an assignable pseudo-intellectual property right and towards a revitalized dignitary right of self-ownership, the social interests advanced by both rights—dignity, autonomy, and economic efficiency—become unified.[123] But, as *straightforward* as this may sound, the obstacles do not end there. To effectuate any recognition of biometric data as a protected property and privacy right under the right of publicity framework, the meaning of identity or likeness under the right of publicity must be reconfigured to include biometric data; the commercial value of biometric data in today's economy must be recognized, at least as a precautionary measure for courts that require pre-existing commercial value;[124] the

---

121 This is a phrase used by Rothman in her book, *The Right of Publicity*, to refer to the original holder of the identity as opposed to a "publicity-holder," which refers to an entity that has been assigned the identity-holder's right of publicity, perhaps by contracting for exclusive rights to a person's likeness, for instance. *Id.* at 7.

122 *Id.* at 137.

123 *Id.* The argument that economic efficiency could be advanced by broader publicity protections is that users could be more engaged with sharing and networking without fear of biometric identity theft from companies or entities purporting a "free" service but really selling users' data to advertising agencies, data brokers, and the like. *See Privacy Policy*, SNAP INC. (Sept. 14, 2020), https://www.snap.com/en-US/privacy/privacy-policy [https://perma.cc/5KWL-AL46] ("Because most of our services are free, we also use some information about you to try and show you ads you'll find interesting."). Also, companies who are more transparent and give more protections to users could gain a competitive advantage in the market where states and foreign countries are trending towards greater privacy and data protections. *See* Gene Marks, *Biometrics May Answer Your Security Concerns – But Don't Forget Privacy*, GUARDIAN (Apr. 4, 2019, 6:00 AM), https://www.theguardian.com/business/2019/apr/04/biometrics-small-business-security-privacy [https://perma.cc/KWR6-P5QV].

124 This seems like it would be challenging to do at this moment in time because of the lack of transparency between businesses, data brokers, and consumers as to what the precise value of biometric data is. All we know is the value of biometric data in the aggregate by looking at how valuable biometric technology

actual and potential economic, reputational, or emotional injury resulting from continued misappropriation of our identity must be appreciated; and finally, limitations must be placed on this reimagined right of publicity and its scope narrowly tailored to focus on harms against identity-holders.[125] It could be that the best method of protection over biometric data lies with stronger data privacy laws. Nonetheless, in the face of a slow-moving legislature, and the reality that some states may never adopt a biometric data privacy statute on their own, it is useful to analyze a possible alternative.

1. What Counts as Identity?: "Name and Likeness" Fails to Capture the Modern Ways We Are Identified

In an action under misappropriation, or the right of publicity,[126] "the question before the courts has been . . . whether there has been appropriation of an aspect of the plaintiff's identity."[127] In order for liability to attach, the specific individual's identity must first be discernable from the claim.[128] Only then can the courts continue with their analysis.[129] The right of publicity has expanded over time to encompass more than name, photograph, or likeness, for the necessary "indicia of identity."[130] Now identity can include fabricated "persona,"

---

has become. *See Biometric System Market - Global Forecast to 2024 supra*, note 14.

125 Doing so would limit who could bring suit for a violation of a right of publicity, thus narrowing the pool of potential litigants.

126 All references to the right of publicity will also refer to actions under the privacy tort of misappropriation as many courts use the terms interchangeably. *See, e.g.*, Somerson v. World Wrestling Entm't, Inc., 956 F. Supp. 2d 1360, 1365 (N.D. Ga. 2013) (quoting Thoroughbred Legends, LLC v. Walt Disney Co., No. 1:07–CV–1275–BBM, 2008 WL 616253, at *11 n.13 (N.D. Ga. Feb. 12, 2008) ("[t]here is no substantive difference between the interests protected by the common law 'right of publicity' and the interests protected by the appropriation prong of the invasion of privacy tort.")); Gionfriddo v. Major League Baseball, 114 Cal. Rptr. 2d 307, 313 (Cal. Ct. App. 2001) ("The common law right of publicity derives from the fourth category of invasion of privacy identified by Dean Prosser, described as 'appropriation' of a plaintiff's name or likeness for the defendant's advantage."); *see also* Posner, *supra* note 94, at 411(finding the privacy tort of appropriation and right of publicity basically identical).

127 Prosser, *supra* note 90, at 403.

128 *Id.* at 404–05.

129 *Id.* at 405.

130 *See* ROTHMAN, *supra* note 89, at 97.

or even a substantial reference to a particular individual that would allow identification.[131]

It takes no great stretch of the imagination to connect a person's likeness or identity with one's biometric data; arguably, they are one in the same. A person's "likeness" is often comprised of unique physical or behavioral attributes such that a reasonable person would be able to see and identify the specified individual. Biometric data, as described *supra* in Section II(A), is a reference to the unique physical and behavioral traits that reliably and accurately identify human beings.[132]

Some states, like Indiana for example, employ statutory language, which implies that certain biometric identifiers already qualify for protection under their statutes.[133] The relevant portion of Indiana's statutory right of publicity lists that "voice; []signature; . . . []distinctive appearance; . . . or []mannerisms" would all qualify as protected under the statute.[134] These attributes are also considered biometric identifiers because, in addition to fingerprints and facial recognition mapping, a person's signature and their distinctive bodily movements, such as keystrokes or gait, are measurable, identifiable, behavioral attributes.[135] Additionally, in New York, there is a statute providing for both a civil and a criminal cause of action regarding a person's right of publicity.[136] The civil statute prevents the unauthorized use of a person's voice, a specified biometric identifier. [137] However, in the event a state statute fails to list a specific biometric identifier, the inclusion of the word "likeness" should arguably encompass biometric data, as it is essentially comprised of a person's likeness. Where possible, a change should be made to the state's publicity statutes to include "biometric indicator," which would arguably satisfy the full definition of likeness.

---

131 *Id.* at 89.

132 *See Biometrics Review*, *supra* note 8.

133 IND. CODE § 32-36-1-7 (2020).

134 *Id. Contra* 9 R.I. GEN. LAWS § 9-1-28 (2020) (prohibiting only the unauthorized use of name, picture, or portrait; specifically, § 9-1-28.1(a)(2) provides a "right to be secure from an appropriation of one's name or likeness").

135 *See Biometrics Review*, *supra* note 8.

136 N.Y. CIV. RIGHTS LAW § 50 (McKinney 2020).

137 *Id.* § 51.

2. Biometric Data Has Commercial Value, but No One is Willing to Share

There are no hard and fast numbers assigning a specific dollar value to a person's biometric data.[138] While it can be discerned that biometric data has value based on the skyrocketing market value of the technology needed to facilitate its use, exact numbers remain elusive. "[T]he shadowy world of data brokers,"[139] "[who] are notoriously secretive" provides little insight into how much they charge for sharing sensitive information, or even how many data brokers exist and do business.[140] "Getting answers from the data brokers themselves, as Congress found, is next to impossible[.]"[141] Legislatures agree that biometric data is being collected and marketed, and acknowledge the risk of the exploitation of this valuable asset in the statement of intent portions of their biometric data privacy statutes.[142] For example, Washington and Illinois include legislative intent passages that speak to the presumption of a risk of harm, or even a particularized harm, to citizens whose biometric data was vulnerable to collection and misuse.[143] By acknowledging this risk, the legislatures are implying that biometric data has an innate value, or worth, to the owner. If more courts, like the *Fraley* court, recognized the inherent commercial value of biometric data, then demonstrating economic harm would not be such an arduous task. In acknowledging this inherent value, users would be able to substantiate the claim that biometric data has pre-existing commercial value and is therefore capable of exploitation.

---

138 At least, not that this author could find while scouring the web.

139 *See* Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping up Information About You?*, VICE: MOTHERBOARD (Mar. 27, 2018, 10:00 AM), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/YJ7P-LBK2].

140 Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK: TECH. & SCI. (May 30, 2016, 2:30 PM), https://www.newsweek.com/secretive-world-selling-data-about-you-464789 [https://perma.cc/5D6C-YH8N].

141 *Id.*

142 *See* BI, WASH. REV. CODE. § 19.375.900 (2020) ("[C]ollection and *marketing* of biometric information about individuals, without consent or knowledge of the individual whose data is collected, is of increasing concern." (emphasis added)); *see also Take Control of Your Virtual Identity #GDPR*, EUR. COMMISSION (June 2019), https://ec.europa.eu/commission/sites/betapolitical/files/virtual_identity_en.pdf [https://perma.cc/L4TC-6TJK] ("[Companies] map your virtual identity . . . . [T]hen monetise your virtual identity for targeted advertising.").

143 *See supra* text accompanying notes 60 & 78.

Although the proposition of value premised on the magnitude of the market can be made, it is unclear whether this large aggregate number would be persuasive enough to establish proof of pre-existing commercial value.

Weighing biometric data's benefits to the economy and security against the potential harm to autonomy still favors limitations on the commodification of likeness or identity. It is useful to remember that a partial limitation on the assignability and transferability of one's publicity rights, including biometric identifiers, may not have the impact necessary to chill the market. First Amendment defenses to the rights of privacy and publicity are avenues that would protect the use of biometric data in cases of newsworthiness or expressionist works, which are also very important to our society. Absent tighter regulations, these First Amendment defenses operate as some of the only protections given the current disarray of state publicity laws. Considering the effort and transactional costs involved in litigating these issues, limiting the transferability of publicity rights remains a heavy task. [144]

It is important to reflect on the societal concerns with the loss, or substantial decrease, of autonomy over biometric data and the ultimate goal to have awareness and control over when and how our identities are used. It is true that to function comfortably in today's society, individuals must engage with the internet and social media. However, it does not follow that in exchange for providing users with a "free" service, companies should then be able to collect users' unique and valuable biometric data, and share it with unknown or undocumented third party associates.[145] Without facing any regulations or compulsion to disclose, there is no impetus to reveal which third-parties these companies are selling information to and for what specific purpose.[146] In this fashion, lack of knowledge is lack of autonomy because without knowledge, a person has no power or control over how their biometric information is shared or used. Every individual has a right of publicity,[147] whether the sale or usage of their biometric data was

---

144 *See* Jennifer Rothman, *Rothman's Roadmap to the Right of Publicity*, RIGHT OF PUBLICITY ROADMAP.COM, https://www.rightofpublicityroadmap.com/ [https://perma.cc/G4MP-ZZZW] (illustrating how varied state-to-state right of publicity and common law misappropriation laws are).

145 *See Privacy Policy*, *supra* note 28.

146 This is currently the case with the data brokerage market. *See* Grauer, *supra* note 139.

147 *See supra* note 113 and accompanying text.

conducted openly or clandestinely. While it may seem extreme to completely disallow the assignability of biometric data in return for use of a service, ultimate control should remain with the "identity-holder."[148] If the dissemination of biometric data cannot be regulated on the front end, then users should at least be provided with an exit strategy.

One solution, as previously mentioned, may be in acknowledging a right of publicity action where the user could enjoin the use of their biometric data, or at minimum, claim damages for its misuse. Another potential strategy also briefly discussed previously, is a regulatory solution. This regulatory solution is an exit strategy that would include the ultimate right to regain control over one's own data at a time of their choosing, or at a minimum, the guaranteed and periodic destruction/anonymization of biometric data, commonly referred to as the "right to be forgotten."[149] A comprehensive solution, whether judge-made or regulatory, should begin with an examination of the regulatory solutions currently in effect, specifically those in the European Union and California.

V. EIGHT LETTERS MAKE A BIG IMPACT: GDPR AND CCPA'S POTENTIAL IMPACT ON PRIVACY RIGHTS

The European Union's GDPR and California's CCPA are at the forefront of the global trend to slow the rampant dissemination of individuals' biometric and personal data in order to reinforce privacy rights and address security concerns.[150] While the two regulations are similar, there are differences and takeaways that can be analyzed to assess how these regulations address concerns for autonomy over biometric data and whether they are better suited to address those concerns over a reimagined right of publicity.

---

148 ROTHMAN, *supra* note 89, at 7.

149 *See Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 42.

150 *See* Dimitri Sirota, *California's New Data Privacy Law Brings U.S. Closer to GDPR*, TECHCRUNCH (Nov. 14, 2019, 2:55 PM), https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/ [https://perma.cc/9XUA-HNMK].

A. The GDPR: EU General Data Protection Regulation is Two Years Old and Europe is Still Standing

The EU General Data Protection Regulation went into effect in May of 2018.[151] This regulation immediately created "one set of rules directly applicable in all the European Member States regarding the protection of personal data."[152] The GDPR protects EU residents' data—including biometric data—by compelling companies to: (1) provide users with an opt-in option *first* before "processing"[153] any data; (2) disclose information about the processing of the user's data in "clear and plain language";[154] (3) provide users with the right to object to any "take-it-or-leave-it" services;[155] (4) give users access to all of their data, and ensure the transferability to the user in portable electronic format;[156] (5) inform the user if their data has been hacked or "leaked";[157] and (6) grant users' requests that all their personal data be deleted, otherwise known as "[t]he right to be forgotten."[158] In addition to EU Member States, any "[n]on-EU established organizations will be subject to the GDPR if they process personal data about EU data subjects. This makes the GDPR a global law."[159] In some cases, the GDPR has appointed Data Protection Officers as an enforcement measure to verify that companies are in compliance with the GDPR.[160] Were a company to process an EU resident's data

---

151 *See Take Control of Your Virtual Identity #GDPR*, *supra* note 142.

152 *See Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 42.

153 "The term 'processing' is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data)." Dr. Detlev Gabel & Tim Hickman, *Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation [https://perma.cc/NRK5-NUWL].

154 *See Take Control of Your Virtual Identity #GDPR*, *supra* note 142.

155 *Id.*

156 *Id.*

157 *Id.*

158 *Id.* The "right to be forgotten" means that EU residents can request a company delete all of their personal data unless a legitimate reason is presented for its preservation. *Id.*

159 *See Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 42.

160 *Id.* (especially companies having over 250 employees).

without complying with the GDPR or without the user's explicit consent, the company would face serious penalties.[161]

Unlike the varied methods of relief afforded in state statutes across the U.S., the GDPR allows all EU residents a private right to lodge a formal complaint for "material or non-material damage caused by a data controller or data processors breach of the GDPR."[162] Civil penalties under the GDPR include a potential fine of €20 million, or 4% of the company's annual profit.[163] A German "social networking operator was fined €20,000 for failing to secure users' data."[164] Google is also facing a $57 million fine for non-compliance with the GDPR's transparency and opt-in guarantee.[165] Additionally, a data brokering company was fined €220,000 for "failing to inform citizens that their data was being processed by the company."[166] The GDPR has been operating for only two years, but by instituting some serious penalties, it has already shown that it means business. It is hard to tell at such an early stage if we can expect the same from California's newest act.

---

[161] *Id.* This is not without some exceptions. For example, the "biometric information is necessary for carrying out obligations of the controller or the data subject in the field of employment, social security and social protection law"; "to protect the vital interests of the individual and he/she is incapable of giving consent"; "it's critical for any legal claims"; there is a public health reason affecting public interest. *Id.* Moreover, Member States must conform to these regulations, but they are allowed "to introduce other limitations regarding the processing of biometric information." *Id.*

[162] Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKER & HOSTETLER LLP 6 (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [https://perma.cc/ZF6M-5637].

[163] *Id.* at 7.

[164] *GDPR in Numbers*, EUROPA, https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf [https://perma.cc/36VF-SGMG]. CNIL, a French data protection watchdog concluded in its report that there is an "alleged lack of transparency. 'Essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information[.]'" Dillet, *supra* note 22.

[165] *See* Dillet, *supra* note 22. Google's fine is the largest fine under the GDPR to date. Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019) https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html [https://perma.cc/QR92-XR95].

[166] *GDPR in Numbers*, *supra* note 164.

B. California's 2020 Rollout of the CCPA

"On June 28, 2018, California became the first U.S. state with a comprehensive consumer privacy law when it enacted the California Consumer Privacy Act of 2018 (CCPA)."[167] This regulation went into effect January 1, 2020 and aims to protect consumers residing or domiciled in California. [168] In some ways, the CCPA is similar to the GDPR in that the main goal of the CCPA is to protect the processing of personal information capable of identifying a human being.[169] One of the most important provisions from the GDPR, "the right to be forgotten," has also made its way to the CCPA, where "a consumer has the right to deletion of personal information a business has collected."[170] There is also an important exception to both the CCPA and the GDPR protection schemes: data that has been de-identified, or otherwise made anonymous.[171] Indeed, if the information can no longer be connected, or successfully used, to identify an individual, users would have no need to control that data because their identity or likeness would not be at stake.

---

167 Jehl & Friel, *supra* note 162, at 1.

168 *Id.* Defined as: "California residents that are either: In California for other than a temporary or transitory purpose. Domiciled in California but are currently outside the State for a temporary or transitory purpose. Consumers include: Customers of household goods and services. Employees. Business-to-Business transactions." *Id.* at 2.

169 *Id.* The CCPA excludes from "personal information" matters of public record and other information under the protection of different legislation outside the regulation's scope. *Id.*

170 *Id.* at 5. Unlike the GDPR, which sets forth six circumstances under which a user may request deletion of their data, the CCPA has no prerequisites to users' data deletion but such requests are subject to exceptions. *Id.* The regulation does allow businesses to have some discretion over whether they honor a request, although revocation of consent should be enough. *Id.*

171 *See* Ribarić & Pavešić, *supra* note 4, at 296.

> The terms de-identification and anonymization are often used interchangeably, but there is difference between them. De-identification refers to the reversible (two- directional) process of removing or obscuring any personally identifiable information from individual records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them.
>
> Anonymization refers to an irreversible (uni-directional) process of de-identification that does not allow the original personal identifiers to be obtained from de-identified ones.

Id.

While the GDPR focuses on data processors in the general sense, meaning that any person or entity can process a resident's individual data, the CCPA targets large-scale businesses that utilize data brokers to engage primarily in the buying and selling of data.[172] The Act only regulates commercial companies that do business in California, or companies that are under the control, or share common branding with, a Californian entity. To fall within the scope of the regulation, it must be shown that the entity *also* satisfies one of the following requirements: "Has a gross revenue greater than $25 million. Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes. [Or] [d]erives 50 percent or more of annual revenues from selling consumers' personal information."[173] Where the GDPR regulates all the data controllers and processors established in or providing services or goods within the EU, it is clear the CCPA is much narrower in scope. The regulation of the data broker industry, in California alone, could be immensely helpful in determining how that industry works and adequately assessing the risk levels associated with the dissemination of sensitive data.

Another key difference between the two approaches is the ability to opt out. The GDPR provides users with an opt-out ability, where data subjects can withdraw consent and "opt-out of processing data for marketing purposes" at any time. but the option is not as strict as the CCPA's. The California law requires action on the part of companies to "enable and comply with a consumer's request to opt-out of the sale of personal information to third parties[.]"[174] Additionally, the CCPA requires that businesses "include a 'Do Not Sell My Personal Information' link in a clear and conspicuous location on a website homepage."[175]

One of the biggest differences between the GDPR and the CCPA is *who* may file an action against businesses that allegedly violate the regulations. Under the CCPA, private individuals generally cannot sue businesses, but there is an avenue "if there is a data breach, and even then, only under limited circumstances."[176] Otherwise, it falls to the

---

172 Jehl & Friel, *supra* note 162, at 1–2.

173 *Id.* at 1.

174 *Id.* at 4.

175 *Id.*

176 *California Consumer Privacy Act (CCPA)*, CA.GOV, https://oag.ca.gov/privacy/ccpa [https://perma.cc/23TM-LEQX] (select the seventh option entitled "What can I do if I think a business violated the CCPA?"

California Attorney General to bring an action against businesses.[177] Under the GDPR, all EU residents, or "data subjects," have a right to compensation from a data processor or controller that violated the Regulation;[178] the subject may institute an action for that compensation in any competent Member State court where he or she resides or where the company has an establishment.[179]

C. The Reimagined Right of Publicity & The CCPA

On its face, California's Consumer Privacy Act seems to mitigate some of the concerns surrounding autonomy and biometric data because it allows users to regain ownership and control of their data. Because this regulation is in the heart of one of the largest economies in the world—Silicon Valley in California—there is risk of a chilling effect on tech companies seeking to innovate through the use of biometrics.[180] Furthermore, because the CCPA only affects large-scale companies, data brokers, and entities doing business in California, the effect it will have on the United States is largely unknown. However, with many tech giants based in California,[181] it is possible the effects of the CCPA will be felt nationwide as companies overhaul their privacy policies to account for the increased protections of biometric data.

It is also possible that the CCPA could support the resurgence, or a reimagined version, of the right of publicity. Instead of eclipsing the

---

under the heading "A. GENERAL INFORMATION ABOUT THE CCPA"). Private individuals

> can sue a business if [their] nonencrypted and nonredacted personal information was stolen in a data breach as a result of the business's failure to maintain reasonable security procedures and practices to protect it. If this happens, [they] can sue for the amount of monetary damages [they] actually suffered from the breach or 'statutory damages' up to $750 per incident.

Id.

177 *Id.* Although private consumers may also file complaints against the businesses with the California Attorney General in order to initiate the process. *Id.*

178 2016 O.J. (L 119) 679 at art. 82.

179 *Id.*

180 *See* Samantha Ann Schwartz, *CCPA Critics Warn Innovation Could Lose Under the Law. What's at Stake?*, CIODIVE (July 14, 2020), https://www.ciodive.com/news/california-privacy-security-ccpa/579716/ [https://perma.cc/5BLX-HL5M].

181 Barbra Murray, *Bay Area Tech Giants Expand Across US*, COM. PROP. EXECUTIVE: RES. CTR. (Oct. 14, 2019), https://www.cpexecutive.com/post/bay-area-tech-giants-expand-across-us/ [https://perma.cc/DEC7-9LLY].

right of publicity, the CCPA could work in conjunction with the right of publicity, by providing evidence of the commercial value of a non-celebrity's biometric data. Working in concert, the CCPA would operate as a preventative measure by deterring companies from usurping user identities, while the right of publicity would operate as the endgame by enjoining companies' continued use or control over users' identities. The CCPA's effect on data brokers, with its focus on transparency and compliance with data privacy and publicity rights, will shed light on which companies sell biometric data, to whom, and for what purpose.[182]

VI. CONCLUSION

> *Under the spreading chestnut tree*
> *I sold you and you sold me:*
> *There lie they, and here lie we*
> *Under the spreading chestnut tree.*[183]

Given the newness of the CCPA, which went into effect in January 2020, it may be pragmatic to wait and observe any windfall, or fallout, from this comprehensive privacy statute before deeming it—or the GDPR—the best possible solution toward granting users increased autonomy over their biometric data. Perhaps the CCPA will serve as a model for a nationwide biometric data privacy law and perhaps it will not. Nevertheless, it will be interesting to see California "serve as a "laboratory" to address this complex socio-economic issue, "without risk to the rest of the country."[184] It seems that the CCPA, as well as the GDPR, will carry out the intent driving the right of publicity: protect individuals' rights over their person against another's exploitation to their own benefit. This is not an easy path. If these regulatory efforts do not effectuate a complete solution, a reimagined right of publicity may be the best option to defend against the misappropriation of a newly commodified identity.

---

182 *See* Timothy Tobin et al., *The Challenge Ahead – The Impact of the CCPA on Data Driven Marketing and Business Models*, HOGAN LOVELLS (Nov. 30, 2018), https://www.engage.hoganlovells.com/knowledgeservices/news/the-challenge-ahead-the-impact-of-the-ccpa-on-data-driven-marketing-and-business-models_1 [https://perma.cc/388P-BZ93].

183 GEORGE ORWELL, NINETEEN EIGHTY-FOUR 73 (1949).

184 New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).